Anti-Money Laundering Supervision: Trust or Company Service Providers

Who this guidance is for

This guidance is addressed to firms, proprietors, directors, managers, employees and Nominated Officers of trust or company service providers who are the subject of the Regulations. A trust or company service provider may be supervised by a number of Supervisory Authorities including the Financial Conduct Authority, the Accountancy Professional Bodies, the Legal Professional Bodies and HMRC. The professional bodies are listed in schedule 1 of the Regulations.

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

Further sources of guidance

Businesses that provide both accountancy services (ASP) and trust or company services and are supervised by HMRC should follow the Consultative Committee of Accountancy Bodies (CCAB) guidance for ASP activities, and refer also to this guidance for trust or company service provider activities.

CCAB guidance:

https://www.ccab.org.uk/reports.php

This guidance explains measures brought about by the 2017 Regulations, which came into force on 26 June 2017.

The Joint Money Laundering Steering Group (a group made up of trade associations in the financial services industry) also publishes free detailed guidance. The guidance is for members of the trade associations and firms supervised by the Financial Conduct Authority (FCA), for compliance with the Regulations. It contains detailed coverage of how to do due diligence checks on different types of

customers, report suspicious activity and do staff training and record keeping:

The Joint Money Laundering Steering Group publishes more information about businesses' obligations and the level of risk in other jurisdictions (Annex4-1 of part 1)
http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current

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

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

General Introduction

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

Meeting your legal obligations is important because it contributes to tackling the serious economic and social harm from organised crime, it also reduces the threat from terrorism in the UK and around the globe.
If you would like to know more about some of the success of UK suspicious activity reporting (SAR) see the National Crime Agency SARs annual report.

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

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

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

There is more detail about these requirements in the fit and proper test and HMRC approval guidance.

Status of the guidance

This guidance has been approved by HM Treasury.

This guidance replaces HMRC's anti-money laundering guidance for trust or company services providers published in October 2010. The guidance is effective from 26 June 2017.

Meaning of words

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

The word 'should' is a recommendation of good practice, and is the standard that HMRC expects to see. HMRC will expect you to be able to explain the reasons for any departures from that standard. The phrase ‘relevant business’ is the term used to describe carrying out regulated activity listed in the Regulations.

1. Introduction: Money Laundering and Trust or Company Service Providers

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

Money laundering takes many forms. Here are some examples detected by HM Revenue and Customs:

- Company formation using trust or company service providers to set up complex trust and company structures to layer funds or hide their true criminal origin.
- Accommodation address providers can be used to hide the identity of businesses.
- Nominee shareholders can be used to hide the identity of the business owners.

Terrorist financing

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

Legislation

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

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017
- Criminal Finances Act 2017
- Terrorist Asset-Freezing etc. Act 2010
- Anti-terrorism, Crime and Security Act 2001
- Counter-terrorism Act 2008, Schedule 7

Information on sanctions can be found through:

- HMT Treasury Sanctions Notices, Guidance and News Releases

1.4 The Proceeds of Crime Act sets out the primary offences related to money laundering:

- concealing, disguising, converting, transferring or removing criminal property from the UK
- entering into or becoming involved in an arrangement which facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
- the acquisition, use and/or possession of criminal property.

1.5 The primary money laundering offences apply to everyone and you commit an offence if you know or suspect that the property is criminal property.

1.6 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 trust or company service providers. A regulated business must consider making a suspicious activity report for any part of its business even if it is not trust or company services.

1.7 The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses like those in trust or company service providers must report a belief or suspicion of offences related to terrorist financing, such as:

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

1.8 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 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 process and procedures in place to prevent persons associated with the business from criminally facilitating tax evasion.

1.9 The Regulations set out what relevant businesses such as trust or company service providers must do to prevent the use of their services for money laundering or terrorist financing purposes. This guidance focuses mainly on the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017

1.10 It also gives information on risk indicators within the sector and information in relation to different types of trust or company service providers.

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

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

1.13 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.

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

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

Financial sanctions

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

All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

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

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

1.18 You must report to OFSI as soon as practicable if you know or have reasonable cause to suspect that a designated person has committed an offence. You should report any transactions carried out for persons subject to sanctions or if they try to use your services. You can report a suspected breach, sign up for free email alerts and obtain Information on the current consolidated list of asset freeze targets and persons subject to restrictive measures at:

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

Data Protection

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

Personal data obtained by a business under the Regulations may only be processed for the prevention of money laundering and terrorist financing. You must inform your customers of

this and the information specified in paragraph 2(3) of schedule 1 to the DPA.

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

Trust or Company Service Providers

1.20 Trust or Company Services provider is the term used to describe a firm or sole practitioner carrying out the following activities by way of business in the UK:

- provide formation services for companies or other legal persons
- act, or arrange for another person to act, as a director or secretary of a company
- act, or arrange for another person to act, as a partner (or in a similar position) for other legal persons
- provide a registered office, business address, correspondence address or administrative address for a company, partnership, or other legal person or arrangement
- act, or arrange for another person to act, as a trustee of an express trust or similar legal arrangement
- act, or arrange for another person to act, as a nominee shareholder for another person, unless the other person is a company listed on a regulated market which is subject to acceptable disclosure requirements

Trust or company service providers must comply with the Regulations. They must not carry on business as a trust or company service provider unless they register with HMRC, the FCA, an Accountancy Professional Body or a Legal Professional Body (such as the Law Society) listed in Who needs to register and Schedule 1 of the Regulations.

Penalties

1.21 If a person or business fails to comply with the Regulations, they may face a civil financial penalty or criminal prosecution that could result in an unlimited fine and/or a prison term of up to 2 years. You can find information on the penalties HMRC can issue here.

2. Responsibilities of senior managers

Senior managers

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

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

Minimum requirements

2.3 Senior managers must:

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

Responsibilities

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

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

Actions required

2.6 Senior managers must:

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

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

3. Risk assessment, policies, controls and procedures

Risk-based approach

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

3.2 Services and products provided by trust or company service providers such as complex company structures and the possibility of obscuring beneficial ownership, are attractive to criminals to hide wealth or enable money laundering. Particularly in relation to laundering money through UK and overseas corporate structures.

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

Risks your business may face

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

3.5 The risk profile depends on factors including the nature of your business, how it is structured (e.g. the branch network), the areas it operates in, who your customers are, where they are from and the vulnerability of your services or transactions to exploitation.

3.6 Specific risks in relation to trust or company service providers are covered in risk indicators chapter. For each of these areas you should consider how they could be exposed, for example through the following questions. This generalised list is not exhaustive and will depend on individual business circumstances. (See Chapter 9 on risk indicators for each type of trust or company service providers). 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 is how you identify the risks your business is exposed to. You must be able to understand all the ways that your business could be exposed to money laundering and terrorism financing risks, and design systems to deal with them.

3.8 You must:

- identify and monitor the risks of money laundering and terrorist financing that are relevant to your business - in other words, your business's risk assessment
- take note of information on risk and emerging trends from sources including the National Risk Assessment and HMRCs or your Supervisory Authorities risk assessment in connection with the TCSP sector and amend your procedures as necessary
- assess, and keep under regular review, the risks including those posed by your:
  - customers (see sector guidance on customer due diligence)
  - services
  - financing methods
  - delivery channels, for example face to face, through intermediaries or online
  - geographical areas of operation, including sending money, or transferring funds between companies, to, from or through high risk third countries, for example countries identified by the EU or Financial Action Task Force (FATF) as having deficient systems to prevent money laundering or terrorist financing business

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

The risk assessment must be given to your Supervisory Authority if they ask for it.

In a limited range of circumstances we may tell you that you do not need to keep a record of your risk assessment (if, for example, you are a sole practitioner with no employees, have a small number of well-established clients and where you understand your money laundering and terrorist financing risks). You should check with your Supervisory Authority. Contact HMRC if you are supervised by us and if you think this applies to you.

Specific risks in relation to Trust or Company Service Providers are covered in the Risk Indicators chapter.

Customers and services provided

3.9 Your risk assessment in relation to your customers and the services provided should take account of the full range of circumstances associated with your customers. The following is not an exhaustive list, but you should consider factors including:

- how does the way the customer comes to the business affect the risk for:
  - non face-to-face customers, for example on-line services
  - occasional transactions, as opposed to ongoing business
  - does the pattern of behaviour, or changes to it, pose a risk
  - if you accept customer introductions from an intermediary or third party, have you accepted customers from this source before
- are your customers companies, partnerships, trusts or some combination of these
- do you undertake business in areas with a highly transient population
- do you hold client funds or control their assets, for example in relations to trusts or as part of your services that may be attractive to money launderers
- is your customer base stable or does it have a high turnover
- do you act for international customers or customers you don't meet

- do you accept business from abroad, particularly those based in, or have beneficial owners in, tax havens, or countries with high levels of corruption or where terrorist organisations operate (see: Transparency International corruption perception index)
- do you act for entities that have a complex ownership structure or a cross border element (particularly in relation to cross-border beneficial ownership chains)
- 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 and/or terrorist financing - for example:
    - customers carrying out large one-off cash transactions
    - customers that are not local to the business
    - overseas customers, especially those from a high risk third country identified by the EU or FATF
    - persons subject to UK or EU Financial Sanctions
    - individuals in public positions and/or locations that carry a higher exposure to the possibility of corruption, including politically exposed persons (see guidance on politically exposed persons)
    - customers with a complex business ownership structure with the potential for concealing beneficial owners
    - customers carrying out frequent low value transactions
    - customers sending money to high risk countries
    - large transfers of funds through companies
    - customers with high levels of debt, for example, uncleared County Court Judgements or similar against them.

3.10 Other situations that may present a higher risk and need to be considered in your risk assessment are covered in the enhanced due diligence, sections 4.39 to 4.41, and levels of risk connected with politically exposed persons.

See also suspicious activity reports and Trust or company service providers risk indicators which details some of the specific risks that your business may be subject to.

Policy, controls and procedures

Policy statement

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

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

Controls and procedures

3.12 Senior managers must put in place appropriate controls and procedures to reflect the degree of risk associated with the business and its customers. The policies, controls and procedures that you put in place must be proportionate with regard to the size and nature of your business, and must ultimately be approved by your senior management.

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

Minimum requirements

3.14 You 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 (PEP) or a family member or close associate of a PEP, and do appropriate levels of enhanced due diligence (as described later in this guidance)
- appoint a nominated officer to receive reports of suspicious activity from staff and make suspicious activity reports to the National Crime Agency
- make sure the staff are trained to recognise money laundering and terrorist financing risks and understand what they should do to manage these, including the importance of reporting suspicious activity to the nominated officer
- maintain accurate, up-to-date record keeping and retention of records

Actions required

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

- ensure customer identification and acceptance procedures reflect the risk characteristics of customers
- take further measures for situations such as approving transactions with PEPs (as described later in this guidance)
- 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

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

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

- the appointment of a member of the board of directors (or equivalent body) or senior management who has responsibility for monitoring the effectiveness of and compliance with the policy, controls and procedures, including regular reviews to learn from experience
- individual staff responsibilities under the Regulations
- the process for reviewing and updating the business's policies, controls and procedures
- the process for auditing the business's compliance with its policies, controls and procedures

Making relevant appointments within your business

3.17 Every business must have a nominated officer, no matter what size it is.

Whether you have a compliance officer will depend on the size and nature of your business.

You must inform your Supervisory Authority 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.

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 themselves.

Appointing a nominated officer for the business

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

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

You should make sure that your staff know the name of the nominated officer and any deputy and 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

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

HMRC would not expect you to appoint a compliance officer where you are a sole trader where you carry out regulated activity from one premises, have no more than two or three staff and run an uncomplicated business model or organisation.

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.

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.

3.20 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

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

- carrying out regular audits on compliance with the regulations such as:
  - actively check adherence to the policies, controls and procedures
  - reviewing how effective these are
  - recommending and implementing improvements following such reviews
- ensure compliance throughout the business (including subsidiaries and branches) with anti-money laundering legislation and internal policies/procedures
- oversight of relevant staff (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).

These functions may be carried out from within the business.

3.22 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 a nominated officer.

3.23 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.

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

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

3.24 An officer who is knowingly concerned in a breach of the regulations may be subject to a civil

penalty.

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

3.25 Once you've identified and assessed the risks of money laundering and terrorist financing associated with your business, you must ensure that you put in place appropriate controls and procedures to reduce and manage them. They'll help to decide the level of due diligence to apply to each customer and beneficial owner. It's likely that there will be a standard level of due diligence that will apply to most customers (who will present a relatively low risk of money laundering and terrorist financing), based on your business's risk assessment.

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

3.27 Examples of risk-based controls include:

- introducing a customer identification and verification programme that varies depending on the assessed level of risk
- requiring additional customer identity evidence in higher risk situations
- reviewing low risk customers and applying more due diligence where changes are apparent which alter the risk profile associated with a customer
- varying the level of monitoring of customer transactions and activities depending on the assessed level of risk or activities that might be unusual or suspicious

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

3.28 Identifying a customer or activity as high risk does not automatically mean that they're involved in money laundering or terrorist financing. Similarly, identifying a customer or transaction as low risk does not mean that they're not involved in money laundering or terrorist financing. Your risk assessment of a customer should affect the extent of due diligence measures and scrutiny that you apply to them. Declining a business relationship should be a last resort, when you have concluded that it is not possible to effectively manage the money laundering/terrorist financing risks associated with a particular customer.

Effectiveness of the controls

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

3.30 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

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

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

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

Managing a branch network

3.32 If you manage a branch network you should consider this (non-exhaustive) list of questions to help inform your risk assessment:

- how will you apply risk management procedures to a network of branches
- how will you manage and maintain records, 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's procedures, and given ongoing training on recognising and dealing with suspicious transactions
- if asked, will staff know who the nominated officer is, what the firm's policies are and where they can be found

4. Customer due diligence

4.1 This section sets out and explains the legal definitions and detailed requirements for customer due diligence under the Regulations.

Minimum requirements

You must:

- complete customer due diligence on all customers and beneficial owners before entering into a business relationship or undertaking occasional transaction that requires due diligence
- 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 and when the customer is not physically present when being identified.
- apply customer due diligence when you become aware that the circumstances of an existing customer has changed. This may require you to review the extent of due diligence undertaken, for example, applying enhanced due diligence if the customer now represents a higher risk
- not deal with certain persons or entities if you cannot do customer due diligence 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

Who is the customer

4.2 The customer is the person or entity with whom the business forms, or is intending to form, a contractual relationship. This is, for example, the individual, partnership, trust, company or other legal entity or public body using your services.

A business relationship may be formed before a formal written contract is entered into. In some cases the business and the customer will not have a contract in writing.

4.3 You must check that customer is who they say they are. This is often referred to as 'know your customer', or exercising customer due diligence. 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 of your customers.

4.4 You must do customer due diligence when:

- establishing a business relationship with a customer
- carrying out an occasional transaction with a customer of €15,000 or more
- money laundering or terrorist financing is suspected

- you suspect that information previously obtained for due diligence checks on a customer is not reliable or adequate

4.5 Customer due diligence means:

- identifying all customers and verifying their identity
- identifying all beneficial owners, where applicable, and taking reasonable measures to verify their identity to satisfy yourself that you know who the beneficial owners are
- where the beneficial owner is a specific type of legal person (e.g. certain companies) or legal arrangements (e.g. trusts), taking reasonable measures to understand who controls and owns them
- 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
- retain records of these checks and update them when there are changes

More details on these measures are below.

Timing

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

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's little risk of money laundering or terrorist financing

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 where 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.

To use this exception, a business will have to be able to show, why 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

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

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

You must:

- terminate any existing business relationship with the customer
- consider whether to make 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

4.8 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 trust or company service provider exists where:

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

4.9 For a trust or company service provider the service of forming a company for a customer is not an occasional transaction but must be treated as forming a business relationship. This is the case even if the formation of the company is the only transaction carried out for that customer. This is due to the potential risk involved in facilitating the formation of a complex company structure that may be abused by a customer.

Ongoing monitoring of a business relationship

4.10 You must continue to monitor a business relationship after it is established. This means you must monitor activities and transactions, and where necessary the source of funds, to ensure they are consistent with what you know about the customer and the customer's business and risk assessment.

You must also undertake reviews and keep the information you collect for this purpose up-to-date. The records should be reviewed periodically and expired documents, such as passports and driving licenses, replaced with copies of newly issued documents.

Occasional transaction

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

Forming a company for a client is not to be treated as an occasional transaction.

Beneficial owners

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

Examples of beneficial owners may include:

- client of a principal trust and company service provider for whom you are an intermediary
- a customer of a company for whom you are providing a registered office, business address or correspondence services
- trustee or beneficiary of an express trust

4.13 For a corporate body that is not a company whose securities are listed on EEA regulated market and certain other main markets[1], a beneficial owner is any natural person who:

- owns or controls over 25% of the shares or voting rights
- ultimately owns or controls whether directly or indirectly including bearer shares holdings or other means, more than 25% share or voting rights in the business
- holds the right, directly or indirectly, to appoint or remove a majority of the board of directors
- has the right to exercise, or actually exercises, significant influence or control over the corporate body
- exercises ultimate control over the management
- controls the corporate body

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.

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.

A joint interests 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 pre-determined.

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.

As well as companies incorporated under the Companies Acts, limited liability partnerships

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

industrial & provident societies and some charities (often companies limited by guarantee or incorporated by an Act of Parliament or Royal Charter) are corporate bodies.

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

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

4.15 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 whose main interest the trust is set up or operates
- any individuals who has control over the trust.

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

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

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

4.18 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

4.19 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

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

Extent of customer due diligence

4.21 The extent of customer due diligence measures depends on the degree of risk. It depends on the type of customer, business relationship, product or transaction.

It goes beyond simply carrying out identity checks to understanding who you're dealing with. This is because even people you already know well may become involved in illegal activity at some time, for example where 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 influenced.

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

Simplified due diligence

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

4.23 You will have to risk assess the customer to establish that they are low risk.

4.24 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 identify, and take reasonable measures to verify, 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 taking reasonable measures to verify beneficial owners' 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)
- use at least one authoritative 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.
- 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

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

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

- it is supported by your customer risk assessment
- enhanced due diligence does not apply
- you monitor the business relationship or activities to ensure that there is nothing unusual or suspicious from the outset
- it is not prevented by information on risk provided by HMRC or any other Supervisory Authority in periodically published risk assessments
- the customer is not from a high risk third country identified by the EU, FATF or HMT
- the customer is not a politically exposed person or a family member or known close associate of a politically exposed person
- there are safeguards used in non- face to face services such as electronic signatures to Regulation (EU) N°910/2014 standard
- 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 that legal entity.

4.26 To decide whether a customer is suitable for simplified due diligence you should consider, at least, 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.

4.27 Type of customers that may indicate lower risk:

- a public authority or publicly owned body in the UK
- a financial institution that is itself subject to anti money laundering supervision in the UK or equivalent regulation in another country (assessed in accordance with paragraph 4.28 below)
- a company whose securities are listed on a regulated market
- beneficial owners of pooled accounts held by a notary or independent legal professional, provided information on the identity of the beneficial owners is available upon request
- a European Community institution
- A pension scheme

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

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

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

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

4.30 The Joint Money Laundering Steering Group publishes more information about businesses' obligations and the level of risk in other jurisdictions (Annex 4-I of part I)

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

4.32 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.

4.33 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.

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

4.35 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 and where the source of funds are transparent and where there are no other indicators of higher risk may be suitable, subject to your risk assessment, for simplified due diligence.

Your decisions may be tested, as part of an HMRC compliance visit, on the basis of the evidence that your business holds.

You must not continue with simplified due diligence if you:

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

Enhanced due diligence

Enhanced due diligence applies in situations that are higher risk. This means taking additional measures to examine the background and purpose of the transaction; increasing the degree and nature of monitoring the business relationship; and depending on the nature of the risk taking a range of additional due diligence measures as outlined below.

4.36 You must do this when:

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

4.37 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 EU's 4th Money Laundering Directive may not be subject to enhanced due diligence if your risk assessment finds it is not high risk and enhanced due diligence is not necessary.

4.38 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.

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

- changes to an entity shortly after formation, for example, directors and shareholders
- 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

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

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

4.41 Geographical factors indicating higher risk, including:

- Countries identified by a credible source as:
  - not subject to equivalent anti money laundering or counter terrorist measures
  - with a significant level of corruption, terrorism or supply of illicit drugs
  - subject to sanctions or embargoes issued by EU or UN
  - providing funding or support for terrorism
  - having organisations designated under domestic sanctions legislation or "proscribed" by the UK
  - having terrorist organisations designated by the EU, other countries and international organisations
- has been assessed by organisations such as FATF, FATF-style Regional Bodies, World Bank, Organisation for Economic Co-operation and Development and the International Monetary Fund as not having in place effective anti-money laundering measures.

Additional measures to take

4.42 If enhanced due diligence is appropriate, then you must do more to verify identity and scrutinise the background and nature of the transactions than for standard customer due diligence. How this goes beyond standard due diligence must be made clear in your risk assessment and procedures. For example:

- obtain additional information or evidence to establish the identity from independent sources such as more documentation on identity or address or electronic verification alongside manual checks
- take additional measures to verify the documents supplied such as by checking them against additional independent sources, or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who are competent at document inspection and impostor detection, or a person from a regulated industry or in a position of trust
- 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

Certification

4.43 If the original documents are not produced for verification, or cannot be validated with the issuing source, then any certified document used as part of the customer due diligence measures must have:

- a statement that the document is " Certified to be a true copy of the original seen by me" and where appropriate, "This is a true likeness of the person" from the person who is competent at document inspection and impostor detection, such as a person from a regulated industry or in a position of trust
- an official stamp of the person certifying and indication of professional status
- signed and dated with a printed name
- occupation and address or telephone number.

Politically exposed persons (PEPs)

4.44 Politically exposed persons are persons that are entrusted with prominent public functions, whether in the UK or abroad.

The definition does not include:

- middle ranking or more junior officials
- persons who were not a politically exposed person 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

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.

4.45 Politically exposed persons include:

heads of state, heads of government, ministers and deputy or assistant ministers	
members of parliament or similar legislative bodies	**includes** regional governments in federalised systems and devolved administrations, including the Scottish Executive and Welsh Assembly, where such bodies have some form of executive

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

4.46 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; and
- parents of PEPs.

Brothers and sisters of PEPs should also be treated as "family members". Beyond this definition, firms should take a proportionate and risk-based approach in assessing whether

any given individual is a family member of a PEP – it may, for example, be appropriate to treat a wider circle of family members (such as aunts and uncles) as subject to enhanced due diligence measures in cases where a firm has assessed a PEP to present a higher risk.

4.47 Close associates are persons who have:

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

Levels of risk connected with politically exposed persons

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

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

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

- news agencies and sources
- government and parliament websites
- Electoral Commission: http://search.electoralcommission.org.uk/
- Companies House Persons of Significant Control: https://beta.companieshouse.gov.uk/
- work by reputable pressure groups focussed on corruption risk such as Transparency International and Global Witness.

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

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

4.50 If a customer is a politically exposed person, family member or known close associate of one, then you must put in place the following enhanced due diligence measures:

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

You must, however, assess in each case the level of risk that the politically exposed person presents and apply an appropriate level of enhanced due diligence.

4.51 More frequent and thorough measures should be taken if the politically exposed person is higher risk. Similarly, a reduced level of enhanced due diligence measures can be applied to lower-risk politically exposed persons. A politically exposed person who has a prominent public function in the UK should be treated as lower risk unless other factors in your risk assessment that are not linked to their position as a PEP indicate a higher risk. The same treatment should be applied to family members or close associates of lower risk UK politically exposed persons.

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

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

4.54 The level of risk of a politically exposed person may vary depending on where they are from and the public accountability they are subject to. The following are examples only.

4.55 A lower risk politically exposed person may be one who holds office in a country with traits such as:

- low levels of corruption
- political stability and free and fair elections
- strong state institutions where accountability is normal
- credible anti-money laundering measures
- a free press with a track record for probing official misconduct
- an independent judiciary and a criminal justice system free from political interference
- a track record for investigating political corruption and taking action against wrongdoers
- strong traditions of audit within the public sector
- legal protections for whistle blowers
- well-developed registries for ownership of land, companies and equities

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

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

4.57 A high risk politically exposed person may be from, or connected to, a country viewed as having a higher risk of corruption that may have traits such as:

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

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

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

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

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

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

- wealth derived from the granting of government licences or contracts such as energy, mining or permission for major construction projects

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

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

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

- supervision 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

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

4.63 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 non-binding upon trust and company service providers, but provides detailed guidance as to the approach that you should take to identifying and treating both higher-risk and lower-risk PEPs.

Identifying individuals

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

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.

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

4.65 You should verify these using identity evidence that has been issued by a recognised body, for example a Government department, that has robust identity proofing measures, and includes security features that prevent tampering, counterfeiting and forgery with the customer's full name and photo, with a customer's date of birth or residential address such as:

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

4.66 When verifying the identity of a customer using documents you must take a copy and keep it on file. It may also be appropriate to 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.

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

4.67 Where the customer doesn't have one of the above documents you may wish to 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 the company that issued it, commonly by confirmation of a reference number, name and address, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement

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

- spellings
- validity
- photo likeness
- whether addresses match

4.69 If you verify the customer's identity by documents, you must see the originals and not accept photocopies, unless certified (see Certification) as described below:

- photocopied identity documents can be accepted as evidence provided that each copy document has an original certification by an appropriate person to confirm that it is a true copy and the person is who they say they are
- for standard customer due diligence an appropriate person to certify is, for example, a bank, financial institution, solicitor or notary, independent professional person, a family doctor, chartered accountant, civil servant, or minister of religion – a person who is competent at document inspection and impostor detection.

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

4.70 More information on official documents and how to spot counterfeits and forgeries is published by the Home Office in their 'Basic Guide to Forgery Awareness' and 'Guidance on examining identity documents'.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536918/Guidance_on_examining_identity_documents_v._June_2016.pdf

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.

4.71 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 of 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.

4.72 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

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

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

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

It should be possible to determine whether such alternative documentation is genuine, for example through use of an organisation's stamp.

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

4.75 An electronic records check carried out on limited information establishes only that an individual exists, not that the customer is that individual. For example, 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.

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

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

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

- it is registered with the Information Commissioner's Office to store personal data
- it is accredited to give identity verification services through a government, industry or trade association process that involves meeting minimum standards
- the standards it works to, or accreditation, require its information to be kept up to date
- its compliance with the standards is assessed
- it uses a range of positive information sources, and links a person, through other sources, to both current and previous circumstances
- it uses a range of negative information sources, such as databases relating to identity fraud and deceased persons
- it uses a wide range of alert sources, such as up to date financial sanctions information
- 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.
- it should be able keep records of the information used to verify identity information

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

and the scoring system for pass/fail.

Individuals not resident in the UK

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

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

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

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

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

4.81 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.

4.82 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

4.83 You should establish the names of all directors (or equivalent), and must identify the ultimate beneficial owners (the section on beneficial owners will tell you who they are).You must look through the ownership structure of any companies or trusts to establish the ultimate beneficial owners.

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

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

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.

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

Obligation of customers to provide information

4.86 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 trust and company service provider 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

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

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

4.88 This information will assist in identifying beneficial owners but it will not provide you with all the information you need to verify who the beneficial owner is.

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

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

Beneficial owners

4.89 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.

4.90 Where your customer is a trust or company service provider acting for another individual

who is the beneficial owner, you must identify and take reasonable measures to verify the beneficial owner as well as your customer. You must verify the identity of a beneficial owner taking account of the level of risk associated with your business relationship. You should use any available public records to identify beneficial owners such as company registers, or ask the customer for relevant information. You should also ask for evidence of the beneficial owner's identity, just as you would for a customer, based on documents, data or information obtained from a reliable and independent source or obtain the information in some other way.

You will not have satisfied your obligation to identify, verify and understand the structure of a beneficial ownership if you rely solely on the information contained in a register of People with Significant Control.

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

Reliance on third parties

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

- another UK business subject to the Regulations
- a business in the European Economic Area (EEA) 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

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

4.92 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 customers ends

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

4.94 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.

4.95 Reliance does not include accepting information from others to verify a person's identity for your own customer due diligence obligations, nor electronic verification, which constitutes outsourcing a service. Within outsourcing arrangements, you still remain responsible for any failure to apply due diligence measures appropriately.

4.96 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.

5. Reporting suspicious activity

5.1	**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 to a money laundering or terrorist financing offence (consent) from the NCA before proceeding with a suspicious transaction or entering into arrangements. ● It is a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place.
5.2	**Actions required:** ● enquiries made in respect of internal reports must be recorded ● the reasons why a report was, or was not, submitted should be recorded ● keep a record of any communications to or from the NCA about a suspicious transaction report

Suspicious activity reports ("SARs")

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

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

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

5.6 You can submit a suspicious activity report to the NCA by registering with the NCA SAR online system. 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.

5.7 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.

5.8 For help in submitting a report or with online reporting to the NCA contact the UK Financial Intelligence Unit (UK FIU) helpdesk:

- Defence Against Money Laundering (DAML) Enquiries. All contact with the UKFIU DAML Team is via email: DAML@nca.x.gsi.gov.uk
- Queries regarding SAR Online/general enquiries:
  - Option 1 - Telephone 0207 238 8282
  - Option2 - email – ukfiusars@nca.x.gsi.gov.uk

5.9 Submitting a request for a defence to the NCA, whether you are granted a defence, or not, does not replace the requirement on the business to complete customer due diligence before entering into a business relationship (see Defence SAR below).

5.10 It is important that you have detailed policies, controls and procedures on internal reporting and the role of the nominated officer (see nominated officer below).

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

5.12 A suspicious activity report must be made to the NCA no matter what part of your business the suspicion arises in.

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

Nominated officer

5.14 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.

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

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

5.17 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.

5.18 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.

A defence (consent)

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

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

5.21 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.

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

5.23 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.

5.24 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.

5.25 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.

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

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

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

5.28 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

5.29 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.

5.30 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

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

Suspicious activity

5.31 Here are some warning signs of potentially suspicious activity that your systems should be capable of picking up and flagging for attention. This is not an exhaustive list, and these signs aren't always suspicious. It depends on the circumstances of each case.

New customers

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

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

Regular and existing customers

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

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

Services provided

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

- a third party, apparently unconnected with the customer, bears the costs, or otherwise pays for the service
- an unusually big cash or foreign currency transaction
- the customer won't disclose the source of the funds or reasons for transfers between companies
- 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 or unexpected movement of funds into a company

6. Record keeping

Minimum requirements

You must retain:

- copies of the evidence obtained to satisfy customer due diligence obligations and details of customer transactions for five years after the end of the business relationship
- details of occasional transactions for five years from the date of the transaction
- details of actions taken in respect of internal and external suspicion reports
- details of information considered by the nominated officer in respect of an internal report, where the nominated officer does not make a suspicious activity report
- copies of the evidence obtained if you are relied on by another person to carry out customer due diligence, for five years from the date that the third party's relationship with the customer ends, the agreement should be in writing

You must also maintain:

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

The points below are to be kept under regular review:

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

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

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

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.

Records from branches that have closed should also be retained for the required period.

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.

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

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

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

electronic form. The aim is to ensure that the business meets its obligations and, if requested, can show how it has done so. This evidence may be used in court proceedings.

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

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

7. Staff awareness

7.1 Core obligations

You must:

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

Larger and more complex businesses must:

- screen relevant staff before they take up post and during the course of the appointments assess that they are effective in carrying out their function and are of good character and integrity.

7.2 Actions required

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

- provide appropriate training to make relevant staff aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the business
- ensure that relevant employees have information on, and understand, the responsibilities and legal obligations of the business - individual members of staff, e.g. the functions of the nominated officer and any changes to these positions
- regularly share risk assessment, policy, control and procedures information within the business and with branches and subsidiaries
- consider providing relevant staff with case studies and examples related to the firm's business to illustrate where risks of money laundering and terrorist financing are most likely to arise
- train relevant staff in how to operate a risk based approach to assessing the risks of money laundering and terrorist financing
- provide IT and system security training to staff who have access to it
- where appropriate for larger 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

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

7.4 You must:

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

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

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 and terrorist financing threat that your business may face.

Training

7.5 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) staff in reception, administration and finance functions should be trained, because they'll each have different levels of involvement in compliance, and therefore have different training needs.

7.6 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.

7.7 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.

7.8 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.

7.9 It should cover, in relation to money laundering and terrorist risk, matters including:

- the staff member's duties
- the risks posed to the business
- the business policies and procedures
- how to conduct customer due diligence and check customers' documents
- how to spot and deal with suspicious customers and activity
- document inspection and imposter detection
- how to make internal reports, including disclosures of suspicious activity
- data protection requirements
- record keeping
- the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; Part 7 of the Proceeds of Crime Act; and sections 18 and 21A of the Terrorism Act

7.10 Training may include:

- face-to-face training
- online training sessions
- HMRC webinars or other events organised by your Supervisory Authority
- going to conferences
- taking part in special meetings to discuss the business procedures to safeguard against the risk of money laundering and terrorist financing

- reading relevant publications, whether prepared by HMRC, your Supervisory Authority, industry bodies or internally
- meetings to look at the issues and risks relating to money laundering and terrorist financing

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

7.11 Staff training is necessary when staff join the business, move to a new job or when they change roles. They should also have ongoing training at least every 2 years or when a significant change happens, for example legislation or the business's risk assessment changes.

7.12 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 to evidence your compliance with the Regulations.

7.13 Training records include:

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

8. Trust or company services providers risk indicators

8.1 Trust and corporate entities provide the basis for economic activities in modern economies. They have many genuine uses such as business, finance, family settlements, estate and corporate planning.
They can also be misused by criminals for illegal purposes such as hiding the ultimate beneficial ownership of assets, use of virtual offices, mail forwarding or serviced offices to add a layer of anonymity, legitimating the integration of the proceeds of crime or layering of crime proceeds through various forms of investment such as in the stock market.

Trust or company service providers may not routinely deal directly with a customer's funds, but will be able to focus on the persons they are transacting with and the nature of the services provided. In view of the risks involved, trust or company service providers must be vigilant at all times and report any suspicious activity where necessary.

8.2 The following are some examples of risk indicators in relation to the services provided:

- establishment of multi-jurisdictional and/or complex structure of corporate entities and or trusts without obvious commercial rationale
- the use of multiple companies or trusts which adds a layer of complexity to ownership particularly where those layers seem unnecessary, for example, trusts owning trusts or offshore shell companies
- the fee paid is considerably more or less than you would expect for the level of services provided
- professionals assisting customers to use schemes that can disguise income, assets and ownership
- customers or professionals being evasive or reluctant to provide required CDD information or documentation or where ownership is said to be confidential
- the number of intermediaries or professionals used seems excessive or there seems to be no need for a professional
- excessive or unnecessary use of nominees
- intermediary chains where trust or company service providers act as nominee director for large numbers of limited companies
- intermediary chains where trust or company service providers market themselves and their jurisdictions as facilitating anonymity and disguised asset ownership
- payments (local or foreign) are made or received without a clear connection to the actual activities of the corporate entity
- use of off-shore bank accounts without legitimate economic requirement and where sources and/or destinations of funds are unknown
- establishing a company primarily for the purpose of collecting funds from various sources which are then transferred to local or foreign bank accounts that have no apparent ties with the company
- large movement of funds through a company with no good legal or commercial reason or an absence of any underlying transactions
- The transfer of funds in the form of "loans" to individuals from trusts and non-bank shell companies facilitating a system of regular transfers to these corporate vehicles from the "borrowing" individuals in the form of "loan repayments"
- incorporation of a company by a non-resident with no links or activities in the United Kingdom or the jurisdiction where the company is established

- the parties are native to, resident in, or incorporated in a higher-risk country
- the money flow generated by a company is not in line with its underlying business activities
- shares owned by companies and trusts in off-shore jurisdictions or high risk third countries or countries with high levels of corruption, illicit drug dealing or organised crime
- multiple appearances of the same parties in transactions over a short period of time
- the purchase of companies that have no obvious commercial purpose
- companies which continuously make substantial losses

8.3 The customer or associates may indicate a higher risk depending on their behaviour, transparency or what they request. Examples of risk indicators:

- customer unwilling or refuse to provide information including documentary proof of himself/herself or beneficial owner(s) of trusts or companies
- carry out transactions for themselves or on behalf of the company that does not correspond with their background
- the beneficial ownership is veiled in complexity making it impossible to determine
- client is secretive about the reasons for and way a company structure is being set up
- client favours legal entities that are not transparent or do not require registration of beneficial ownership information
- client wants to use jurisdictions with, for example, weak anti money laundering laws or controls, limited corporate registration requirements, where there is no requirement to update ownership changes, unrestricted bearer share usage, secrecy laws or limited beneficial ownership information requirements
- searches on a customer or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement
- your searches indicate connections to politically exposed persons or their family members
- where the customer is, or appears to be, acting on behalf of another person, an unwillingness to give the names of the persons they represent
- The person acting as a director or representative does not appear to be a suitable representative or does not appear to have the expertise that the role requires
- clients whose owners or directors have a lavish lifestyle that appears to exceed known sources of income
- frequent changes in ownership, officers, beneficiaries or trustees

Service supplier chains

8.4 If you accept business from another trust or company service provider, in an intermediary or service supplier chain, they are your customer. The client of the principal trust or company service provider will be a beneficial owner. Customer due diligence must be done by the intermediary trust or company service provider on:

- the principal trust or company service provider and their beneficial owners
- the end client of the principal trust or company service provider's as a beneficial owner

8.5 If the intermediary trust or company service provider has contact with the end client or takes instruction from or provides services directly to them, the intermediary trust or company service provider may have to carry out customer due diligence measures on the end client as their own customer, rather than as beneficial owners.

The greater the level of contact with the end client, the more likely they are to be deemed to be customers of the intermediary trust or company service provider.
Where a trust or company service provider in the chain is a sole practitioner you should look through this and carry out customer due diligence on the end client.

8.6 The appropriate level of customer due diligence will depend on your risk assessment and the jurisdiction involved, whether they have equivalent anti money laundering measure to the UK. If a high risk third country is involved or the transaction is assessed as high risk, enhanced due diligence will be necessary. It may not be advisable to proceed unless the identity of the end client has been verified based on evidence obtained from them and the additional level of due diligence has been satisfied.

8.7 Subject to the criteria in “Reliance on third parties”, and your risk assessment, an intermediary may be able to rely on the customer due diligence carried out by another trust or company service provider.

9. Where to find more information

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

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

Post: HMRC Anti Money Laundering Supervision
Alexander House
21 Victoria Avenue
Southend on Sea
SS99 1AG

9.2 If they're unable to answer your query directly, they'll be able to pass your query on to the relevant section.

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

9.4 If you are supervised by a professional body you should contact them directly