Anti-Money Laundering Supervision: Estate Agency and Letting Agency Businesses

Contents

1. General Introduction

1.1. 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).

1.2. 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.

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

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

1.5. 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.

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

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

Status of this guidance

1.8. This guidance has been approved by HM Treasury (HMT).

1.9. This guidance replaces HMRC's guidance: “Anti-Money Laundering Supervision: Estate Agency Businesses” published on 20 June 2014, last updated on 1 May 2019, and MLR9a guidance published on 31 January 2014. This guidance is effective from 10 January 2020. Any new requirements are not retrospective. This includes the requirements of Letting Agents as defined within the Regulations.

Meaning of words

1.10. In this guidance, the word 'must' denotes a legal obligation. The main chapters summarise the legal obligations under the heading 'minimum requirements', followed by the actions required to meet the legal obligations.

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

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

1.13. For the purpose of this guidance, the phrase 'client' refers to current or prospective customers of the relevant business such as the vendor, buyer, landlord, tenant and other relevant parties to the transaction, such as a trustee holding a tenancy on behalf of a minor.

Further sources of guidance

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

1.15. JMLSG publishes more information about businesses’ obligations and the level of risk in other jurisdictions (Annex 4-1 of part 1).

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

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

2. Money Laundering and Estate Agency and Letting Agency Businesses

2.1. Money laundering is how criminals change money and other assets into clean money or assets that have no obvious link to their criminal origins. Money laundering can take many forms, but in the property sector it can involve:

- buying a property asset using the proceeds of crime, letting it or selling it on, giving the criminal an apparently legitimate source of funds
- criminals hiding behind complex company structures involving multiple countries and multiple bank accounts to disguise the real purpose of a transaction and hide its beneficial ownership
- a more direct method of paying an Estate Agency business or Lettings Agent a large amount and reclaiming it later
- the money for a purchase resulting from a mortgage fraud operation
- ghost lettings in different forms, such as:
    - where no-one physically occupies the premises when you would reasonably expect there to be an occupier, and rent is paid regularly
    - properties advertised as 'to let' but not available.

2.2. Relevant businesses may not handle client money but will have knowledge of both parties to a transaction, other intermediaries and how a transaction is funded. Some relevant businesses may handle deposits.

2.3. Tax evasion is a criminal offence that can lead to money laundering. For example, the sale price of a property may be set below the Stamp Duty threshold by manipulating the price of furniture and fittings. Tax may also be evaded by hiding behind complex legal structures.

2.4. The proceeds of crime include the proceeds of corruption and super-prime property is an attractive way for individuals to hide this money.

Terrorist financing

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

- fund-raise or are involved in fund-raising, use, or intend to use, or possess money or other property for the purposes of terrorism
- facilitate the retention or control of terrorist property by concealing, transferring or removing it from a jurisdiction
- do not comply with a prohibition imposed by a freezing order or enable any other person to contravene the freezing order

2.6. A person may also commit a Terrorist Finance offence by dealing with funds or economic resources which are owned, held or controlled by a designated person, or making available funds or economic resources to or for the benefit of a designated person (please visit the Office of Financial Sanctions Implementation (OFSI) website).

Legislation

2.7. The primary UK legislation covering anti-money laundering and counter-financing of terrorism includes:

- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended from time to time (referred to in this guidance as "the Regulations")
- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Criminal Finances Act 2017
- Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019, ISIL (Da'esh) and Al-Qaida (United Nations Sanctions) (EU Exit) Regulations 2019 and Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019)
- Sanctions and Anti Money Laundering Act (2018)
- Anti-terrorism, Crime and Security Act 2001
- The Counter Terrorism Act 2008, Schedule 7

2.8. The Regulations set out what relevant businesses such as Estate Agency and Letting Agency businesses must do to prevent their services being used for money laundering or terrorist financing purposes. This guidance focuses on what you must do to meet your obligations in relation to:

- risk assessment, policies, controls and procedures
- customer due diligence
- reporting suspicious activity
- record keeping
- staff awareness and training.

2.9. This guidance also gives information on risk indicators within the sector and information in relation to different types of Estate Agency and Letting Agency businesses.

2.10. The Regulations apply to the following businesses when carried on in the UK:

- Estate Agents, that is businesses carrying on Estate Agency work and explained in section 3 of this guidance
- Letting Agents as defined within the Regulations, see section 3 of this guidance
- credit institutions
- financial institutions

- auditors, insolvency practitioners, external accountants and tax advisers
- independent legal professionals
- trust or company service providers
- high value dealers
- art market participants
- casinos
- crypto asset exchanges
- custodian wallet providers.

2.11. Relevant businesses must comply with the Regulations. They must not carry out Estate Agency or Letting Agency work if they are not registered with HMRC. If you believe the Money Laundering Regulations are not being complied with, you can report it at GOV.UK: https://www.gov.uk/government/organisations/hm-revenue-customs/contact/money-laundering. All details provided remain confidential. If you suspect customers are involved in money laundering or terrorist financing, you should send a Suspicious Activity Report to the National Crime Agency. Our GOV.UK page has more information.

2.12. Information on Financial Sanctions can be found through:

- HM Treasury Sanctions Notices, Guidance and News Releases: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation.
- Further guidance and information across all of the UK sanctions framework: https://www.gov.uk/guidance/uk-sanctions

2.13. 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

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

2.15. Under the Proceeds of Crime Act it is also an offence to fail to report suspicious activity and tipping off any person that you've made such a report. This applies to nominated officers and employees of businesses in the regulated sector, such as Estate Agency and Letting Agency businesses. This obligation extends across the whole business. This means a relevant business which conducts other activities, not covered by the Regulations, anything within the business that is deemed suspicious from a money laundering or terrorist financing perspective, the business should consider a suspicious activity report.

2.16. The Terrorism Act sets out the primary offences relating to terrorist financing. Supervised businesses must report belief or suspicion of offences related to terrorist financing, which can be found at 2.5.

2.17. The Criminal Finances Act 2017 makes important amendments to the Proceeds of Crime Act, the Terrorism Act and the Anti-terrorism Crime and Security Act. It extends the powers of law enforcement to seek further information, recover the proceeds of crime and combat the financing of terrorism. Involvement in money laundering offences may result in unlimited fines and/or a prison terms of up to 14 years.

2.18. It also introduces corporate criminal offences of failing to prevent the facilitation of tax evasion. These offences can result in corporates being found criminally liable for anyone providing services for or on their behalf who criminally facilitates tax evasion. The defence that corporates can raise is that they had procedures in place to prevent persons associated with the business from facilitating tax evasion. HMRC has published guidance to help businesses understand the offences and put processes and procedures in place. This guidance can be found here: https://www.gov.uk/government/publications/corporate-offences-for-failing-to-prevent-criminal-facilitation-of-tax-evasion

2.19. The Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019 provide HMT with the power to designate persons for the purpose of financial sanctions where there are reasonable grounds to suspect that they are, or have been involved in terrorist activity (whether in the UK or abroad). Similar powers are exercised by the FCDO under the Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019 and ISIL (Da'esh) and Al-Qaeda (United Nations Sanctions) (EU Exit) Regulations 2019. Financial sanctions involve the restriction of an individual or entity's access to financial resources, for example through the imposition of an asset-freeze.

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

2.21. The Counter-Terrorism Act 2008, Schedule 7 gives powers to HMT to issue directions to firms in the financial sector in relation to customer due diligence, ongoing monitoring, systematic reporting and limiting or ceasing business.

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

Financial sanctions

2.23. UK financial sanctions apply within the territory of the UK and to all UK persons, wherever they are in the world.

2.24. All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the 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.

2.25. The UK imposes sanctions applied by the UN as well as its own autonomous sanctions regimes

2.26. OFSI publishes a list of all those subject to financial sanctions imposed by the UK. OFSI helps to ensure that these financial sanctions are properly understood through sanction notices, guidance and news releases.

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

2.28. 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

2.29. GOV.UK guidance will make clear which regulations apply to each business whether it is statutory instruments made under The Sanctions and Anti-Money Laundering Act 2018, or retained EU law. As is the case now, we advise stakeholders to check the legislation and guidance that is added to GOV.UK.

Data Protection

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

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

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

- the identity and the contact details of the controller and the controller's representative if they have one
- the contact details of the data protection officer, if you have one
- the reason you're processing the personal data, including the legal basis

- who will receive the personal data
- whether you intend to transfer the personal data outside of the UK, and if so, whether they have a UK data adequacy agreement, or appropriate safeguards
- how long you will store the personal data
- the existence of a right to request access to and deletion of personal data, including data portability
- the right to complain to the Information Commissioners Office
- whether providing the personal data is a statutory or contractual obligation and the possible consequence of failing to provide it
- the existence of any automated decision making, including profiling.

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

Penalties

2.34. If a person or business fails to comply with the Regulations, they may face civil penalties or criminal prosecution. This could result in unlimited fines and/or a prison term of up to two years. You can find information on the penalties HMRC can issue on GOV.UK.

2.35. Not complying with the regulations may lead to money laundering charges under the Proceeds of Crime Act 2002.

3. Estate Agents and Letting Agents

3.1. Anyone who engages in Estate Agency or Letting Agency work must comply with the Regulations. HMRC supervise Estate Agency and Letting Agency businesses under these Regulations. A business must not carry on as a relevant business until they have applied to register with HMRC.

The Regulations define 'Estate Agent' as a firm or sole practitioner, who or whose employees carry out Estate Agency work (within the meaning given by section 1 of the Estate Agents Act 1979). The National Trading Standards Estate and Letting Agency Team confirmed a business qualifies as an Estate Agent under the act if it meets either of the requirements listed in sections 1(1)(a) or 1 (1)(b); it does not have to meet both: https://www.bristol.gov.uk/web/ntselat/what-estate-agency-work-is1

3.2. The MLR definition includes Estate Agents based in the UK who deal with overseas property, either exclusively or alongside other property services. It can also cover Estate Agency businesses based abroad if they are doing business with UK customers.

3.3. The definition of Estate Agency work is very broad and will cover businesses that will not consider themselves to be 'Estate Agents' which is why we refer to 'Estate Agency businesses'. These may include businesses that are construction companies, social housing providers and asset management companies as these may carry out Estate Agency work.

3.4. The Regulations define 'Letting Agent' as a firm or sole practitioner who, or whose employees, carry out Letting Agency work, when carrying out such work. 'Letting Agency work' is work consisting of things done in response to instructions received from a prospective landlord seeking to find another person to let land/property or a prospective tenant seeking to find land/property to rent, and where an agreement is made for the letting of land/property, for a term of at least one calendar month or more. In addition, the rent must be or equivalent to, during at least part of the term, a monthly rent of 10,000 Euros or more, or its equivalent in another currency. This threshold only refers to the rate for the letting each calendar month, not deposits, floats or similar. An agreement is made between the landlord and tenant, implying the tenant will let the property from the landlord for a specified period of time and at a specified price. If the tenancy agreement does not make clear the duration of the agreement, if there is a chance that it could meet the definition above, it would be best practice to conduct customer due diligence as per the requirements.

3.5. Each month, HMRC publishes a monthly average conversion rate for Euros which can be used to calculate the value of lettings in Euros, to identify whether or not Lettings Agents will be in scope of the Regulations. The conversion rate calculations can be found at: https://www.gov.uk/government/collections/exchange-rates-for-customs-and-vat

Estate Agency work

3.6. Under Section 1 of the Estate Agents Act 1979, Estate Agency work includes introducing/negotiating with people who want to acquire or dispose of an interest in land (or their Scottish equivalents) including commercial or agricultural property (whether in the UK or abroad):

- where this is done in the course of a business
- pursuant to instructions from a client

3.7. Subject to satisfying paragraph 3.6, Estate Agency work can include:

- high street or online residential Estate Agency businesses
- commercial Estate Agency businesses
- property or land auctioneers
- land agents
- relocation agents, property finders, private acquisitions specialists
- a sub-agent providing Estate Agency services to a principal Estate Agency business
- asset management businesses that also provide Estate Agency services
- business brokers or transfer agents that broker the sale or transfer of client businesses to third parties
- social housing associations that offer Estate Agency services including the re-sale of shared ownership units
- letting or property management agents that offer Estate Agency services to landlord customers or who undertake the sale of leases for a premium (where the bulk of the rent is paid up front)
- construction companies (house builders) or developers to the extent that they offer Estate Agency services beyond the sale of their own constructed or bought units. For example, land/property may be held by one company in a group and a second within the group carries out Estate Agency work in respect of that land/property.
- in Scotland, a solicitors' property centre.

Letting Agency work

3.8. Under Regulation 13, a letting agent means a firm or sole practitioner who, or whose employees, carries out specified letting agency work (when carrying out such work), where relevant thresholds apply (see paragraph 3.4).

3.9. Subject to satisfying paragraph 3.4, Letting Agency work includes:

- high street or online residential Letting Agency businesses
- commercial Letting Agency businesses
- land agents that also carry out Letting Agency work as defined within the Regulations (see paragraph 3.4 above)

- a sub-agent that does Letting Agency work as defined within the Regulations, to a principle Letting Agency or Estate Agency business
- asset management businesses that also do Letting Agency work as defined within the Regulations
- business brokers or transfer agents that broker a lettings agreement or arrangement such as the tenancy agreement
- social housing associations that do Letting Agency work as defined within the Regulations
- property management agents that also do Letting Agency work as defined within the Regulations
- in Scotland, a solicitors' property centre that also conducts Letting Agency work as defined within the Regulations

Exclusions

3.10. The definition of Estate Agency or Letting Agency does not apply to:

- the publication of advertising or giving out information, for example by newspapers
- an intermediary such as an internet property portal for private sales/lets which merely provide a platform for private clients to advertise their properties and provide a means for vendors and buyers to contact and communicate with one another. However, this exemption applies only if the business does nothing else covered by the general definition of Estate Agency work or Letting Agency work
- work done by solicitors or their employees as part of their work as solicitors. However, if a solicitor has a separate business which provides services of a relevant business, they will fall within the definition and must register with HMRC
- private sales and/or private landlords who do not use a third party to enable the transaction
- for Letting Agency businesses, short lets for a period shorter than one calendar month in total and / or properties for a value equivalent less than 10,000 Euros per calendar month, or its currency equivalent
- those who carry out any surveys or valuations independently of any other Estate Agency work. (Please note, this exemption does not cover surveyors who conduct lease extensions for a capital value)
- property management which is independent of any other Estate or Letting Agency work
- work connected with planning applications and matters covered by the Town and Country planning legislation solely in relation to Estate Agency work
- Estate Agency work carried out entirely outside of, and with no connection to, the UK
- work done in the course of arranging mortgages solely in relation to Estate Agency work.

The Regulations and employees of Estate Agents and Letting Agents

3.11. Employees of Estate Agents or Letting Agents who carry out Estate Agency or relevant Letting Agency work are not themselves individually supervised by HMRC. However, their employers will be responsible for their compliance with the Regulations.

Franchise business models

3.12. Franchise business models can vary in their operation and in terms of how control is exercised. Frequently there are indicators that both the franchisor and franchisee can make decisions that could be viewed as being in control of how their businesses are conducted.

3.13. Where a franchise agreement provides that a franchisee has substantial independence from the franchisor, for example they can make key decisions that affect its ability to operate as a business and choose how it does business and make a profit even within the confines of a franchise agreement, then a franchisee is not an agent and is operating independently on its own behalf. A franchisee in these circumstances must register with HMRC in its own right. The franchisee is responsible for complying with anti-money laundering obligations and other legal and regulatory requirements.

3.14. The same criteria will apply to local representatives of online relevant businesses who are carrying out their activities in the course of business.

3.15. The franchisor, where it is not merely the brand holder, must also ensure that they register if they are carrying out activity identified as a relevant business.

3.16. If the sub-licensees of the franchise are in fact employees of a relevant business, then their activities must be accounted for within the registration of that relevant business. In order to obtain an indication as to whether a sub-licensee is an employee there is a self-determination tool available to the public on GOV.UK. This is normally how people decide their status for themselves. Of course, this is dependent on the inputting of accurate information and may be subject to review by HMRC.

3.17. Should sub-licensees act as agents of the registered relevant business or brand holder then the registered principal can register other premises within its registration from which the sub-licensees work. To be an agent, the principal must have control over the work and activity of the agent when those agents are not its employees. The registered principal is then taking responsibility for the activity of the agent and, in consequence, the compliance of the agent and any breaches of the Regulations by the agent will attract a penalty or prosecution of the registered principal.

4. Responsibilities of senior managers

Senior managers

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

4.2. A senior manager is an officer or employee who has sufficient knowledge and the authority to make decisions that affect your business's exposure to money laundering and terrorist financing risk. Examples include a director, manager, branch 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

4.3. 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 high risks
- Appoint a nominated officer to report suspicious activity to the NCA
- Devote enough resources to address the risk of money laundering and terrorist financing.

Responsibilities

4.4. 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. Senior managers must approve the policies, controls, and procedures.

4.5. 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 subsidiaries and branches.

Actions required

4.6. Senior managers must:

- carry out a written risk assessment identifying how and where your business is vulnerable to money laundering and terrorist financing
- take a risk-based approach to mitigating and managing the residual risks which will focus more effort on higher risks
- 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 the risk assessments
- review and update the policies, controls and procedures to reflect changes to the risks faced by the business
- make sure those conducting relevant activity are appropriately trained and equipped to implement policies adequately, including systems in place to support them
- make sure that the policies, controls and procedures are communicated to and applied to subsidiaries or branches in or outside the UK
- monitor effectiveness of the business's policy, controls and procedures and make improvements where required
- have systems to identify when you are transacting with persons from or based in high risk third countries identified by the FATF or high risk third countries identified by HMT or financial sanctions targets advised by OFSI and take additional measures to manage and lessen the risk
- approve the establishment, or continuation, of a business relationship with a politically exposed person or a family member or known close associate of a politically exposed person
- devote enough resources to deal with money laundering and terrorist financing.

4.7. The risk assessment and policies, controls and procedures must be reviewed in response to changes to your business, the market, and information from HMRC or changes to the legislation at least on an annual basis.

5. Risk assessment and policies, controls and procedures

Risk based approach

5.1. A risk-based approach is where you assess the risks that your business could be used for money laundering or terrorist financing and put in place appropriate measures to mitigate those risks. A risk-based approach should balance the costs to your business and customers with a realistic assessment of the risk that criminals may exploit the business for money laundering and terrorist financing. It allows you to focus your efforts on the areas of highest risk areas and reduce unnecessary burdens.

Risks your business may face

5.2. Assessing your business's risk profile will help you understand the risks to your business and how they may change over time, or in response to the steps you take. This will help you design the right systems that will spot suspicious activity and ensure that staff are aware of what sort of money laundering activities they are likely to encounter. The risk assessment depends on the nature of the business, how it is organised, customers and activities. For each of these areas you should consider how they could be exposed.

5.3. Further information regarding risks can be found later in section 10 of this guidance.

Risk Assessment

5.4. All businesses must develop a business risk assessment. Your business 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.

5.5. The business risk assessment will be overarching for the entirety of the business and is required to develop the business' policies, controls and procedures. The business risk assessment will act as a guide for developing the separate customer risk assessments and guide businesses in considering what level of customer due diligence is required for their customers.

5.6. You must:

- assess, and keep under regular review, the risks including those posed by your:
    - customers and counterparties and any underlying beneficial owners (see guidance on customer due diligence on who is a beneficial owner)

    - geographical areas of operation, including receiving money from, to, or through high risk third countries, for example countries identified by the UK or FATF as having deficient systems to prevent money laundering or terrorist financing
    - type of products and services provided by your business
    - the transaction itself
    - your customers
    - delivery channels of the business, for example non face to face services
    - for politically exposed person, their financing methods
- take note of information on risk and emerging trends from sources including the National Risk Assessment and HMRCs risk assessment and amend your procedures as necessary.

5.7. Your risk assessment must be in writing (this can be in a digital format) and subject to regular review. It needs to reflect changes in your business and the environment that you do business in. At least an annual review of the risk assessment is recommended and any revisions must be noted in the document.

5.8. The risk assessment must be given to HMRC when we ask for it. When providing this information, the business needs to be able to provide what information the risk assessment is based upon.

5.9. In a limited range of circumstances, we may tell you that you do not need to keep a record of your risk assessment (if, for example, you are a sole practitioner with no employees, have a small number of well-established clients and where you understand your money laundering and terrorist financing risks). We will expect you to be compliant with the requirements of the Regulations in all other respects. You should contact HMRC if you think this applies to you.

5.10. Your risk assessment, in relation to customers and services provided, must take account of the full range of circumstances associated with a client based on information you have or behaviours indicating higher risk. The following is not an exhaustive list, but you should consider factors including:

- the way the client comes to the business affects the risk for:
    - non face-to-face customers
    - does the pattern of behaviour, or changes to it, pose a risk?
    - if you accept instructions from another agent, sub agent or third party, what is your knowledge and understanding of that agent's client base? If appropriate are they registered with HMRC?
    - buyers who may be carrying out large one-off cash transactions
    - clients that are not local to the area and where another business, local to them, would be better placed to meet their needs
    - overseas clients especially from a high risk third country identified by the FATF or a high risk third country identified by the UK
    - individuals in public positions and/or locations that carry a higher exposure to the possibility of corruption, including politically exposed persons (see sector guidance on politically exposed persons)

- is the client a company, partnership, or trust; are there complex or opaque business ownership structures in place? That is, any client which is a legal person, owned by another legal person. For example, a limited company owned by a beneficial owner indirectly, through another legal entity
- do you act for international clients or persons you have not met?
- do you accept business from abroad, particularly those based in, or have beneficial owners in, tax havens, or countries with high levels of corruption (Transparency International corruption perception index) or where terrorist organisations operate?
- do you accept cash payments, for example, at auction or as monthly rent?
- do you accept payments that are made to or received from third parties or from overseas accounts?

5.11. Risk assessments in relation to delivery channels, transactions and countries are also key factors that should be considered when developing your business risk assessment. Similarly to the customers, as highlighted above, you should take into account the full range of circumstances associated with countries, delivery channels and transactions.

5.12. For further information relating to risk assessments, you can read the UK National Risk Assessment, the EU Supra-National Risk Assessment and FATF risk based approach guidance for estate agents.

5.13. Other situations that may present a higher risk and need to be considered in your risk assessment are covered in the enhanced due diligence, and risk information when dealing with politically exposed persons.

5.14. See also suspicious activity reports and Estate Agency and Letting Agency Business risk which details some of the specific risks that your business may be subject to.

Policies, controls and procedures

Policy statement

5.15. Your policy statement, being proportionate to the size and nature of the business, 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 will 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. It must make clear who has responsibility for maintaining, managing and monitoring the policies, controls and procedures.

5.16. Policies, controls and procedures must be in writing (which can be a digital format) and be communicated throughout your organisation to staff, branches and subsidiaries in and outside the UK. These policies, controls and procedures must be regularly reviewed and updated. All changes made must be recorded and kept as per the record keeping requirement of the Regulations. In addition, these must be approved by senior management.

Controls and procedures

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

5.18. You must take into account situations that, by their nature, can present a higher risk of money laundering or terrorist financing and take enhanced measures to address them. The specific measures depend on the type of customer, identity of the customer, business relationship, jurisdiction, product or transaction, especially large or complex transactions or unusual patterns of activity that have no apparent economic or lawful purpose. Conversely, the measures that you put in place to manage risks associated with lower-risk customers should be less onerous. The risk assessment that you conduct must underpin the nature of your measures for mitigating and managing money laundering and terrorist financing risks.

5.19. 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 or a family member or close associate of a politically exposed person, and do appropriate levels of enhanced due diligence (as described later in this guidance)
- appoint a nominated officer to receive reports of suspicious activity from staff and make suspicious activity reports to the NCA. The nominated officer can delegate responsibilities but must do so clearly and in writing
- make sure the staff and any agents a business uses for the purpose of its business 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
- ensure staff are aware of the anti-money laundering policies and procedures you have put in place
- ensure that policies, controls and procedures are followed
- maintain accurate, up-to-date retention and keeping of records.

5.20. The following actions are also required to be covered within your policies, controls and procedures and must be kept under regular review:

- ensure identification and acceptance procedures reflect the risk characteristics of all clients
- take further measures for higher risk situations such as approving transactions at senior management level with politically exposed persons
- ensure low risk situations are assessed and records retained to justify your assessment and that these are in line with the business's overall risk assessment
- ensure arrangements for monitoring systems and controls are robust and reflect the risk characteristics of clients to the business

- carry out regular assessments of your systems and internal controls to make sure they are working and meet the requirements of the Regulations
- ensure staff and agent training is appropriate to the individual employee and kept up to date and content regularly reviewed
- ensure staff know the names of the nominated officer and any deputy
- ensure policies are in place for sharing information with entities within the same corporate structure/group about customers, customer accounts and transactions
- when the business adopts new products, business practices or technology, these must be immediately incorporated into the business' policies, controls and procedures.

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

5.22. The policy of a larger, more complex business must include:

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

5.23. 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.

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

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

Appointing a nominated officer for the business

5.26. 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 NCA. You should also appoint a deputy to act in the absence of the nominated officer. If you are a sole trader, with no employees, you will be the nominated officer by default, and must report suspicious activity to the NCA.

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

5.28. 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).

Appointing a compliance officer for larger, more complex businesses

5.29. You must 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/branch network, geographical area you operate in, type of customers, and the complexity of the business.

5.30. Businesses with, for example, more premises, who 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 monitored and are consistent throughout the organisation.

5.31. 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.

5.32. Where a compliance officer is needed, the business must appoint a person from the board of directors, its equivalent or senior management.

5.33. 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. In addition, it may not be practical to appoint a separate compliance officer so this person may also act as a nominated officer.

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

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

5.36. Relevant staff are persons involved in the identification of risk, carry out controls or procedures to reduce risk or are otherwise involved in your compliance, such as customer due diligence checks, with the Regulations including the receiving of documents from clients.

5.37. Screening means an assessment of the skills, knowledge and expertise of these staff to carry out their functions effectively and the conduct and integrity of the individual.

5.38. 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.

5.39. Given the importance of this role, businesses may need to appoint a deputy compliance officer.

5.40. The compliance officer and nominated officers should 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

5.41. You are an ‘officer’ if you are:

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

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

5.43. 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

5.44. Once you have identified and assessed the risks and warning signs, you must ensure that you put in place appropriate controls and procedures to reduce or deal with them. They will help to decide the level of customer due diligence to apply to each client, beneficial owner and other relevant individuals. This is explained further below. It is likely that there will be a standard level of due diligence that will apply to most clients (who will present a low risk of money laundering and terrorist financing), based on your business's risk assessment.

5.45. Procedures should be easily accessible to staff and detailed enough to allow staff to understand and follow them easily. They must include as a minimum:

- the types of clients and transactions that you consider to be lower risk and why they may qualify for simplified due diligence and those that are higher risk and merit closer scrutiny
- how to carry out customer due diligence and enhanced due diligence on higher risk clients and different types of legal entity
- how to carry our customer due diligence in the case of more unusual transactions. For example, where you are contacted in respect of a sale by a person with a power of attorney or an executor of a will
- how to identify politically exposed persons and what to do when one is identified, in particular how to identify their source of wealth and source of funds
- what to do if you are dealing with an individual subject to the sanctions regime or who is based in a jurisdiction of concern
- any other patterns or activities that may signal that money laundering or terrorist financing is a real risk and what to do if these are identified
- how to keep records and where and for how long they should be kept
- how and when to conduct ongoing monitoring of transactions and customers
- clear staff responsibilities and the name and role of the nominated officer and when reference must be made to these individuals
- how to report suspicious activity to the nominated officer and how the nominated officer should make a report to the NCA
- how and when staff are trained and how that training is recorded

- how to audit and monitor the policies and procedures and the internal controls in place to ensure that the policies and procedures are followed correctly by staff.

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

Effectiveness of the controls

5.47. Managing the money laundering and terrorist financing risks to your business is an ongoing process, not a one-off exercise. You must document the risk assessment and policies, controls and procedures, 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.

5.48. Compliance audits must be documented indicating the branch visited, files reviewed, staff spoken to and whether the check was satisfactory or not. If it is not satisfactory then the required remedial action taken must be recorded.

Managing group subsidiaries

5.49. 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. The subsidiary or branch outside of the UK is within UK scope if they are engaging in activity as stated within the Estate Agents Act or within the Regulations. For Letting Agency businesses for properties within the UK, this is explained further within section 3 above. 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 subsidiaries or branches in third countries are complying with the money laundering and terrorist financing requirements of that country

- ensuring that subsidiaries or branches in a third country are applying anti-money laundering and 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 HMRC.

6. Customer due diligence

Minimum requirements

6.1. You must:

- complete customer due diligence on all clients, and all other relevant parties before entering into a business relationship or occasional transaction, see paragraph 6.9.
- take reasonable measures to verify the identity of beneficial owners of clients and, if the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement, take reasonable measures to understand the ownership and control structure of it.
- 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, for example someone acting on behalf of a company or trust
- apply enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, including politically exposed persons
- identify politically exposed persons, their family members and close associates and verify their identity, source of wealth and/or funds. You must also have a procedure in place so that a senior manager can consider whether to do business with that person
- apply customer due diligence, when you become aware that the circumstances of an existing customer, relevant to their risk assessment, has changed
- not deal with certain persons or entities if you cannot carry out 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.

6.2. Estate Agency businesses do not commonly handle the funds used to buy a property. However, they are a key facilitator in a property sale and come into contact with both parties to the transaction at an early stage and are in an ideal position to identify suspicious activity.

6.3. Letting Agency businesses are more likely than Estate Agency businesses to handle funds, as in the payments from clients either as physical cash or cleared funds. This, in itself, increases the risk that agents may unwittingly and directly facilitate money laundering and terrorist financing. For example, the Lettings Agency business may be used to ‘clean’ money when a ‘tenant’ requests that a holding deposit be returned as they are not following through with a tenancy agreement. Further information on risks in the sector can be found in the National Risk Assessment.

The customer

6.4. The customer is the person or entity with whom the relevant business forms a business relationship, which is also usually a contractual relationship often referred to as the client. This can be a vendor or landlord (that is the owner or owners of the property or other interest in land) or the person, or persons, who buys or lets the property.

6.5. For Estate Agents, it is usually the vendor although in the case of repossessions it may be a lender. Under the regulations Estate Agents must also treat the purchaser as a customer for the purposes of CDD at the point when the purchaser's offer is accepted by the seller.

6.6. For Letting Agents, it is usually the landlord and the tenant (although, again, both must be treated as a customer for the purposes of CDD). Letting Agents should consider whether a guarantor may also be their customer. In addition, for lettings, the business will potentially have other customers in the form of trustees of a letting arrangement. A property finder will normally act for a buyer to find a property. An auctioneer may act for vendors and buyers.

6.7. The Regulations state that a relevant business enters into a business relationship when contact is established with a client and is expected to have an element of duration.

6.8. For an Estate Agency business, they will enter into a business relationship with a purchaser at the point at which an offer is accepted, having already entered into a relationship with the seller, usually at the point of marketing the property.

6.9. For a Letting Agency business, they will enter into a business relationship with a tenant or trustees of a letting arrangement at the point at which the tenant's offer is accepted, where the tenancy is for at least a month, and for rent of (for at least part of the term) equivalent to 10,000 euros or more a month, before the tenancy agreement is confirmed. Due diligence upon the landlord/tenant/trustee must be completed before the agreement is made.

6.10. Section 6.21 onwards defines what the guidance perceives as offer acceptance. The person who is not a customer in the commercial sense (the counterparty), must be treated in the same way as a customer for the purposes of the Regulations, for example, the same obligations to apply an appropriate level of customer due diligence.

When to undertake customer due diligence

6.11. You must carry out customer due diligence on your customer and the counterparty to the transaction. The level of due diligence will depend on your risk assessment of each person in line with your overall risk assessment.

6.12. If you are acting as the Estate or Letting Agent, you must verify that all parties to the property sale or tenancy agreement are who they say they are. This is often referred to as 'know your customer' or exercising customer due diligence. You must carry out customer due diligence on all customers even if you knew them before they became your customers. This is because you must be able to demonstrate that you know all your customers.

6.13. If, to verify the identification of your customer, you are accepting notarised copies of documents, you should satisfy yourself that the notary is who they say they are and are allowed to notarise the relevant documents.

6.14. You must undertake customer due diligence when:

- establishing a business relationship with a client
- carrying out an occasional transaction over the value of 15 000 euros with a client as an Estate Agency business
- As a letting agent, prior to the conclusion of a contract to let land for a term of a month or more and at a rent which during at least part of the term is equivalent to a monthly rent of 10,000 euros or more.
- money laundering or terrorist financing is suspected
- you suspect that information obtained for due diligence checks on a client is not reliable or adequate
- conducting ongoing monitoring, particularly for letting agreements.

6.15. Customer due diligence requires:

- identifying all vendors and all buyers, landlords, tenants, trustees of a letting arrangement or other parties involved and verifying their identity (more details below)
- identifying all beneficial owners of the customer and taking reasonable measures to verify their identity to satisfy yourself that you know who they are
- obtaining information on the purpose and intended nature of the business relationship, although in most cases this will be self-evident for Estate Agency and Letting Agency businesses
- conducting ongoing monitoring of the business relationship to ensure transactions are consistent with what the business knows about the client, and the risk profile
- retaining records of these checks and updating them when you become aware of changes
- understanding the ownership and control structure of a customer when the customer is one of the following:
    - legal person
    - trust
    - company
    - foundation
    - or other.

Business relationship with a customer

6.16. A business relationship is formed with a business' direct customer when, on establishing contact, the business expects the relationship with the customer to have an element of duration. A business relationship is formed no later than when a contractual relationship is formed and may be formed before that. In some cases, the relevant business and the customer will not have a contract in writing. In most cases a property sale or a tenancy agreement involves an element of duration so will be a business relationship rather than an occasional transaction.

Timing in relation to a customer

6.17. The customers' identity and where applicable the identity of beneficial owners, must be verified before entering into a business relationship or an occasional transaction. For Letting Agents, this relates to all new clients from 10 January 2020 and includes any agreements that are renewed, but not where a tenancy automatically becomes periodic.

6.18. You can make an exception to when customer due diligence is carried out on any party to a sale only if both the following apply:

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

6.19. 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 only during the course of setting up the business relationship and so it must be completed by the time that the relationship is established, which is not later than when there are contractual liabilities. Nor does this exception mean that you can use it where it is hard to verify a customer's or beneficial owner's identity.

6.20. It's important to note, it is not expected that this exception will be used very often and to use this exception, a business will need to explain in its risk assessment why it considers certain types of business relationship or transaction has little risk of money laundering or terrorist financing.

Business relationship with the counterparty

6.21. In the case of an Estate Agent, a business relationship is entered into with a buyer, who is not the customer, when the buyer's offer is accepted by the vendor. The Estate Agent at this point is enabling the transaction to go ahead and therefore needs to satisfy the Regulations that they have identified and verified all parties relevant to the transaction.

6.22. In the case of a relocation agent, property finder or investment broker, a business relationship is also formed with the vendor, no later than at the point the buyer's offer is accepted. In this scenario, the customers of the relocation agent, property finder or investment broker are the buyer and also the Estate Agent and will be required to conduct due diligence on that Estate Agent. In this case, the buying agent may well be able to rely on the customer due diligence carried out by an Estate Agent (and vice versa) with their consent, rather than carrying out due diligence checks themselves - see Reliance on third parties.

6.23. Prospective buyers are not included in a business relationship unless they are a customer, for example an auctioneer may charge a fee to a bidder for participating in an auction. The bidder is a customer of the auctioneer.

6.24. Regarding auctioneers, a business relationship is entered into with the buyer on the binding of the contract when the gavel has fallen. Customer due diligence must be carried out before a binding contract is entered into. This may be achieved by either:

- pre-registering bidders so that customer due diligence is carried out before the hammer falls
- creating a condition precedent (that customer due diligence is undertaken) so that the contract is not binding until customer due diligence is completed.

The bidders should be pre-warned to bring sufficient evidence to enable an appropriate level of customer due diligence to be carried out.

6.25. Regarding buying agents, a business relationship is entered into when the buyer instructs the agent. Therefore, customer due diligence must be completed before this point.

6.26. A Letting Agency business will enter into a business relationship with a tenant or other relevant party at the point at which the tenant's offer is accepted. This must be before the tenancy agreement is confirmed.

Timing in relation to the counterparty

6.27. For an Estate Agent, the formal acceptance of an offer is considered to take place at exchange of contracts. Therefore, where the customer due diligence obligation on the buyer arises, this must take place and be completed before a binding contract is entered into. This is normally when:

- contracts are exchanged
- a binding contract is entered into
- a sealed bid is opened, if a binding contract is entered into.

6.28. If these events do not create a binding contract, customer due diligence must still be completed before the point at which the sale becomes irrevocable.

6.29. In order to ensure customer due diligence is completed on time you may consider that a helpful trigger point to begin the process of customer due diligence would be around the time when the terms are agreed, normally on the signing of a Memorandum of Sale by all parties involved in residential sales or Heads of Term in commercial sales, again by all parties involved.

6.30. For Letting Agent businesses, this must be before the signing of the tenancy agreement. In practice this means that customer due diligence should be carried out as early as possible on the counterparty. Relevant businesses should advise a serious prospect that customer due diligence will have to be carried out at the time of acceptance of the offer or before, so that they have evidence to hand, to prove identity.

6.31. For the purposes of defining a business relationship for vendors and landlords in particular, where a condition precedent exists, the business relationship is entered into only when the condition is fulfilled and customer due diligence has taken place.

6.32. For Letting Agent businesses where the value of the let is just below the threshold but the let would fall into scope otherwise, it is important to consider whether there is a realistic likelihood of the let value rising above the threshold during the lifetime of the contract. If so, customer due diligence must be completed before the signing of the tenancy agreement and before the business accepts any money (see paragraph 6.25). For example, a let for seven years with a value of £8,000 per month, increasing 10% per year would fall into scope before the contract ends. It would, therefore, be necessary to complete customer due diligence at the start of the contract.

6.33. If any person is not prepared to prove who they are you must terminate the business relationship and consider completing a suspicious activity report.

6.34. If, prior to the timings given above, the counterparty has agreed terms with a conveyancer, for a relevant business to act for them, you may be able to rely on the customer due diligence that the third party has carried out if they are prepared to agree to be relied on (see Reliance on third parties).

Situations where you do not need to carry out customer due diligence on the counterparty

6.35. You do not need to carry out customer due diligence on persons when:

- you respond to, for example, marketing campaigns by requesting further information on property such as location, details of the property as these may not result in any further contact or interest and are at a stage much earlier than the point at which an offer is accepted
- a potential buyer/tenant makes an offer after your contractual relationship with your client has come to an end and you are therefore no longer in a business relationship with the vendor/landlord.

Situations where a relevant business may not be able to comply with the duty to do customer due diligence before exchange

6.36. In most cases, you will be aware of who the buyer or tenant is. In some circumstances, a relevant business will genuinely not be aware of an offer from a buyer or tenant, will not be aware of the identity of the buyer or tenant, or will become aware of the buyer or tenant at a late stage. In those circumstances, the following action that needs to be undertaken is explained below.

Estate Agency or Letting Agency business is unaware of sale or tenancy

6.37. This may occur, for example, where a vendor or landlord finds the buyer or tenant themselves or via another agency, and excludes the original relevant business.

6.38. In such situations, a business who is not aware of an offer being made can be considered to have taken all reasonable steps to avoid contravening the requirement to carry out customer due diligence on the buyer or tenant. To ensure the business has taken all reasonable steps, the business must have included, in their contract with the vendor or landlord (and where appropriate, a contract between a principal and sub-agents), terms that provide that the information on the buyer(s) – and any changes in those details - will be given to the business in sufficient time and prior to exchange/completion of the tenancy agreement. This will be regarded as the business having carried out appropriate customer due diligence.

6.39. For example, in a joint sole agency relationship, the business who did not identify the buyer/tenant (agent 1) requests due diligence from the agent who did identify the buyer/tenant (agent 2) but, agent 1 does not provide agent 2 with the due diligence. It would be best practice for agent 1 to document that they have requested this information but it has not been provided. Within a joint sole agency relationship, both agents would be expected to conduct simplified due diligence upon each other (assuming they are both supervised under the Regulations).

Estate Agency or Letting Agency business is unaware of final buyer or tenant

6.40. The buyer or tenant may change at a late stage, without the knowledge of the relevant business (so the business has carried out customer due diligence on the wrong buyer or tenant).

6.41. An agent who is genuinely not aware of a late change of buyer or tenant will be considered to have taken all reasonable steps and exercised all due diligence to avoid contravening the requirement to carry out customer due diligence on the buyer/tenant, if that agent has taken reasonable steps to stay informed of changes. This should include provision in their contract with the vendor/landlord to provide the details of the prospective buyer/tenant – and any changes in those details – in sufficient time and prior to exchange to allow the business to carry out appropriate customer due diligence.

Estate Agency or Letting Agency business becomes aware of a buyer or tenant close to exchange or agreement

6.42. This may occur, for example, where a relevant business, other than the agent who introduced the buyer or tenant or forwarded the buyer or tenant's offer, becomes aware of a buyer or tenant close to exchange or agreement with insufficient time to complete customer due diligence. Another example can be within a joint sole agency; the agent who does not find the buyer.

6.43. An agent who became aware of such a buyer or tenant and was (at the point of exchange or agreement) genuinely making conscientious and appropriate efforts to complete customer due diligence, will be considered to have taken all reasonable steps and exercised all due diligence to avoid contravening the requirement to carry out customer due diligence on the buyer. In the joint sole agency example, please refer to 6.37.

6.44. HMRC considers that relevant businesses who forwarded the buyers or tenant's offer or who introduced the buyer or tenant will have had time and opportunity to complete customer due diligence on the buyer/tenant before exchange of contracts or agreement made and is less likely to be able to demonstrate that they had insufficient time or opportunity to complete customer due diligence.

Failing to carry out customer due diligence when an Estate Agency or Letting Agency business is aware of the sale and aware of the buyer or the tenancy and the tenant

6.45. In any other case the relevant business is required to undertake customer due diligence. If they are unable to obtain sufficient information to do customer due diligence, they must terminate their relationship with the client and consider submitting a suspicious activity report. In obtaining sufficient information, the business must ensure they are complying with the Regulations, as well as their own risk assessment and policies, controls and procedures.

6.46. Where suspicion of money laundering or terrorist financing arises, you must consider reporting the circumstances to the NCA.

6.47. most cases a property sale or a tenancy agreement involves an element of duration so will be a business relationship rather than an occasional transaction.

Extent of customer due diligence

6.48. The extent of customer due diligence measures depends on the degree of risk. It depends on the type of client in the business relationship, product or services provided, and any geographical risk which will be covered within your business risk assessment. It goes beyond simply carrying out identity checks to understand who you are dealing with. The business must risk assess the customer to understand the level of due diligence required. To truly be able to risk assess customers, the business must know who they are entering into a business relationship with. It is important that changes in the client's business circumstances are monitored so the relevant business can ensure their client remains consistent within the stipulated risk assessment for their business model. For example, where their personal circumstances change, or they face some new financial pressure. Your customer due diligence measures and knowing your customer should reduce the risk of this and the opportunities for staff to be influenced.

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

Non-compliance with customer due diligence

6.50. If you cannot comply with the customer due diligence measures, you must not:

- carry on relevant business activity with, or for, the client, including but not limited to the vendor, buyer, landlord or tenant
- establish a business relationship or carry out an occasional transaction with the client.

Instead, you must:

- terminate any existing business relationship with the client
- consider whether to make a suspicious activity report.

Ongoing monitoring of a business relationship

6.51. You must continue to monitor a business relationship after it is established and for its duration. This means you must monitor transactions on a risk-based approach, and where necessary the source of funds, to ensure they are consistent with what you know about the client or other relevant parties and their risk assessment. As part of your ongoing monitoring, you may need to contact an existing client to review any information and customer due diligence must be conducted at this point. An example may be when renewing a tenancy agreement. Examples of other things you must review include:

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

6.52. For an ongoing business relationship, you must also keep the information you collect up-to-date in line with your risk assessment. It should be checked periodically and reviewed where you become aware of a change, for example, a change to a legal entity.

Occasional transactions

6.53. For the purpose of the Regulations, an occasional transaction means a transaction which is not carried out as part of a business relationship. This could be for example, selling of small plots or a purchase of property/land at auction which is 15,000 Euros or more (or the sterling equivalent). The value of the transaction here means the gross value of the land/property transaction, not the value of your fees.

6.54. Estate Agents must apply customer due diligence measures if they carry out an occasional transaction that amounts to 15,000 euros or more, whether the transaction is executed in a single operation or in several operations which appear to be linked. This does not, however, apply to letting agents.

Beneficial owners

6.55. Beneficial ownership refers to the person or persons who ultimately own or control an asset (for example, a property or a company) and benefit from it. For an entity, such as a company or trust, the beneficial owners are individuals who ultimately own or control the entity, or on whose behalf a transaction or activity takes place. More details are given below.

6.56. Examples of beneficial owners include:

- the client of a principal agent (the agent with a direct relationship with the customer) for whom you are a sub-agent

- a purchaser customer of a company for whom you are providing property finding services
- any co-owners of a property who are not your customer whatever the share held.

6.57. For a corporate body, that is not a company whose securities are listed on EEA regulated markets and certain other regulated markets, for example, in USA, Japan, Switzerland and Israel, a beneficial owner is any individual who:

- owns or controls more than 25% of the shares or voting rights
- ultimately owns or controls, whether directly or indirectly including bearer shares, holdings or other means, more than a 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.

6.58. 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 beneficial owner of the legal entity.

6.59. If an individual has significant control over a company but is not a shareholder or a director of the company, it is good practice to obtain evidence of this, as part of the customer due diligence.

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

6.61. 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.

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

6.63. For a partnership that is a body corporate (other than a limited liability 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 (see section 2 in Scottish qualifying partnerships guidance)
- exercises ultimate control over the management.

6.64. For a trust, a beneficial owner includes:

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

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

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

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

6.67. 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.

6.68. 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.

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

6.70. In a sub-agency arrangement, the beneficial owner is the vendor customer or, for relocation sub agents, the purchaser customer of the principal agent. Customer due diligence must be carried out accordingly.

6.71. If the sub-agent has contact with the principal agent's customer, the sub-agent may have to carry out customer due diligence measures on the vendors or purchasers as customers of the sub-agent, rather than as beneficial owners. The greater the level of contact with the vendor or purchaser, the more likely they are to be deemed to be customers of the sub-agent. For example, the sub-agent marketing the customer's property on behalf of the principal agent would mean that the sub-agent must complete due diligence upon the vendor.

6.72. Subject to the criteria in Reliance on third parties, sub-agents may be able to rely on the customer due diligence carried out by a principal agent.

6.73. Where the customer is a legal person, trust, company, foundation or similar legal arrangement the relevant person must take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement. If the business has exhausted all possible means of identifying the beneficial owner, it will be deemed acceptable if the business is able to take reasonable measures to verify the identity of the senior person within the business (customer) responsible for management. The business should keep records in writing of actions taken to try to achieve this and any difficulties the business had.

Simplified due diligence

6.74. Your business may apply a simplified form of customer 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. Some examples of potential lower risk factors are highlighted below in paragraph 6.80.

6.75. You will have to risk assess the clients to establish that they are low risk, that is, you will have to detail why they are low risk and document that assessment. When doing so you must take into relevant information made available by HMRC and the risks factors within the business-wide risk assessment.

6.76. This does not mean you do not have to do customer due diligence, and you are still required to identify and verify clients' identity, and take reasonable measures to verify the beneficial owners' identity. However, under simplified due diligence 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 the beneficial owner's identity:
    - during the establishment of a business relationship or
    - within a reasonable time, which HMRC would expect to normally be no more than 14 days from the start of the business relationship or transaction (this does not mean exemption from customer due diligence and any delay to customer due diligence must not be prohibited by any other legal requirement you are subject to)
- using at least one authoritative identity document to verify identity that:
    - demonstrates the person's name, and (at least) either their address or date of birth
    - contains security features that prevent tampering, counterfeiting and forgery
    - has been issued by a recognised body that has robust identity proofing measures (e.g. passport).
- using 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
- adjusting the frequency of customer due diligence reviews, for example, to when a change occurs.

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

6.78. 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 services provided to ensure that there is nothing unusual or suspicious from the outset
- it is not contradictory to information on risk provided by HMRC or any other authority in periodically published risk assessments
- the client is not established in or operates from a high risk third country identified by the FATF or a high risk third country identified by the UK
- the client is not a politically exposed person, or a family member or known close associate of one
- the client is seen face to face as is any co-owner
- the source of funds or wealth for the sale and purchase are transparent and understood by your business

- a sale, purchase or tenancy agreement is not complex or unusually large, for example, over £1 million for a residential sale, although your risk assessment may indicate that a lower sum would be considered large in your geographical location
- the client is not resident outside the UK
- for Estate Agency businesses, the property is not buy to let
- if the client is not an individual, that the legal entity is not registered or administered outside of the UK
- if the client is not an individual, that there is no beneficial ownership beyond a single UK legal entity customer.

6.79. To decide whether a client is suitable for simplified due diligence you must consider them to be low risk under all the factors to be considered in a risk assessment – see risk assessment above.

6.80. Type of customers that may indicate lower risk include:

- 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
- 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 that does not allow assignment of interests.

6.81. Geographical factors that may indicate a lower risk include:

- resident or established in an EEA state
- situated outside the EEA 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 and the FATF-style Regional Bodies as having in place effective anti-money laundering measures.

6.82. You must consider all of the factors, for example a customer from an EEA state is not automatically low risk simply because they are from the EEA. For example, the client could be from one EEA state, which is owned by a trust within another EEA state with the beneficial ownership in another EEA state – this level of complexity would increase the risks. All of the information you have on a customer must indicate a low risk.

6.83. You will need to record evidence, as part of your customer risk assessment, that a party to the sale or tenancy agreement is eligible for simplified due diligence. You will also need to conduct ongoing monitoring in line with your risk assessment.

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

6.85. Your decision may be tested by HMRC during compliance visits on the basis of the evidence that your business holds.

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

6.87. You must not continue with simplified due diligence if:

- you suspect money laundering or terrorist financing
- you're in doubt whether documents obtained for identification are genuine
- you doubt whether the person is the one demonstrated by the documentation
- you suspect that the documents obtained for identification may be lost, stolen or otherwise fraudulently acquired
- the business' circumstances change and your risk assessment no longer considers the customer, transactions or location as low risk
- any of the circumstances means that enhanced due diligence must apply.

Enhanced due diligence

6.88. Enhanced due diligence applies in situations that are high risk. It involves taking additional measures to identify and verify the client's identity and doing additional ongoing monitoring. In the case of politically exposed persons, this will include the source of funds.

6.89. 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 in published material or where, for example, a law enforcement interest has been registered with the Land Registry. In particular, further information relating to super-prime properties and other high risk areas can be found within the National Risk Assessment
- a client or any party relevant to the transaction is established in or operates from a high risk third country identified by the FATF or a high risk third country identified by the UK
- a person has given you false or stolen documents to identify themselves (immediately consider making a suspicious activity report)

- a client is a politically exposed person, an immediate family member or a close associate of a politically exposed person
- the transaction is complex and unusually large, or there is an unusual pattern of transactions, such as, in the case of legal entities, it has more than 2 levels of ownership, though this is dependent on what the business identifies as irregular based on their experiences
- the purchase, sale or tenancy agreement is for an unusually large amount for your type of business, location or for the individual
- a residential property is a super prime property. What a business identifies as super prime would be reflective of factors such as the region and the competitiveness of the market, usually within the top 5% of the local market values or
- during the course of completing due diligence, the business identifies a client is a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in that EEA state.

6.90. A branch or subsidiary of an EEA entity located in a high risk third country which fully complies with the parent's anti-money laundering policies and procedures and where the parent is supervised under the 5th Directive may not be subject to enhanced due diligence if your risk assessment finds it is not high risk.

6.91. You must consider a number of factors in your risk assessment when deciding if enhanced due diligence needs to be applied – see section 5 above. The following are some examples of things to take account of.

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

- any unusual aspects of a business relationship
- a person is resident in a high risk area/country
- use of a legal person or arrangement used to hold personal assets
- a company with nominee shareholders or shares in bearer form
- a person or business that has an abundance of cash or funds with no apparent source
- 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 example, fraud, money laundering, bribery or corruption.

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

- if the customer is a corporate body, 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.

6.94. Geographical factors indicating higher risk, including:

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

Additional measures to take

6.95. 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:

- obtaining 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
- taking additional measures to verify the documents supplied such as by checking them against additional independent sources, or requiring that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who are competent at document inspection and impostor detection, or a person from a regulated industry or in a position of trust
- if receiving payment, ensuring it is made through a bank account in the name of the person you are dealing with
- taking 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 (origin of the customer's overall wealth) and source of funds (origin of the funding of the transaction)
- carrying out more scrutiny of the business relationship and satisfying yourself that it is consistent with the stated purpose

- more regular and stringent ongoing monitoring checks (as per the business' policies, controls and procedures).

6.96. In the case of a person established in or operating from a high risk third country, the enhanced due diligence measures must include:

- additional information on the client and beneficial owner
- the intended nature of the business relationship
- source of funds and/or source of wealth of the client and beneficial owner
- reason for the transaction
- obtain senior management approval to establish and continue a business relationship
- conduct enhance monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Certified Documentation

6.97. 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 a person who is competent at document inspection and impostor detection, such as a person from a regulated industry or in a position of trust, as with passport photos
- an official stamp of the person certifying and indication of professional status
- been signed and dated with a printed name of the signatory, not the business
- the occupation and address or telephone number.

6.98. You must ensure that the person certifying the copy exists and is an appropriate person to certify the document.

6.99. Certifying a copy of a document does not constitute enhanced due diligence.

Politically exposed persons

6.100. Politically exposed persons are persons that are entrusted with prominent public functions held in the UK or abroad. The definition does not include:

- middle ranking or more junior officials (However, your risk assessment should consider whether they may be representing someone who is a politically exposed person)

- persons who were not a politically exposed person under the 2007 regulations where they ceased in office prior to 26 June 2017, such as former MPs or UK Ambassadors.

6.101. In the UK, public servants below Permanent or Deputy Permanent Secretary will not normally be treated as having a prominent public function.

6.102. 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 (for example, over the selection of candidates or distribution of significant party funds)
  - political parties who have some representation in a national or supranational Parliament or similar legislative body
- members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal, except in exceptional circumstances, in the UK:
  - 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, for example Vice Admiral, Lieutenant General or Air Marshal
- members of the administrative, management or supervisory bodies of state owned enterprises. This only applies to ‘for profit’ enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprises
- directors, deputy directors and members of the board, or equivalent of an international organisation:
  - includes international public organisations such as the UN and NATO
  - does not include international sporting federations.

6.103. Under the Regulations, you must also identify if your client is a family member or a known close associate of apolitically exposed person. The definition of a family member includes a spouse or civil partner, children (including those of the politically exposed person’s spouse or civil partner), and parents. Siblings should also be considered within the definition as a member family.

6.104. 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.

6.105. 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.

Politically exposed persons' risk

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

6.107. 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:

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

6.108. You are not required to, but you may decide to use a commercial provider to assist in identifying a politically exposed person especially if your business may be attractive to politically exposed persons.

6.109. Whatever source is used, you need to understand how any database is populated, for example what datasets are used and 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.

6.110. If a client is a politically exposed person, family member or known close associate of one, then you must put in place the following measures in addition to carrying out enhanced customer due diligence:

- obtaining senior management approval before establishing a business relationship with that person
- taking adequate steps to establish the source of wealth and source of funds that are involved in the proposed business relationship or transaction.

6.111. More frequent and thorough measures should be taken if the politically exposed person is higher risk.

6.112. 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. Similarly, a reduced level of enhanced due diligence measures can be applied to lower-risk politically exposed persons. A politically exposed person who has a prominent public function in the UK should be treated as lower risk unless other factors in your risk assessment indicate a higher risk. The same treatment should be applied to family members or close associates of lower risk UK politically exposed persons.

6.113. You must continue to apply enhanced due diligence when the politically exposed person has left their function or position 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 politically exposed persons 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.

6.114. 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.

6.115. 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 acting 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.

6.116. 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.

6.117. 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.

6.118. 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 contracts 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.

6.119. 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;
- related or associated with a politically exposed person who is no longer in office
- under 18 years of age.

6.120. 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
- have wealth derived from preferential access to the privatisation of former state assets
- have 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
- have wealth or lifestyle inconsistent with known legitimate sources of income or wealth
- are subject to credible allegations of financial misconduct made in relation to bribery or dishonesty
- hold an appointment to a public office that appears inconsistent with personal merit.

6.121. 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 has been 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.

6.122. 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.

Identifying individuals

6.123. As part of your customer due diligence measures, you must identify individuals by obtaining a private individual's given and family name, date of birth and residential address as a minimum.

6.124. 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.

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

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

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

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

6.128. Where the person does not have one of the above documents you may wish to ask for the following:

- a valid and genuine identity document from a recognised and authoritative source, such as a government issued document (without a photo) which includes the person's full name and also secondary evidence of the person's address, for example an old style driving licence or recent evidence of entitlement to state or local authority funded benefit such as housing benefit, council tax benefit, pension, tax credit
- secondary evidence of the customer's address, that can be verified as true by an authoritative source, commonly by confirmation of a reference number, name and address, for example a utility bill, bank, building society or credit union statement or the most recent mortgage statement.

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

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

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

6.131. The Nominated Officer, or other responsible person, must understand the types of document abuse within this guidance and cascade relevant parts to staff as part of their training programme.

6.132. If you verify the client's identity by documents, you must see the originals and not accept photocopies unless certified 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. The person should be competent at document inspection and impostor detection.

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

6.134. 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 (for the purposes of a second document). How and when this may be done must be covered in the risk assessment.

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

6.136. Where a person acts under a power of attorney, they are a customer as well as the donor (or grantor). Where the donor has lost mental capacity, his identity should be verified as a beneficial owner. Power of attorneys can act either independently of each or jointly whereby decisions must be agreed by the named attorneys. You must verify that they have the power to act in this role as well as carry out appropriate customer due diligence.

Persons without standard documents

6.137. 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 licences and passports to lapse.

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

6.139. 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.

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

6.141. 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

6.142. Simply carrying out an electronic records check 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).

6.143. 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.

6.144. 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. In addition, electronic verification alone cannot provide source of funds/wealth information which can only be given by the customer.

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

- use a package which addresses the risks detailed in your risk assessment and understand how it addresses those risks
- use multiple positive information sources, such as addresses or bill payment details
- use negative sources, such as databases identifying identity fraud and deceased persons
- use data from multiple sources collected over a period of time
- incorporate checks that assess the strength of the information supplied
- ensure that the system is set to fail/refer a customer at a level appropriate to the risk posed by the customer you are carrying out customer due diligence on
- retain, or have access to, sufficient records in order to comply with your record keeping requirements, which must take into account events such as an external provider going out of business.

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

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

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

- it is a notified eID scheme under the UK eIDAS Regulation;
- it is provided by means of a trust service covered by the UK eIDAS Regulation;
- it is accredited, or certified, to offer the identity verification or trust services through a government, industry or trade association process that involves meeting minimum published standards (such as those set out in the government's guidance on identity proofing , GOV.UK Verify or the eIDAS regulation);
- it is registered with the Information Commissioner's Office to store personal data
- the standards it works to, or accreditation, require its information to be kept up to date
- its compliance with the standards is assessed
- it uses a range of positive information sources, and links a person, through other sources, to both current and previous circumstances
- it uses negative information sources, such as databases relating to identity fraud and deceased persons

- it uses a wide range of alert sources, such as up to date financial sanctions information
- it has transparent processes that enable the firm to know the level of certainty as to the identity
- should be able to keep records of the information used to verify identity and make them available to the relevant authorities as required

6.149. The third-party provider should have processes that allows you to capture and store the information they used to verify an identity, if it is not one of the following:

- an eIDAS eID or trust service; or
- accredited, or certified, to offer eID or trust services through a governmental, industry or trade association process that involves meeting minimum published standards; or
- regulated, recognised, approved or accepted by the relevant national authority for the provision of digital identity or trust services; then
- they, the third party provider should have processes that allows you to capture and store the information they used to verify an identity.

Individuals not resident in the UK

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

6.151. If you have concerns that an identity document might not be genuine, contact the relevant embassy or consulate or use this link to PRADO (Public Register of Authentic travel and identity Documents Online): http://www.consilium.europa.eu/prado/en/prado-start-page.html

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

Identifying organisations

6.153. 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
- the trust deed (in trust cases). This must be obtained in such cases.

6.154. 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.

6.155. For private or unlisted companies you must take reasonable steps to obtain and verify the:

- 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.

6.156. It will also be necessary to establish the names of all directors (or equivalent), the ultimate beneficial owners and the names of individuals who own or control over 25% of its shares or voting rights - or the names of any individuals who otherwise exercise control over the management of the company. You must look through the ownership structure of any companies or trusts to establish the ultimate beneficial owners.

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

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

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

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

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

6.160. Where an individual claims to act on behalf of a client, 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

6.161. Where you cannot verify identities through reliable independent sources it may be obtained from the company itself if your risk assessment allows for this. 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 an Estate Agency business you can request that they provide you with the following information:

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

6.162. 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

6.163. If the customer:

- is subject to the requirements of Companies Act 2006, Part 21A
- is subject to the requirements of Limited Liability Partnerships (Register of People with Significant Control) Regulations 2016
- is subject to the requirements of the Scottish Partnerships ((Register of People with Significant Control) Regulations 2017 or
- on or after 10 March 2020, is subject to registration under Part 5 of the Regulations detailed at Regulations 42 to 45,

the relevant Estate Agent or Letting Agent business must collect proof of registration or an excerpt of the register for which they are registered, from the customer before a business relationship is established.

6.164. If a business identifies discrepancies within the PSC register, it is a requirement for the business to report this discrepancy. Further guidance regarding reporting discrepancies can be found here: https://www.gov.uk/guidance/report-a-discrepancy-about-a-beneficial-owner-on-the-psc-register-by-an-obliged-entity

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

6.166. 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.

6.167. The corporate person and trustee must notify you of any changes to the information supplied.

Beneficial owners

6.168. You must identify the existence of any beneficial owners (the section on customer due diligence gives information on who is a beneficial owner). You must take reasonable measures to verify the beneficial owner's identity so that you are satisfied that you know who the beneficial owner is. If it is a legal person, trust, company, foundation or similar legal arrangement you must take reasonable measures to identify and verify the ownership structure and look through the structures until you reach individuals who are the ultimate beneficial owners.

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

6.170. Where a client is incorporated and where you have made unsuccessful attempts, and have exhausted all ways, to identify the beneficial owner of a corporate body, you may treat the most senior person managing the customer as the beneficial owner. For example, a company may not have an ultimate beneficial owner due to the number of shareholders. You must keep written records that clearly show all the steps you have taken to identify the beneficial owners, the progress made and why they have been unsuccessful and consider whether they should be treated as a higher risk or even suspicious due to the number of entity layers.

6.171. It is common for property to be jointly owned by more than one individual. You must identify any co-owners, who are not your customers, as these will be beneficial owners. The customer you are dealing with may be either an owner or acting for the owners. You will need to carry out customer due diligence on all owners and any person acting on behalf of the owners. Ownership can be established through the HM Land Registry for England and Wales, the Land Registers for Northern Ireland and the Registers of Scotland.

Reliance on third parties

6.172. You must do customer due diligence before entering into a business relationship with a client. As relevant businesses are usually the first professional to be instructed and, because of this, they are usually unable to rely on a third party, such as a solicitor, bank or building society to carry out customer due diligence as these professionals are not employed until the business relationship has progressed.

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

- another UK business subject to the Regulations including another relevant business
- a business in the European Economic Area (EEA) who is subject to the 5th 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.

6.174. You may not rely on a business established in a high risk third country identified by the FATF or a high risk third country identified by the UK

6.175. The third party must agree that you will rely on them. The arrangement must include that the third party must:

- gives you details of the customer due diligence they hold so that you know it meets your risk requirements
- obtain immediately copies of the customer due diligence information from the third party on request
- ensure the third party retains copies of the due diligence information for five years from the date on which the transaction occurs or your business relationship with the customer ends.

6.176. 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.

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

6.178. For example, under Regulation 27 of the Regulations, it is the obligation of the introducing agent (forthwith called Agent A) to conduct customer due diligence checks and not the subsequent agent (Agent B). The obligation will always remain with Agent A as stipulated under Regulation 39 (1) and (7). If Agent B is to conduct customer due diligence, then they must understand and abide by the rules regarding reliance under Regulation 39. In this transaction, the customers for Agent A are the tenant and Agent B. For Agent B, their customers are Agent A and the landlord. Each agent must conduct the relevant checks on all parties

6.179. Reliance can only be on the customer due diligence carried out by another supervised business in order to meet their own requirements under the Regulations. It does not include accepting information from others to verify a person's identity for your own customer due diligence obligations such as obtaining a certified copy of a document, nor electronic verification which constitutes outsourcing a service. Within outsourcing arrangements, you still remain responsible for any failure to apply due diligence measures appropriately.

6.180. 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.

6.181. Sub agents can rely on the customer due diligence carried out by principal agents if it meets the conditions above.

6.182. Any arrangement for reliance should be written.

6.183. If you have requested reliance, but the other party refuses, the Estate or Letting Agent must clearly document what they have done in order to satisfy the requirement for due diligence and provide a clear audit trail of the steps they have undertaken.

7. Reporting suspicious activity

Minimum requirements:

7.1. You must:

- 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 (or their appointed alternate) must consider all internal reports. The nominated officer must make a report to the NCA as soon as it is practical to do so, even if no transaction takes place, if they consider that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or financing terrorism.
- The business must consider whether it needs to seek a defence against money laundering or terrorist financing offences (DAML) (formerly known as a consent SAR) from the NCA before proceeding with a suspicious transaction or entering into arrangements.
- It is a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place.

7.2. 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
- a record of any communications to or from the NCA (or other relevant authorities) about a suspicious activity report should be kept.

Suspicious activity reports (SAR)

7.3. This is the name given to a report sent to the NCA under the Proceeds of Crime Act or the Terrorism Act. You can access the NCA reporting portal through their website. The report identifies individuals or entities who you, or an employee, know, suspect, or have reasonable grounds to know or suspect, may be involved in laundering money or financing terrorism.

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

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

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

7.7. The suspicion is that the funds or property involved in the transaction is the proceeds of, or could be used in, any crime or is linked to corruption or terrorist activity. You do not have to know what sort of crime they may have committed but one or more warning signs of money laundering, which cannot be explained by the client, a colleague or any counterparty involved in the business relationship or transaction, will be relevant.

7.8. As a relevant business in the supervised 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 client and the transaction would cause a reasonable property professional in your position to have a suspicion. There is guidance about submitting a SAR within the supervised 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. Further information can be found here: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/446-guidance-on-submitting-better-quality-sars-1/file

7.9. You can submit a suspicious activity report to the NCA by registering with the NCA online. The NCA provides information and registration details online and the NCA prefers this method. The system does not 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.

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

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

7.11. Submitting a request for a DAML to the NCA, whether you are granted a defence, or not, does not replace the requirement on the business to complete customer due diligence before entering into a business relationship (see paragraph 7.22 below).

7.12. It is important that you have detailed policies, controls and procedures on internal reporting and the role of the nominated officer (see paragraph 7.16 below).

7.13. 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.

7.14. A suspicious activity report should be considered no matter what part of your business the suspicion arises in.

7.15. 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

7.16. You must appoint a nominated officer to make 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.

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

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

7.19. The nominated officer should consider 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 client, transaction or activity as the business has on its records.

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

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

Defence against money laundering (DAML)

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

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

7.24. The NCA has also produced good practice guidance and frequently asked questions to help you to produce good quality DAML SARs, Defence Against Money Laundering (DAML) FAQ.

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

7.26. A DAML relates to the principle offences in Proceeds of Crime Act (s. 327 to 329) and the Terrorism Act (s. 15-18) but not to other criminal offences.

7.27. A DAML 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.

7.28. 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.

7.29. 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.

7.30. 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.

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

7.32. The NCA has published information on obtaining a defence. Some of the key points are that:

- you only receive a DAML to the extent to which you ask for it. So you should clearly provide all the information on the transaction, persons involved and provide information on what the criminal assets are, their value (or an estimate) and whereabouts. For example: 'We seek a DAML in acting for a client (name/address/date of birth of customer) to find a property. He is residing at (full address and postcode) and wishes to purchase a residential property in Central London to a value of £x. He is represented by a solicitor (name and address). The funds and fees of (£x) may be the proceeds of crime due to the suspicions arising from the explanations given by the client that the purchase price would come from savings and an unspecified windfall and that large amounts of cash can be obtained to ensure the purchase goes smoothly. He also says he is prepared to pay over the asking price to secure a quick sale"
- you cannot ask for a general DAML to trade with a person, only to carry out a particular transaction
- if the request is urgent and you need a DAML sooner, you should clearly state the reasons for the urgency and perhaps contact the NCA to discuss the situation.
- the NCA will confirm their decision in writing.

7.33. Requesting a DAML 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.

Example of when you may consider making a SAR

7.34. These are some of the (non-exhaustive) factors to consider in deciding whether or not to submit a suspicious activity report when you deal with new transactions:

- checking the client's identity is difficult
- the client is reluctant to provide details of their identity or provides documents which may be fake
- the client is trying to use intermediaries to protect their identity or hide their involvement
- you must go through several legal entities in order to identify the beneficial owner or you are unable to identify whether there are any beneficial owners
- whether there is no apparent reason for using your business's services - for example, another business is better placed to handle the transaction due to location or specialism
- their lifestyle does not appear to be consistent with your knowledge of their income or income does not appear to be from a legitimate source
- the client is keen to sell, buy or let quickly at an unusually low or high price for no legitimate reasons
- part or full settlement is offered in cash or foreign currency, with weak reasons
- individuals or their associates are subject to, for example, adverse media attention, have been disqualified as directors or have convictions for dishonesty.

Tipping off

7.35. 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.

7.36. 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 person.

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

Regular and existing customers

7.38. These are some of the (non-exhaustive) factors to consider when deciding whether or not to submit a suspicious activity report in relation to your regular and existing customers:

- the transaction is different from the normal business of the customer
- the size and frequency of the transaction is different from the customer's normal pattern
- the pattern has changed since the business relationship was established
- the nature of any payments made changes. For example, a buyer's payment to an auctioneer is made in cash rather than through a bank account
- there has been a significant or unexpected improvement in the customer's financial position and the customer cannot give a proper explanation of where the money came from or their source of wealth or funds.

Property and Letting Transactions

7.39. These are some of the (non-exhaustive) factors to consider when deciding whether or not to submit a suspicious activity report in relation to the services you carry out:

- a third party, apparently unconnected with the client bears the costs, or otherwise pays the transaction costs
- large transaction paid for fully in cash or foreign currency
- the buyer or tenant will not disclose the source of the funds or the vendor or landlord the source of wealth where required
- unusual involvement of third parties, or large payments from private funds, particularly where the buyer appears to have a low income
- complex corporate structures are being employed for no apparent reason
- where the buyer or tenant are known to the vendor or landlord personally
- where a let or sale is agreed without the buyer or tenant having viewed the property/land
- unusual source of funds, such as virtual currencies or mortgage from an unknown or foreign bank.

7.40. These are some of the (non-exhaustive) factors to consider when deciding whether or not to submit a suspicious activity report in relation to letting transactions:

- request is made for the business to hold a large amount of client funds, which would seem unusual for the relevant business
- client does not appear to have the lifestyle that matches the amount needed to cover letting value
- full or large payment of a long let is made in cash (physical or cleared funds) up front and this request is made by a client and not the Letting Agency business
- multiple lets are being taken up for no apparent reason

- where it is known that a client of the business is immediately sub-letting the property/land and this would be considered unusual by the relevant business.

7.41. These are not complete lists and these signs are not always suspicious nor will you always have direct knowledge of them.

8. Record keeping

Minimum requirements:

8.1. You must retain:

- a copy of your customer contract and relevant documentation relating to the purchase, sale or tenancy
- copies of the evidence obtained to satisfy customer due diligence and details of client's transactions for at least five years after the end of the business relationship, and are not required to be kept more than 10 years
- a copy of your agreement with any customer due diligence outsourcing service provider
- details of transactions for a minimum of 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. These must be retained for five years from the date that the third party's relationship with the customer ends and the agreement should be in writing
- details of the customer due diligence held by another supervised business on which you are relying.

8.2. You must also maintain a written record of:

- your risk assessment, along with any changes that have been made
- your policies, controls and procedures, along with any changes that have been made
- internal audits of your procedures
- a written record of 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.

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

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

8.4. The records should be reviewed periodically to ensure that information is up to date where, for example, a change of ownership has occurred. This review need only include ongoing relationships.

8.5. 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.

8.6. After the period above, any personal data obtained for the purposes of the Regulations must be deleted unless you are required to keep them in relation to legal or court proceedings or any other legislation, or the data subject has given consent to the retention of the data.

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

8.8. This evidence may be used in court proceedings.

8.9. 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.

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

9. Staff awareness

Minimum requirements:

9.1. You must:

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

9.2. Larger and more complex businesses must:

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

Minimum action required:

9.3. You should ensure that your business addresses each of the following points and keeps the extent to which these points are satisfied under regular review:

- provide appropriate training to make relevant staff and agent aware of money laundering and terrorist financing legislation and issues, including how these crimes operate and how they might take place through the business
- ensure that relevant employees and agents have information on, and understand, the responsibilities and legal obligations of the business under this legislation - individual members of staff, for example, the functions of the nominated officer and any changes to these positions
- regularly communicate your risk assessment, policy, control and procedures information within the business and with branches and subsidiaries
- regularly give training to relevant staff in how to recognize and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing. Consider providing 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
- where appropriate for a larger and 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.

9.4. Your staff are the best defence against persons who could be involved in money laundering and terrorist financing who may try to abuse the services provided by your business.

9.5. You must take steps including:

- telling your staff about your anti-money laundering and counter terrorism financing obligations
- giving them suitable (risk based) training on their legal obligations
- telling them how to identify and deal with the risks
- making them aware of data protection obligations
- making them aware about how to effectively verify the identity of individuals.

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

9.7. Relevant staff are persons involved in Estate Agency and/or Letting Agency work.

Training

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

9.9. The training process should therefore cover the whole end to end process from receiving client's' instructions, through to market appraisal, dealing with offers through to completing the transaction.

9.10. 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.

9.11. Each member of staff must be ready to deal with the risks posed by their role. Their training must be appropriate to their role, and often enough, to keep their knowledge and skills up to date.

9.12. It must cover as a minimum:

- the staff member's duties

- the risks posed to the business
- the business policies, controls and procedures
- how to conduct customer due diligence and check client's documents where this is part of their role
- how to spot and deal with suspicious persons and activity
- document inspection and imposter detection including the Home Office guidance
- 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 as amended 10 January 2020; Part 7 of the Proceeds of Crime Act; and sections 18 and 21A of the Terrorism Act.

9.13. Training may include:

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

9.14. Your 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.

9.15. 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.

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

9.17. 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, confirmation of their understanding of the obligations or electronic training records
- an updated training schedule.

10. Estate Agency or Letting Agency Business risk

10.1. A relevant business in a metropolitan area with an international clientele is likely to present a different risk profile to a high street business in a small market town. However, both may be targeted by criminals if they have few or no controls in place.

10.2. The environment you do business in affects your risk assessment, for example, if you have super-prime property or if you have many high net-worth customers or deal with people from a particular country or region, this will influence the business-wide and/or client risk assessment.

10.3. You should be aware of the risk of transactions being used for tax evasion, for example, the use of complex legal entities or the manipulation of property prices to just below a Stamp Duty threshold, perhaps by 'rigging' the price of fixtures and fittings. You should also look closely at transactions, especially woodland or agricultural land purchases that may be intended to avoid Inheritance Tax.

10.4. Other areas of particular concern are:

- relevant business staff being offered bribes, for example in relation to valuations or planning applications
- the source of funds potentially coming from mortgage fraud by a client
- landlords not complying with their legal obligations, for example, licensing requirements
- attempts to pay fully or partially for the purchase of a property from the proceeds of criminal activity like internet fraud, drug dealing, prostitution or human trafficking
- acceptance of disproportionate corporate hospitality
- use of a client fund account for non-property transactions or other funds handling services
- tenants attempting to sell or let properties they have rented or persons selling properties they do not own
- lettings being used as brothels and other similar facilities which will assist in money laundering or terrorist financing
- lettings which are empty for part of or throughout the agreement
- owner of various properties using multiple agents without justification
- virtual currencies being used to finance property transactions
- true identity of landlords being hidden through tenancy agreements.

Identifying risks in the transaction

10.5. Identifying a client or transaction as high risk does not automatically mean that they are involved in money laundering or terrorist financing. Similarly, identifying a person or transaction as low risk does not mean that they are not involved in money laundering or terrorist financing.

10.6. Below are some warning signs of risk or potentially suspicious activity for new or existing clients. These are not complete lists and these signs are not always suspicious nor will you always have direct knowledge of them. It depends on the circumstances of each case.

- searches on a party to a transaction or associate show, for example, adverse media attention, disqualification as a director, convictions for dishonesty or association with bribery in relation to contract procurement
- being evasive or reluctant to provide required customer due diligence information or documentation or where ownership is said to be confidential
- checking the person's identity is difficult
- the person is reluctant to provide details of their identity or provides fake documents
- the person is trying to use intermediaries to protect their identity or hide their involvement
- non-UK resident using intermediaries where it makes no commercial sense
- no apparent reason for using your business's services - for example, another business is better placed to handle the size of the transaction or the location of the property
- part or full settlement in cash or foreign currency, with weak reasons
- use of cash in a quick sale or tenancy agreement, or cash exchanges directly between clients - perhaps including a cash deposit
- poor explanation for the early redemption of a previous mortgage, especially where redemption incurs a penalty cost
- the customer or counterparty does not take up services that are attractive or is willing to pay fees that seem unnecessary
- the property value doesn't fit the customer's profile
- the client has not viewed the property or has only seen it on the internet
- customers are similar - a group of purchasers with similar profiles purchases new builds or off plan can be an indicator of organised mortgage fraud
- the ownership is not transparent and uses complex trusts, offshore arrangements or multiple companies possibly involving multiple countries
- reluctance to employ a solicitor or other professional for conveyancing.

10.7. How a transaction is carried out or requests made by a client may indicate a greater risk:

- the use of multiple companies or trusts which adds layers of complexity to ownership particularly where those layers seem unnecessary, for example, trusts owning trusts or offshore shell companies
- a property has multiple owners or is owned by nominee companies
- where multiple properties are purchased, resold or exchanged
- a large cash deposit with the balance from an unusual source
- multiple payments of smaller amounts possibly through different accounts and to avoid thresholds put in place by overseas authorities

- sale or letting price significantly above or below market price
- the use of property management or investment companies who may not trade to make ownership less transparent
- an unknown third party appears at a late stage
- unusual speed or requests to expedite transactions unnecessarily, possibly over or under value
- a sudden or unexplained change in ownership
- the immediate resale (flipping) or letting of property at a higher value
- a third party, apparently unconnected with the client bears the costs, settles invoices or otherwise pays the transaction costs
- the customer requests payment to a third party who has no apparent connection with the customer
- an unusually big cash or foreign currency transaction, and the buyer will not disclose the source of the funds
- unusual involvement of third parties, cash gifts, or large payments from private funds, particularly where the buyer appears to have a low income
- using multiple intermediaries or professionals to hide ownership or to arrange unusually complicated transactions
- you're asked to hold a big sum in your client account, then refund it to the same or a different account
- proceeds of a sale or rental sent to a high-risk jurisdiction or unknown third party
- successive transactions, especially of the same property, with unexplained changes in value
- unusual source of funds, for example complex loans or unexplained charges
- the owner, landlord or builder isn't complying fully with their legal obligations, perhaps to save money
- a previously sold property is re-marketed following renovation without an obvious source of funding.

11. More information

11.1. You can contact HMRC by:

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

11.2. Further information about the obligations set out in this guidance is available from:

Property mark

Royal Institution of Chartered Surveyors

Association of Relocation Professionals

The Association of Residential Managing Agents

The Joint Money Laundering Steering Group

11.3. Information on the role of the National Trading Standards Estate and Letting Agency Team and whether you need to join a property redress schemes is available at:

National Trading Standards Estate and Letting Agency Team