Anti-money laundering supervision: High Value Dealers

General Introduction

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

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

You can find more about some of the successes of UK suspicious activity reporting (SAR) in the National Crime Agency SARs annual report.

Almost all businesses supervised by HM Revenue and Customs (HMRC) for anti-money laundering purposes are subject either to fit and proper test or approval requirements under the Regulations. These requirements are to ensure that businesses' beneficial owners and those in senior management are appropriate people to undertake those roles. Relevant persons must pass the appropriate test before the business can register, and 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 carefully avoid using language 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 the guidance

This guidance has been approved by HM Treasury.

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.

This guidance document is designed to provide a detailed explanation of the requirements. It is however merely guidance and is not intended to be a substitute for legal advice.

Meaning of words

In this guidance, the word 'must' denotes a mandatory requirement. Each chapter summarises the legal obligations under the heading 'minimum requirements', followed by the actions required to meet the legal obligations.

The word 'should' is a recommendation of good practice and is the standard that HMRC expects to see. HMRC will expect you to be able to explain the reasons for any departures from that standard.

The phrase 'relevant business' is the term used to describe an entity carrying out regulated activity listed in the Regulations. Within the Regulations, they are referred to as a relevant person.

The words 'minimum requirements' signify the legal minimum that your business is required to do. The words 'actions required' clarify what HMRC expects you to do to meet these 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 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 high value dealers. 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 publishes more information about businesses' obligations and the level of risk in other jurisdictions in Annex 4-1 of part 1.

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

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

1. Money laundering and high value dealers

Money Laundering

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 can take many forms, but for high value dealers (HVDs) it can involve:

- exchanging cash for high value items that can be easily transferred and sold on, sometimes at a loss, such as jewellery or vehicles
- exchanging cash for large quantities of lower value items that can be sold onwards easily such as alcohol
- exchanging cash for high value assets that are then returned and clean cash refunded.

1.3 Tax evasion is a criminal offence that can lead to money laundering. For example, sale or purchase of high value goods for cash can be underreported to avoid paying VAT or corporation tax.

Terrorist financing

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

- fund-raise or are involved in fund-raising, use, or intend to use, or possess money or other property for the purposes of terrorism
- conceal, transfer or remove from a 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
- make available funds or economic resources, directly or indirectly to a designated person, or deal with funds or economic resources which are owned, held, or controlled by a designated person.

Proliferation financing

1.5 Proliferation financing means the act of providing funds or financial services for use, in whole or in part, in the:

- manufacture,
- acquisition,
- development,
- export,
- trans-shipment,
- brokering,
- transport,
- transfer,
- stockpiling of,

or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.

Legislation

1.6 The Money Laundering Regulations 2017 set out what relevant businesses such as high value dealers must do to prevent the use of their services for money laundering, terrorist financing or proliferation financing purposes. This guidance focuses mainly on these Regulations.

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

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- 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
- Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019, ISIL (Da’esh) and Al-Qaida (United Nations Sanctions) (EU Exit) Regulations 2019 and Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019)
- Sanctions and Anti Money Laundering Act (2018)
- Anti-terrorism, Crime and Security Act 2001
- The Counter-Terrorism Act 2008, Schedule 7

1.8 Information on Financial Sanctions can be found through:

- HM Treasury Sanctions Notices, Guidance and News Releases

- Further guidance and information across [all of the UK sanctions framework] on GOV.UK

1.9 The Proceeds of Crime Act sets out the primary offences related to money laundering, which apply to everyone:

- 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.

1.10 The primary money laundering offences apply to everyone.

1.11 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 high value dealers. This obligation extends across the whole business, so a high value dealer should also report any suspicious activity not related to a relevant cash payment.

1.12 The Terrorism Act sets out the primary offences relating to terrorist financing. Regulated businesses, like high value dealers, must report belief or suspicion of offences related to terrorist financing, which can be found at section 1.4.

1.13 The Criminal Finances Act 2017 makes important amendments to the Proceeds of Crime Act, 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 also introduces corporate criminal 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.

1.14 The Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019, ISIL (Da'esh) and Al-Qaida (United Nations Sanctions) (EU Exit) Regulations 2019 and Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019) broadly replace Part I of the Terrorist Asset-Freezing etc. Act 2010 and give the FCDO and 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 restrict their 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 terrorists and allows for freezing orders to be made against national security threats and the civil asset seizure regime for terrorism.

1.16 The 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 *HM 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 under UK autonomous financial sanctions legislation and UN sanctions. OFSI helps to ensure that these financial sanctions are properly understood through sanctions notices, guidance and news releases.

1.18 As a supervisory authority HMRC is responsible for monitoring the compliance of the businesses it supervises within 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.

Data Protection

1.19 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, using or disclosing of the information.

1.20 Personal data obtained by a relevant person under the Regulations may only be processed for the prevention of money laundering, terrorist financing or proliferation financing, unless use of the data is allowed by other legislation or after obtaining the consent of the data subject.

1.21 You must provide new customers with a statement that personal data will only be used for the purposes of preventing money laundering, terrorist financing or proliferation 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 a UK 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.

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

Financial sanctions

1.23 UK financial sanctions apply within the territory of the UK and to all UK persons, legal or natural, wherever they are in the world.

1.24 All individuals and legal entities who are within or undertake activities within the UK's territory must comply with UK financial sanctions that are in force. All UK nationals and 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.

1.25 The UK imposes sanctions applied by the UN as well as a number of its own domestic sanctions, implemented by the OFSI (e.g. Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019, ISIL (Da'esh) and Al-Qaida (United Nations Sanctions) (EU Exit) Regulations 2019 and Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019)).

1.26 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 e-alert notices which go out to subscribers, published guidance and news releases.

1.27 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 under financial sanctions regulations. You should report any transaction(s) carried out for persons subject to sanctions or if they try to use your services.

1.28 When reporting to OFSI you must include the information or other matters on which the knowledge or suspicion is based and any identifying information that you hold about the person or designated person. If you know or have reasonable cause to suspect that a person is a designated person and that person is your customer, you must also state the nature and amount of funds or economic resources held by you for that customer.

1.29 Reports of frozen funds and economic resources, information regarding a designated person, and notifications of credits to frozen accounts should be emailed to: ofsi@hmtreasury.gov.uk. Reports regarding suspected breaches should be submitted to OFSI. You can sign up for free email alerts and obtain information on the current consolidated list of asset freeze targets and persons subject to restrictive measures.

1.30 To assist in complying with financial sanctions we recommend that you refer to the 'Frequently Asked Questions' on the OFSI website.

High Value Dealers

1.31 "High Value Dealer" is the term used to describe businesses and sole traders that make or receive relevant cash payments of 10,000 euros or more (or equivalent in any currency) in exchange for goods. This includes when a customer deposits cash directly into your bank account, or when they pay cash to a third party for your benefit.

1.32 HMRC considers a relevant cash payment to be:

- a single cash payment of 10,000 euros or more for goods
- several cash payments for a single transaction totalling 10,000 euros or more, including a series of payments and payments on account
- cash payments totalling 10,000 euros or more which appear to have been broken down into smaller amounts so that they come below the relevant cash payment limit

1.33 You must not make or receive a relevant cash payment unless you have applied to register as an HVD with HMRC. Guidance on how to register with HMRC for anti-money laundering supervision in on GOV.UK.

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 on GOV.UK.

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 high value dealer 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, terrorist financing and proliferation financing.

2.2 A senior manager is an officer or employee who has sufficient knowledge of your business' exposure to money laundering, terrorist financing and proliferation financing risk and is of sufficient authority to make decisions that affect your business' risk exposure. 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 address the risk of money laundering, terrorist financing and proliferation 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. The 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, terrorist financing and proliferation 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, terrorist financing and proliferation financing identified in risk assessments. This will take a risk-based approach, focusing on higher risk whilst mitigating and managing the residual risks
- ensure policies, controls and procedures are reviewed and updated to reflect changes to the risks faced by the business and written records of any changes are kept.
- approve the establishment, or continuation of a business relationship with a politically exposed person or a family member or known close associate of a politically exposed person

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

- make sure those conducting relevant activity are appropriately trained and 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 persons from or based in high risk third countries identified by the Financial Action Task Force (FATF), Foreign Commonwealth and Development Office (FCDO) or financial sanctions targets by HM Treasury as advised by OFSI and take additional measures to manage and lessen the risk
- devote enough resources to deal with money laundering, terrorist financing and proliferation financing.
- check the most up to date version of Schedule 3ZA of the Regulations, when dealing with a high risk third country.
- devote enough resources to deal with money laundering, terrorist financing and proliferation financing.

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, terrorist financing or proliferation 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, terrorist financing and proliferation financing that your business faces allowing you to effectively manage and mitigate these risks.

3.2 Several features of the high value dealer sector make it attractive to criminals, such as the anonymity of cash, the one-off nature of many transactions and the ease of carrying high value goods across borders.

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, terrorist financing and proliferation 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, terrorist financing and proliferation financing.

Risks your business may face

3.4 Assessing the risks your business faces will help you understand those risks and how they may change over time, or in response to the steps you take. 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 may face depends on factors including the nature of the business, how it is structured (e.g., branch network), the areas it operates in, who your customers are, where they are from and the vulnerability of your services or transactions to financial exploitation.

3.6 Specific risks in relation to high value dealers are covered in section 8. 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.

Risk assessment

3.7 Your risk assessment identifies 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, terrorism financing and proliferation financing risks, and design systems to deal with them.

3.8 You must:

- ensure your risk assessment identifies and monitors the risks of money laundering, terrorist financing and proliferation financing that are relevant to your business including those posed by:
  - customers and any underlying beneficial owners (see sector guidance on customer due diligence on who is the beneficial owner) and financing methods
  - services or transactions provided by your business

  - 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 HM Treasury, FCDO or FATF as having deficient systems to prevent money laundering, terrorist financing or proliferation financing.
  - size and nature of your business

- Take note of information on risk and emerging trends from sources including HMRC's risk assessment, the UK National Risk Assessments of money laundering and terrorist financing, and proliferation financing, when published, and amend your procedures as necessary.

3.9 Your risk assessment must be in writing (this can be in a digital format) 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 noted in the document.

3.10 The risk assessment must be given to HMRC when we ask for it, as well as the information on which the risk assessment was based and any records required to be kept, under regulation 18.

3.11 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 terrorist financing and proliferation financing risks). We will expect you to be compliant with the requirements of the Regulations in all other respects. Contact HMRC if you think this applies to you.

Customers

3.12 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.

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

- delivery channels: the way the customer comes to the business affects the risk for
  - non face-to-face customers

  - face to face customers
  - occasional transactions, as opposed to ongoing business
- does the pattern of behaviour, or changes to it, pose a higher risk?
- if you accept customer introductions from an agent or third party, have you accepted customers from this source before?
- are customers companies, partnerships, trusts or some combination of these?
- do you undertake business in areas with a highly transient population?
- is the customer base stable or does it have a high turnover?
- do you act for international customers or customers you don't meet?
- do you accept business from abroad, particularly those based in, or have beneficial owners in tax havens, or countries with high levels of corruption, or where terrorist organisations operate such as shown on the Transparency International 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?
- do your customers fall into categories which indicate that they should be looked at more carefully than other customers that present a low apparent risk of money laundering, terrorist financing, and proliferation financing – for example:
  - customers carrying out large, one-off cash transactions
  - customers that are not local to the business
  - overseas customers especially from a high risk third country identified by HM Treasury, FCDO or FATF
  - individuals in public positions and/or locations that carry a higher exposure to the possibility of corruption, including politically exposed persons (see sector guidance on politically exposed persons)
  - complex business ownership structures with the potential for concealing beneficiaries?

3.14 Other situations that may present a higher risk and need to be considered in your risk assessment are covered in the enhanced due diligence at section 4 and levels of risk connected with politically exposed persons.

3.15 See also the High Value Dealer risk section which details some of the specific risks that your business may be subject to.

Policy, controls and procedures

Policy statement

3.16 Your policy statement must lay out your policy, controls and procedures and how you and other senior managers will manage the business's exposure to risk. It must 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, terrorist financing and proliferation financing and take account of any additional risk due to the size and nature of your business. It should make clear who has responsibility for maintaining, managing and monitoring the policies and procedures.

3.17 Policies, controls and procedures must be approved by a senior manager, kept in writing (this can be in a digital format) and be communicated throughout your organisation to staff, branches and subsidiaries in and outside the UK. It must also be regularly reviewed and updated. You must keep a record of any changes made, the steps taken to communicate the policy, controls and procedures within the business, and copies of any previous risk assessments.

Controls and procedures

3.18 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.

3.19 You must take into account situations that, by their nature, can present a higher risk of money laundering, terrorist financing or proliferation 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 will underpin the nature of your measures for mitigating and managing money laundering, terrorist financing and proliferation financing risks.

3.20 You must ensure that when new products, business practices or technology are adopted, appropriate measures are taken to assess and if necessary, mitigate any money laundering, terrorist financing or proliferation financing risks that may arise.

3.21 You must specify the undertaking of additional measures, where appropriate, to prevent the use for money laundering, terrorist financing or proliferation financing of transactions which might favour anonymity. This could include putting in place additional due diligence measures.

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. You will always need to consider the circumstances of each case, which you will need to assess on an individual basis.

Minimum requirements

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

- carry out customer due diligence checks and conduct ongoing monitoring

- identify when a customer or beneficial owner is a politically exposed person or a family member or close associate of a politically exposed person, 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. The nominated officer can delegate responsibilities but must do so clearly and in writing
- make sure the staff are trained to recognise money laundering, terrorist financing and proliferation financing risks and understand what they should do to manage these, including the importance of reporting suspicious activity to the nominated officer
- ensure staff and the staff of any agents are aware of the anti-money laundering policies and procedures you have put in place
- review and update the business's policies, controls and procedures
- maintain accurate, up-to-date record keeping and retention of records
- have processes in place to monitor and manage compliance with the internal communication of such policies, controls and procedures
- have processes in place to identify and monitor transactions which are unusually large or complex, or contain unusual patterns of transactions without any apparent commercial purpose, or which you regard as particularly likely by their nature to be related to money laundering, terrorist financing or proliferation financing
- have processes in place that specify the taking of additional measures where appropriate to prevent the use for money laundering, terrorist financing or proliferation financing of products and transactions which might favour anonymity
- have policies that ensure you adopt appropriate measures to assess and, if necessary, mitigate the money laundering, terrorist financing or proliferation financing risks of new products, business practices or technologies that you adopt.

Actions required

3.24 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 politically exposed persons
- ensure low risk situations are assessed and records retained to justify your assessment
- ensure arrangements for monitoring systems and controls are robust, and 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 (not including Suspicious Activity Report details) for the purposes of preventing money laundering, terrorist financing and proliferation financing.
- when the business adopts new products, business practices or technology, these must be immediately incorporated into the business' policies, controls and procedures.

3.25 Where the controls you have in place identify any weakness, you should document it and record the action taken to put the problem right.

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

- the appointment of a compliance officer from the board of directors (or equivalent body) or senior management who has responsibility for monitoring the effectiveness of and compliance with the policies, controls and procedures, including regular reviews to learn from experience
- individual staff responsibilities under the Regulations where this is not confined to the Nominated Officer

- the process for auditing the business's compliance with its policies, controls and procedures.

Making relevant appointments within your business

3.27 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 particular reports to the National Crime Agency.

3.28 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.

3.29 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.

3.30 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

3.31 You must appoint a nominated officer from within your business to receive reports of suspicious activity from staff and decide whether to report particular reports 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.

3.32 The nominated officer should be at an appropriate level of seniority in your business to make decisions on whether individual transactions are suspicious and must be reported to the National Crime Agency.

3.33 You should make sure that your staff 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

3.34 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, terrorist financing and proliferation 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.

3.35 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.

3.36 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.

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

3.38 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.

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

- carrying out regular audit(s) on compliance with the regulations such as:
  - actively checking adherence to the policies, controls and procedures
  - reviewing of how effective these are

    - recommending and implementing improvements following such reviews
- ensure compliance throughout the business (including subsidiaries and branches) with anti-money laundering legislation and internal policies/procedures
- oversight of relevant staff and agent screening.

3.40 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.

3.41 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 and nominated officers 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 of the business who is knowingly concerned in a breach of the Regulations may be subject to a civil penalty. That is, they have identified or have knowledge of something that could be considered at risk of breaching the Regulations.

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, terrorist financing and proliferation 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' risk assessment.

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

- the types of customers and transactions that you consider to be lower risk and why they qualify for simplified due diligence and those that are higher risk and merit closer scrutiny
- how to carry out customer due diligence, the identification requirements for customers and beneficial owners and how to carry out enhanced due diligence on higher risk customers
- any other patterns or activities that may signal that money laundering, terrorist financing or proliferation financing is a real risk in connection with an individual customer/transaction
- how to identify politically exposed persons and what to do when one is identified, in particular, how to identify their source of wealth and source of funds
- what to do if you are dealing with an individual subject to the sanctions regime or who is based in a jurisdiction of concern
- 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 to audit and monitor the policies and procedures and the internal controls in place to ensure that the policies and procedures are followed correctly by staff
- how to report suspicious activity to the nominated officer, and how the nominated officer should make a report to the National Crime Agency
- how and when staff are trained and how that training is recorded.

3.52 Examples of risk-based controls could 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 checklist. 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, terrorist financing or proliferation financing. Similarly, identifying a customer or transaction as low risk does not mean that they're not involved in money laundering, terrorist financing or proliferation 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 or proliferation financing risks associated with a particular customer.

Effectiveness of the controls

3.56 Managing the money laundering, terrorist financing and proliferation 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, terrorist financing and proliferation 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 a third country 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 network

3.60 If you manage a branch 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 branches
- how will you manage and maintain records, for example, if the branch closes
- 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 or branches are not implementing risk management procedures
- could you demonstrate that all staff have been trained on the Regulations and the business' procedures, and given ongoing training on recognising and dealing with suspicious transactions and identity verification processes
- if asked, will staff in all your branches know who the nominated officer is, what the firm's policies are and where they can be found.

4. Customer due diligence (CDD)

Minimum requirements

4.1 You must:

- complete customer due diligence on all customers and conduct checks on 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

- apply CDD if you carry out an occasional transaction in cash that that amounts to 10000 euros or more, whether the transaction is executed in a single operation or in several operations which appear to be linked. You must have procedures to identify those who cannot produce standard documents, for example, a person not able to manage their own affairs
- identify and verify a person acting on behalf of a customer and verify that they have authority to act
- apply enhanced due diligence to take account of the greater potential for money laundering or terrorist financing in higher risk cases, including in respect of politically exposed persons or persons established in high-risk countries
- identify politically exposed persons, their family members and close associates and verify their identity, source of wealth and/or funds. You must also have a procedure in place so that a senior manager can consider and give approval on whether to carry out business with that person
- apply customer due diligence, when you become aware that the circumstances of an existing customer have 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 and consider 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.
- understand the ownership and control structure of a customer when the customer is one of the following (non-exhaustive):
    - legal person
    - trust
    - company
    - foundation, or
    - similar legal arrangement

What is required of an HVD under the Regulations?

4.2 At the heart of the Regulations is a requirement that HVDs must identify the physical person who they are dealing with in any transaction or, when dealing with a corporate body or a trust, the person or persons who control that entity. In other words, “Who are you really dealing with?” This is known as customer due diligence (CDD).

4.3 Any person or entity identified in this way will also be required to verify and prove their identity, either through identity documents or official corporate documents, or electronically.

4.4 You must do customer due diligence on all customers, even if you knew them before they became your customers. This is because you must be able to show that you have verified the identity of all your customers.

CDD requirements for high value dealers

4.5 For the purposes of the Regulations, for HVDs, this means that you must apply CDD to:

- the individual or business from whom you are receiving a relevant cash payment
- the individual or business to whom you make a relevant cash payment.

This includes situations where the HVD is dealing as an auctioneer while also trading.

4.6 For these purposes, references to "customer" include the person or persons with whom the HVD establishes a business relationship.

What Customer Due Diligence means

4.7 Customer due diligence means:

- Identifying all customers and verifying their identity
- identifying all beneficial owners, where applicable, and taking reasonable measures to verify their identity to satisfy yourself that you know who the beneficial owners is
- 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 business's risk assessment
- retaining records of these checks and update them when there are changes.

4.8 If you are making or receiving a relevant cash payment for goods by way of business, you will need to perform customer due diligence before undertaking the transaction. If the other party to the transaction is in the UK and also in the business of buying and selling high value goods, part of your customer due diligence must include checking if they are registered with HMRC as a High Value Dealer. You should also check if your customer is registered for supervision if they trade in a regulated sector.

4.9 If they are trading in goods by way of business in the UK but are not registered as a High Value Dealer you should not continue with that relevant cash payment. You should consider reporting this activity to the National Crime Agency (NCA) via a Suspicious Activity Report (SAR). Failure to do this may result in sanctions being applied to your business, including the possibility of withdrawing your HVD status and your details being published on GOV.UK.

4.10 It is also important to confirm the identity of any delivery drivers or intermediaries and ensure they work on behalf of whom you expect and, if they are agents, conduct the appropriate agency checks.

When to undertake Customer Due Diligence

4.11 You must undertake customer due diligence:

- before establishing a business relationship, with a customer when a relevant cash payment meets the definition of an HVD.
- before carrying out an occasional transaction with a customer valued at 10,000 euros or more (in a single operation or in several operations which appear to be linked) – whether you are making or receiving the payment
- when you suspect money laundering or terrorist financing
- when you suspect that information obtained for due diligence checks on a customer is not reliable or adequate

4.12 Example:
A wholesale business (X) sells a quantity of goods to (Y), which is itself a business. (Y) makes a relevant cash payment to X for the goods. X is receiving the payment and is an HVD and must apply CDD on Y and its beneficial owners. In turn Y is making the payment and is also an HVD. Y must carry out CDD on X and its beneficial owners.

4.13 Customer due diligence is required in any situation where you suspect money laundering or terrorism financing. This is regardless of whether the transaction involves a relevant cash payment. You should also consider raising a suspicious activity report in these circumstances.

4.14 HMRC recommend that you perform customer due diligence if you give out your bank details to customers. This is in case your customers choose to deposit cash into your account when they originally told you they would pay by bank transfer. You may wish to raise a suspicious activity report in these circumstances.

Timing of customer due diligence

4.15 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.

4.16 You can make an exception to when customer due diligence is carried out only if both the following apply:

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

4.17 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.

4.18 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 in line with its risk assessment.

Non-compliance with customer due diligence

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

- Make or receive any relevant cash payments to or from the customer
- establish a business relationship or carry out an occasional transaction with the customer for any relevant cash payments

4.20 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.

4.21 You must:

- terminate any existing business relationship with the customer for relevant cash payments
- consider making a suspicious activity report
- if no suspicious activity report is made, record the reasons why you consider that a report is not required.

Business relationship

4.22 A business relationship is a business, professional or commercial relationship between a 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 business exists where:

- another 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
- or any other arrangement facilitates an ongoing business relationship or repeat custom, such as providing a unique customer identification number for the customer to use.

4.23 If the customer is a business, you must collect proof of registration or an excerpt of the register under the law which it is subject before a business relationship is established. For example, in the UK it should 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

4.24 You must collect proof of the customer's registration or an excerpt of the register for which they are registered before establishing a business relationship with them.

4.25 You must report any discrepancy you find between information relating to the beneficial ownership of the customer which becomes available to you.

4.26 From 1 April 2023, before establishing a relationship with a customer that is a company, unregistered company, limited liability partnership, eligible Scottish partnership, trust, or an overseas entity, you must either collect an excerpt of the register which contains full details of the information held or establish that there is no information held at that time. This must also be done as part of ongoing monitoring.

Ongoing monitoring of a business relationship

4.27 You must continue to monitor a business relationship after it is established and for its duration. This means you must monitor transactions on a risk-based approach, and where necessary the source of funds, to ensure they are consistent with what you know about the customer and the customer's business and risk assessment. 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.

4.28 You must also undertake reviews and keep the information you collect up-to-date in line with your risk assessment. It should be checked periodically, and expired documents replaced with copies of newly issued documents.

Occasional transactions

4.29 An occasional transaction is a transaction that is not part of an ongoing business relationship. CDD must be carried out on occasional transactions of €10,000 or more (or the sterling equivalent). It also applies to a transaction totalling €10,000 or more, where the transaction appears to be broken down into several, linked operations to be below €10,000.

4.30 The value of the transaction here means the gross value of the goods in the transaction.

4.31 Linked operations may be several transactions by the same customer for goods. This could be the purchase of alcohol for £15,000 and then paid in three lots of cash of £5,000 or the purchasing of £5,000 of alcohol three times over a short period and then paying the total of £15,000 in cash in one payment. You must have procedures in place to detect this. Because linked operations are deemed higher risk you may need to perform enhanced due diligence on the customer making them. You should also report any suspicious activity you detect, in accordance with your policy.

4.32 HMRC considers multiple cash payments against a single invoice, which together exceed the €10,000 threshold to be linked operations, regardless of how long it takes to make this payment. For example, if a customer pays monthly instalments of £2,000 over a year in cash against the cost of a car.

Beneficial owners

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

4.34 Examples of beneficial owners may include:

- a person that is using another person to shield them from coming into contact with you

4.35 For a corporate body that is not a company whose securities are listed on EEA regulated market and certain other main markets (USA, Japan, Switzerland, and Israel), 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, or
- controls the corporate body.

4.36 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.

4.37 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.

4.38 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.

4.39 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.

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

4.41 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
- exercises ultimate control over the management.

4.42 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
- any individual who has control over the trust

4.43 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 in this list

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

4.45 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

4.46 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

4.47 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.

4.48 If the business has exhausted all possible means of identifying the beneficial owner, it will be deemed acceptable if the business is able to take reasonable measures to verify the identity of the senior person within the business (customer) responsible for management. The business should keep records in writing of actions taken place to achieve this and any difficulties the business had in achieving this.

4.49 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

4.50 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.

4.51 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.

4.52 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.

4.53 Using your risk assessment, you should determine the extent of due diligence you will conduct depending on the type of customer you will be checking, i.e., the entity who is making the payment to you or the entity you are paying. The types of checks you undertake will differ for each, as the risks associated with them will vary.

4.54 For example, if a customer attempts to make a cash payment with a significant amount of Scottish notes when there does not appear to be any reason to do so (e.g., both you and your customer are based in London without any immediate ties to Scotland), you should make enquiries as to why that may be, and if suspicious, you should consider making a suspicious activity report.

4.55 Similarly, if any goods you are purchasing appear to be significantly cheaper than the market rate, you should make enquiries as to why that may be, and if suspicious, you should consider making a suspicious activity report.

Simplified due diligence

4.56 Your business may apply a simplified form of due diligence in some cases.

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

4.58 The expected starting level of due diligence is customer due diligence. You will need to demonstrate why you have deviated from this, if you decide that simplified due diligence is sufficient. You will have to risk assess the customer to establish that they are low risk, taking into account relevant factors, including information made available by HMRC.

4.59 This does not mean you do not have to do customer due diligence, and you are still required to identify and verify customers' identity and take reasonable measures to verify the beneficial owners' identity. 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 of that scheme 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

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

4.61 To apply simplified due diligence, you need to ensure that all of the following apply:

- 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 contradictory to information on risk provided by HMRC or any other authority in periodically published risks assessments
- the customer is not established in or operates from a high risk third country identified by the FATF, FCDO or HM Treasury

- the customer is not a politically exposed person, or a family member or 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
- where the customer is not an individual, that there is no beneficial ownership beyond a single UK legal entity customer
- where the customer is not an individual, that the legal entity is not registered or administered outside of the UK.

4.62 To decide whether a customer is suitable for simplified due diligence you must 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.

4.63 The following types of customer 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

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

- resident or established in an EEA state
- situated outside the UK in a country:
    - subject to equivalent anti-money laundering measures
    - with a low level of corruption or terrorism
    - has been assessed by organisations such as 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.

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

4.66 You must consider all the factors, for example a customer from an EEA state is not automatically low risk simply because they are from the EEA (see also the list of high-risk third countries). All the information you have on a customer must indicate a lower risk.

4.67 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.

4.68 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.

4.69 You must 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, persons of professional standing or persons 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.

4.70 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.

4.71 Your decisions may be tested based, as part of a HMRC compliance, on the evidence that your business holds.

4.72 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, or
- circumstances change and your risk assessment no longer considers the customer, transactions or location as low risk.

Enhanced due diligence

4.73 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.

4.74 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 other supervisor or law enforcement authority provide information that a particular situation is high risk
- a customer or any party relevant to the transaction, operates or is established in a high risk third country identified by the FATF, FCDO or HM Treasury

- a customer or other party is established in, or operates in a high risk third country is published in the most up to date version of schedule 3ZA of the Regulations
- a person has given you false or stolen documents to identify themselves (immediately consider reporting this as suspicious activity)
- a customer is a politically exposed person, an immediate family member or a close associate of a politically exposed person
- the transaction is complex or unusually large or with an unusual pattern and has no apparent legal or economic purpose
- a customer is the beneficiary of a life insurance policy or legal arrangement and presents a high risk of money laundering or terrorist financing for any other reason
- during the course of completing due diligence, the business identifies 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.

4.75 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 is supervised under the 4th Money Laundering Directive may not be subject to enhanced due diligence if your risk assessment finds it is not high risk.

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

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

- unusual aspects of a business relationship
- the customer 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 bearer shares
- 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.

4.78 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
- the transaction involves nominee directors, nominee shareholders or shadow directors or a company formation is in a third country

4.79 Geographical factors indicating higher risk:

- Countries identified by a credible source as:
  - not subject to anti money laundering or counter terrorist measures equivalent to the UK
  - having a significant level of corruption, terrorism or supply of illicit drugs
  - subject to sanctions or embargoes issued by, for example, the 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 UK, EU, other countries and international organisations such as United Nations
- Countries that have 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 not implementing measures to counter money laundering and terrorist financing that are consistent with the FATF recommendations.

4.80 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

4.81 Enhanced due diligence measures must be taken when any business relationship or relevant transaction is established in a high-risk third country.

Additional measures to take

4.82 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 original documents supplied from independent sources, such as more documentation on identity or address or electronic verification alongside manual checks 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, such as a person from a regulated industry or in a position of trust

- ensure any information on identity documents is validated by an authoritative source
- check if the identity is known to be involved with any fraudulent activity or documents
- 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 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
- 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

4.83 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.

4.84 Information about [certification of documents] is available on GOV.UK.

Politically exposed persons (PEPs)

4.85 PEPs are persons that are entrusted with prominent public functions, whether in the UK or abroad. This is because international standards issued by the 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.

4.86 The definition does not include:

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

4.87 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.

4.88 PEPs 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 (for example, 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
- 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, for example 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 NATO
    - does not include international sporting federations.

4.89 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

4.90 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 brothers and sisters) as subject to enhanced due diligence measures in cases where a firm has assessed a PEP to present a higher risk.

4.91 The Regulations require that close associates of PEPs must also have enhanced due diligence measures applied to them. the definition of “close associate” includes:

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

PEP risk

4.92 You must always apply enhanced due diligence on PEPs, their family members or a known close associate on a risk-sensitive basis. You must have appropriate risk management systems and procedures in place to determine whether a customer is a PEP 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 PEPs
- a case by case assessment of the risk posed by a relationship with a PEP
- any information provided through the UK National risk assessment of money laundering and terrorist financing or by HMRC

4.93 Information is available in the public domain that will help you to identify PEPs. You can make use of a number of sources, for example:

- ask the customer
- search the internet
- news agencies and sources
- government and parliament websites
- Electoral Commission
- Companies House Persons of Significant Control register
- Transparency International
- Global Witness

4.94 You are not required to, but you may decide to use a commercial provider to assist in identifying PEPs.

4.95 If a customer is a PEP, family member or known close associate of one, then you must put in place all of 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.

4.96 You must, however, assess in each case the level of risk that the PEP presents and apply an appropriate level of enhanced due diligence. More frequent and thorough measures should be taken if the PEP is higher risk. Similarly, a reduced level of enhanced due diligence measures can be applied to lower-risk PEPs. A PEP 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 PEPs.

4.97 You must continue to apply enhanced due diligence when the PEP has left the 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 PEP you have assessed as higher risk. 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.

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

4.99 The level of risk of a PEP may vary depending on where they are from and the public accountability they are subject to. The following are examples only.

4.100 A lower risk PEP 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

4.101 A PEP 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

4.102 A high risk PEP may be from, or connected to, a country viewed as having a higher risk of corruption that may have with traits such as:

- high levels of corruption
- political instability
- weak state institutions
- weak anti-money laundering measures
- armed conflict
- non-democratic forms of government
- widespread organised criminality or illicit drug supply
- a political economy dominated by 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

4.103 A high risk PEP 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

4.104 A family member or known close associate of a PEP may pose a lower risk if they:

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

4.105 The family and known close associates of a PEP 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.

4.106 Where you have assessed a PEP 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.

4.107 You must always apply enhanced due diligence to PEPs, their family members and known close associates. However, where your risk assessment indicates a lower risk, the PEP, family member 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

4.108 You should identify when a PEP 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 PEPs as well. If the PEP 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.

4.109 Further detail on the identification and treatment of PEPs, their family members and close associates has been provided by the Financial Conduct Authority. This guidance is nonbinding upon high-value dealers but provides further guidance as to the approach that you should take to identifying and treating both higher-risk and lower-risk PEPs.

Identifying individuals

4.110 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 names (s), date of birth and residential address as a minimum.

4.111 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.

4.112 You should verify these using identity evidence that have 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 firearm certificate
- an identity card issued by the Electoral Office for Northern Ireland

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

4.114 When verifying the identity of a customer using documents you must take a copy and keep it on 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.

4.115 Where the customer doesn't have one of these documents, you should ask for the following:

- a valid and genuine identity document from an authoritative source (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 an authoritative source, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement

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

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

4.118 You should check the documents to satisfy yourself of the customer's identity. This may include, but is not limited to checking:

- spellings
- validity
- photo likeness
- whether addresses match
- whether there are anomalies in the documents that suggest they are forgeries or fakes.

4.119 More information on official documents and how to spot counterfeits and forgeries is published by the Home Office in their 'Guidance on examining identity documents.

4.120 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.

4.121 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) taking into account whether there is a risk the property may be being used as a front. This should be covered in the risk assessment.

4.122 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

4.123 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 not driven or travelled for some time and have allowed licenses and passports to lapse.

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

4.125 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

4.126 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 document references or organisation stamps.

4.127 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 non-standard documents may be acceptable.

Electronic verification

4.128 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.

4.129 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 identify 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.

4.130 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 UK eIDAS Regulations
- it is provided by means of a trust service covered by the UK eIDAS Regulations
- 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, GOV.UK Verify or the UK eIDAS regulations)
- it is registered with the Information Commissioner's Office 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 are assessed
- it uses a range of positive information sources, and links a person, through other sources, to both current and previous circumstances
- it uses a wide range of alert source, such as up to date financial sanctions information
- it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.
- should be able 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, or
    - 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**.**

4.131 The extent of the checks should satisfy the level of risk established in your risk assessment. It is not enough 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'.

4.132 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.

Individuals not resident in the UK

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

4.134 If you have concerns that an identity document might not be genuine, contact the relevant embassy or consulate or use the Public Register of Authentic travel and identity Documents Online.

4.135 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

4.136 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.

4.137 Where you find a discrepancy about the beneficial ownership of your customer, you must report it to Companies House.

4.138 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.

4.139 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

4.140 You should establish the names of all directors (or equivalent) and must identify the ultimate beneficial owners (the section on beneficial ownership will tell you 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.

4.141 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

4.142 You do not satisfy your obligation to identify and take reasonable steps to verify the identity of beneficial owners by relying only on information contained in a PSC register.

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

- searching a relevant company registry
- checking the customer is registered to make/receive relevant cash payments
- obtaining a copy of the company's register of members.

4.144 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.

Requirement to report discrepancies in registers

4.145 If the customer is a business, you must collect proof of registration or an excerpt of the register, before you establish a business relationship with them to show the business:

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

4.146 From 1 April 2023, before establishing a relationship with a customer that is a company, unregistered company, limited liability partnership, eligible Scottish partnership, trust, or an overseas entity, you must either collect an excerpt of the register which contains full details of the information held or establish that there is no information held at that time. This must also be done as part of ongoing monitoring.

4.147 The information required is as follows:

- customer is a company, unregistered company, limited liability partnership, eligible Scottish partnership, trust: information relating to beneficial owners of the customer
- customer is an overseas entity: information relating to registerable beneficial owners specified under Schedule 1 of the Economic Crime (Transparency and Enforcement) Act 2022

4.148 You must report any material discrepancy you identify while undertaking CDD or ongoing monitoring as soon as possible.

4.149 A material discrepancy is where the discrepancy may reasonable be considered to:

- be linked to money laundering or terrorist financing, or
- conceal details of the business of the customer

4.150 Discrepancies are in the form of:

- a difference in name
- an incorrect entry for nature of control
- an incorrect entry for date of birth
- an incorrect entry for nationality

- an incorrect entry for correspondence address
- a missing entry for a person of significant control or a registrable beneficial owner
- an incorrect entry for the date the individual became a registrable person

4.151 A material discrepancy or a discrepancy relating to a company, an unregistered company, a limited liability partnership or an eligible Scottish partnership or an overseas entity must be reported to Companies House.

4.152 A material discrepancy or a discrepancy relating to trust must be reported to HMRC.

Obligation of customers to provide information

4.153 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 high value dealer 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

4.154 Guidance on the requirements to maintain PSC registers is on GOV.UK.

Beneficial owners

4.155 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 steps 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.

4.156 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.

4.157 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 written records that clearly show all the steps you have taken to identify the beneficial owners, the progress made and why they have been unsuccessful and consider whether they should be treated as a higher risk or even suspicious due to the number of entity layers.

Reliance on third parties

4.158 You must do customer due diligence before entering into a business relationship or carrying out an occasional transaction involving relevant cash payments.

4.159 As high value dealers are usually approached independently to any other businesses, you are not usually able to rely on another business performing customer due diligence for you.

4.160 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 EEA who is 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.

4.161 You may not rely on a business established in a country that has been identified as a high risk third country by the FATF, FCDO or HM Treasury .

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

- obtain immediately on request, 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.

4.163 If you rely on a third party, you'll 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.

4.164 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.

4.165 Reliance can only be on the customer due diligence carried out by another supervised business in order to meet their own requirements under the Regulations. It doesn't 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.

4.166 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.

4.167 A recipient of a relevant cash payment and a buyer carrying out an occasional transaction or in a business relationship together must not rely on each other.

4.168 Any arrangement for reliance should be written.

5. Reporting suspicious activity

Minimum requirements

- Staff must raise an internal report where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that a terrorist finance offence may be committed.

- The business's nominated officer must consider all internal reports. The nominated officer must make a report to the National Crime Agency (NCA) as soon as it is practical to do so, even if no transaction takes place, if they consider that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, or financing terrorism.

- The business must consider whether it needs to seek a defence against money laundering or terrorist financing offences (DAML) (formerly known as a consent SAR) from the NCA before proceeding with a suspicious transaction or entering into arrangements.

- It is a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place.

Actions required:

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

Suspicious activity report ("SARs")

5.1 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 or entities who you, or an employee, know, suspect, or have reasonable grounds to know or suspect may be involved in laundering money or financing terrorism.

5.2 Having knowledge means knowing something to be true, this does not necessarily mean you must have direct knowledge of the suspicion to be able to report it. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. That said, knowledge can be inferred from surrounding circumstances.

5.3 The term suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation: ‘a possibility that is more than fanciful’. What you identify initially may not seem suspicious, however looking into the issue further may increase your suspicion.

5.4 Reasonable grounds for suspecting are likely to depend upon particular circumstances and the member of staff should take into account such factors as the nature/origin of the transaction, how the funds, cash or asset(s) were discovered, the amounts or values involved, their intended movement and destination, how the funds cash or asset(s) came into the customer’s possession, whether the customer(s) and/or the owners of the cash or asset(s) (if different) appear to have any links with criminals/criminality, terrorists, terrorist groups or sympathisers, whether in the UK or overseas.

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

5.6 As a high value dealer in the regulated sector, you’re 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 customer and the transaction would cause a reasonable professional in your position to have a suspicion.

5.7 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.

5.8 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.

5.9 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

5.10 Submitting a request for a DAML 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.

5.11 It is important that you have detailed policies, controls and procedures on internal reporting and the role of the nominated officer.

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

5.13 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.

5.14 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.

5.15 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

5.16 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.

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

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

5.19 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.

5.20 If a report is made before a transaction is completed or the start of a business relationship, you must ask for a defence to a money laundering or terrorist financing offence from the NCA to go ahead with the transaction.

5.21 Where the nominated officer makes a conscious decision not to file a report to the NCA, they should document their rationale. This will help with any future prosecution for failing to report.

Defence against money laundering (DAML)

5.22 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 (DAML). This was previously 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.

5.23 You should tick the "consent requested" box on the SAR form. Search www.nationalcrimeagency.gov.uk for the latest guidance on 'Requesting a defence from the NCA under Proceeds of Crime Act and Terrorism Act'.

5.24 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.

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

5.26 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.

5.27 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.

5.28 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.

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

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

- a defence is only valid for the transaction reported - any future transactions by the same customer have to be considered on their own merits (and in the light of the suspicions that arose for the original one)
- you can't ask for a general DAML to trade with a customer, only to carry out a particular transaction
- the initial notice period is 7 working days from the date of the report; and if a defence is refused, the moratorium period is a further 31 calendar days from the date of refusal - if you need a defence sooner, you should clearly state the reasons for the urgency and perhaps contact the National Crime Agency to discuss the situation
- the National Crime Agency will contact you by telephone and will confirm their decision in writing

5.31 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

5.32 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.

5.33 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

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

5.35 There 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 are at section 8.

New customers

5.36 These are some of the questions to consider in deciding whether or not to submit a suspicious activity report when you deal with new customers:

- If checking the customer's identity is difficult, given their demographic group and likelihood they would have sufficient identity evidence
- 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
- the customer's identity cannot be proven
- 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

5.37 These are some of the questions to consider in deciding whether or not to submit a suspicious activity report in relation to your regular and existing customers:

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

- there has been a significant or unexpected improvement in the customer's financial position and the customer can't give a proper explanation of where money came from.

Transactions

5.38 These are some of the questions to consider in deciding risk and whether or not to submit a suspicious activity report in relation to the transactions you carry out:

- a third party, apparently unconnected with the customer, bears the costs, or otherwise pays the transaction costs
- an unusually large 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.

6. Record keeping

Minimum requirements

6.1 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

6.2 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

6.3 The points listed are to be kept under regular review:

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

6.4 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 at least 5 years after the end of a business relationship

6.5 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.

6.6 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.

6.7 After this period the records must be deleted unless you are required to keep them in relation to legal or court proceedings or any other legislation, or the data subject has given consent to the retention of the data.

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

6.9 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.

6.10 This evidence may be used in court proceedings against the criminals.

6.11 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.

6.12 All electronic records should be subject to regular and routine backups with off-site storage.

7. Staff awareness

Minimum requirements

7.1 You must:

- ensure relevant staff, your agents and their staff are aware of the risks of money laundering, terrorist financing and proliferation 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, terrorist financing or proliferation financing transactions or activity
- ensure staff, your agents and their staff are trained at regular intervals
- maintain a written record of what you have done to raise awareness and the training given to staff, agents and their staff
- ensure that a relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements.

7.2 Larger and more complex businesses must:

- screen relevant staff 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

7.3 You must 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, agents and their staff aware of money laundering, terrorist financing and proliferation financing issues, including how these crimes operate and how they might take place through the business
- ensure that relevant employees, agents and their 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.

7.4 You should also:

- 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, terrorist financing and proliferation financing are most likely to arise

- train relevant staff in how to operate a risk-based approach to assessing the risks of money laundering, terrorist financing and proliferation 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

Staff

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

7.6 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

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

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

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

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

Training

7.10 When you consider who needs to be trained you should include staff 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.

7.11 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.

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

7.13 Each member of staff 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.

7.14 It must include, in relation to money laundering, terrorist financing and proliferation 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.

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

- the staff member’s duties
- the risks posed to the business
- the business’ policies, controls and procedures
- how to conduct customer due diligence and check customers’ identity documents, including detecting forgeries and imposters
- how to spot and deal with suspicious customers and activity
- how to make internal reports, including disclosures of suspicious activity
- record keeping.

7.16 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 relevant publications
- meetings to look at the issues and risks.

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

7.18 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. 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.

Evidence of training

7.19 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.

7.20 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.

8. High value dealer risk

8.1 A high value dealer selling wholesale alcohol with overseas clients presents a completely different risk to a high street jeweller in a small town. However, both may be targeted by criminals if they have little or no controls in place.

8.2 The environment you do business in affects the individual customer's risk assessment. If you have many high net-worth customers or deal with people from a particular country or region, this will influence the business wide risk assessment. You should also be aware of the risk of transactions being used for tax evasion, for example dealing in goods where tax has not been declared or understated.

Your risk profile

8.3 Assessing your business's risk profile will help you design the right systems that will spot suspicious activity and ensure that staff are aware of what sort of money laundering activities they are likely to encounter.

8.4 A high value dealer that buys bulk, low value goods presents a different risk profile to a high value dealer that sells high-end luxury cars.

8.5 Cash is a key component in organised criminal activity and criminals may try to dispose of cash through the purchase of goods. Because of this, high value dealers must be vigilant to high risk areas.

8.6 You should assess the risks to your own business and consider what is high risk in your own policies, controls and procedures. The following is not an exhaustive list of risk indicators:

- assets that are particularly high value and easily portable such as jewellery
- high risk goods that are commonly used to evade tax such as alcohol or tobacco
- businesses with no security or insurance for large volumes of cash

- businesses that have no established presence
- a business you deal with is not applying the standard of due diligence you would expect
- a business wants to use cash for an “off the record” sale
- the customer asks for delivery in an unusual manner or to an address that is not their own
- visitors to the UK do not have a C9011 form (a form for declaring they are bringing more than €10,000 into the UK)
- the customer appears to be breaking down the transaction to fall below the €10,000 limit.
- use of cash with no apparent commercial or personal rationale beyond anonymity
- purchasing goods or quantities which are inconsistent with business or personal needs

8.7 Low risk indicators should also be included in your risk assessment. The following is not an exhaustive list of low risk indicators and may not represent low risk in all cases. You must consider this list in regard to your own business practices and risk assessment:

- perishable goods that have a limited life
- local customers that fit with the area and your normal trade models
- highly regulated commodities such as guns.

8.8 The risk profile depends on the nature of the business, branch network, customers, and activities. For each of these areas you should consider how they could be exposed. For example:

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

9. High value dealers

9.1 Anyone who makes or accepts relevant cash payments must comply with the Regulations. HMRC supervises High Value Dealers under these Regulations. A business must not make or accept relevant cash payments unless they have applied to register with HMRC.

9.2 The Regulations define high value dealers as a firm or sole practitioner, who or whose employees make or accept cash payments of €10,000 or more, or its equivalent in another currency in exchange for goods, including when this payment is made into your bank account or to a third party for your benefit. It does not include payment made for services. Where a payment is made for goods and services, such as fitting a bathroom, the transaction is only in scope if the goods are valued at more than €10,000 or the equivalent in another currency.

High value dealer sub sectors

9.3 There are a number of sub sectors in the high value dealer sector, they include:

- Alcohol
- Art & Antiques
- Auction
- Caravans, motorhomes & static vans
- Cars
- Cash & carry or wholesaler
- Cash & carry or wholesaler - alcohol
- Commercial vehicles
- Electronic goods
- Food
- High-end retail
- Household, Sports & Guns
- Jewellery
- Other
- Pharmaceutical or chemicals
- Recycling
- Textiles & Clothing
- Vehicles other

10. Where to find more information

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

Email: mlrcit@hmrc.gov.uk

10.2 HMRC always aim 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 GOV.UK.