Anti Money Laundering Supervision: Estate Agency Businesses

Contents

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

General Introduction

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

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

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

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.

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

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

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

Status of this guidance

This guidance has been submitted for HM Treasury approval.

This guidance replaces HMRC's guidance: "Supervision of Estate Agency Businesses by HMRC" published on 13 August 2014 and MLR9a published 31 January 2014. This guidance is effective from 26 June 2017. It is not retrospective.

Meaning of words

In this guidance, the word 'must' denotes a legal obligation. Each chapter summarises the

legal obligations under the heading 'minimum requirements', followed by the actions required to meet the legal obligations.

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

The phrase ‘relevant business’ is the term used to describe carrying out regulated activity listed in the Regulations.

1. Money laundering and Estate Agency Businesses

1.1 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 often involves:

- 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 may also hide behind complex company structures and multiple bank accounts to disguise the real purpose of a transaction and hide its beneficial ownership
- a more direct method may involve paying an estate agency business a large amount and reclaiming it later
- the money for a purchase may be the result of mortgage fraud.

1.2 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. In a commercial setting, there may be underreporting of business turnover.
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

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

Legislation

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

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations)
- Criminal Finances Act 2017.

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

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

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

1.5 Under the Proceeds of Crime Act it's 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 businesses. This obligation extends across the whole business, so an estate agency business which also does lettings must also submit suspicious activity reports where suspicion arises within lettings.

1.6 The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses, like estate agency businesses, must report belief or suspicion of offences related to terrorist financing, such as:

- fundraising for the purposes of terrorism
- using or possessing money for the purposes of terrorism
- involvement in funding arrangements
- money laundering - facilitating the retention or control of money that's destined for, or is the proceeds of, terrorism.

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

1.8 The Regulations set out what relevant businesses like estate 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:

- customer due diligence
- reporting suspicious activity
- record keeping
- staff awareness.

It also gives information on risk indicators within the sector and information in relation to different types of estate agency businesses.
The Joint Money Laundering Steering Group publishes more information about businesses' obligations:

http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current

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

- estate agents, that is businesses carrying on estate agency work
- credit institutions
- financial institutions
- auditors, insolvency practitioners, external accountants and tax advisers
- independent legal professionals
- trust or company service providers
- high value dealers
- casinos.

Estate agency businesses must comply with the Regulations. They must not carry out estate agency work if they are not registered with HMRC.

This is explained in more detail later in this guide.

Financial sanctions

1.10 All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. Your client and their property may be subject to sanctions.
Most financial sanctions are made through EU law which has direct effect under UK law. The Office of Financial Sanctions Implementation works closely with the EU Commission and other member states in implementing sanctions. Other financial sanctions are put in place by UK laws.
You should report any transactions carried out for persons subject to sanctions or if they try to use your services.
You can report a suspected breach, sign up for free email alerts and obtain Information on the current consolidated list of asset freeze targets and persons subject to restrictive measures at:.

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

Data Protection

1.11 The Data Protection Act 1998 governs the processing of information relating to individuals, including obtaining, holding, use or disclosure of information.
Personal data obtained by a business under the Regulations may only be processed for the

prevention of money laundering and terrorist financing. You must inform your customers of this and the information specified in paragraph 2(3) of schedule 1 to the DPA.
This use is necessary in order to exercise a public function that is in the public interest and to carry out a function permitted by legislation.
No other use may be made of the information unless you have consent of the customer or it is allowed by other legislation.

Penalties

1.12 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.

2. Responsibilities of senior managers

Senior managers

2.1 The senior managers of a regulated business are personally liable if they do not take the steps necessary to protect their business from money laundering and terrorist financing.

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

Minimum requirements

2.2 Senior managers must:

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

Responsibilities

2.3 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.

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

2.4 Senior managers must:

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

3. Risk assessment, policies, controls and procedures

Risk based approach

3.1 A risk based approach is where you assess the risks that your business may be used for money laundering or terrorist financing, and put in place appropriate measures to manage and lessen 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 most important areas and reduce unnecessary burdens.

Risks your business may face

3.2 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, for example through the following questions.

Risk Assessment

3.3 Your risk assessment is how you identify the risks your business is exposed to. You must be able to understand all the ways that your business could be exposed to money laundering and terrorism financing risks, and design systems to deal with them.

Minimum requirements

You must:

- identify and monitor the risks of money laundering and terrorist financing that are

relevant to your business - in other words, your business's risk assessment

- take note of information on risk and emerging trends from the National Risk Assessment and HMRC's risk assessment and amend your procedures as necessary
- assess, and keep under regular review, the risks posed by your particular:
  - customers and any underlying beneficial owners (see sector guidance on customer due diligence on who is the beneficial owner)
  - services, for example, auctioneering, property finding or sales agency
  - financing methods
  - delivery channels, for example on-line or other non-face to face services
  - geographical areas of operation, including sending money to, from or through high risk third countries, for example countries identified by the EU or Financial Action Task Force (FATF) as having deficient systems to prevent money laundering or terrorist financing business.

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

In some limited circumstances we may tell you that you do not need to keep a record of your risk assessment, for example a sole practitioner with no employees with a small number of well-established clients and where the money laundering and terrorist financing risks are understood. Contact HMRC if you think this applies to you.

3.4 These are some of the questions to consider which may help inform your risk assessment:

- how does the way the seller or buyer comes to the business affect the risk for:
  - non face-to-face customers
  - occasional transactions, as opposed to ongoing business
  - does the pattern of behaviour, or changes to it, pose a risk
  - if you accept introductions from another agent or third party, what is your knowledge of that agent
- are sellers or buyers companies, partnerships, or trusts
- do you undertake business in areas with a highly transient population
- is the customer type stable or does it have a high turnover of different types of client
- do you act for international sellers or buyers 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 act for entities that have a complex ownership structure or a cross border

element

- do you accept payments that are made to or received from third parties
- do you accept cash payments
- which sellers or buyers may pose a greater risk:
  - buyers who may be carrying out large one-off cash transactions
  - sellers or buyers that are not local to the business
  - those that are non-face to face
  - overseas sellers or buyers especially from a high risk third country identified by the EU and FATF
  - individuals in public positions and/or locations that carry a higher exposure to the possibility of corruption, including politically exposed persons (see sector guidance on politically exposed persons)
- complex business ownership structures, that is, any client which is a legal person, with ownership by another legal person. For example a limited company with over 25% of shares owned by another limited company.

3.5 When designing systems to identify and deal with suspicious activity, there are some warning signs of potentially suspicious activity that your systems should be capable of picking up and flagging for attention - see section 5. Again, this is not an exhaustive list, and these signs are not always suspicious. It depends on the circumstances of each case.

Policy, controls and procedures

Policy statement

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

It must make clear who has responsibility for maintaining, managing and monitoring the policies and procedures.

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

Controls and procedures

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

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

Minimum requirements

3.8 You must also show how you will:

- do customer due diligence checks on sellers and buyers and carry out ongoing monitoring
- identify when a seller, buyer or beneficial owner is a politically exposed person or a family member or close associate of one and do enhanced due diligence
- appoint a nominated officer to receive reports of suspicious activity from staff and make suspicious activity reports to the National Crime Agency and make clear how reports are to be made in their absence
- make sure the staff are trained to recognise money laundering and terrorist financing risks and understand what they should do to manage these, including the importance of reporting suspicious activity to the nominated officer
- maintain accurate, up-to-date record keeping and retention of records for 5 years from the end of a business relationship.

Actions required

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

- ensure identification and acceptance procedures reflect the risk characteristics of sellers or buyers
- 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
- ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of sellers or buyers and 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 training is appropriate to the individual and kept up to date and content

regularly reviewed
- ensure staff know the names of the nominated officer and any deputy.

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

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

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

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

Appointing a nominated officer for the business

3.13 You must appoint a nominated officer, from within your business, to receive reports of suspicious activity from staff and decide whether to report them to the National Crime Agency. You should also appoint a deputy to act in the absence of the nominated officer. If you are a sole trader with no employees you will be the nominated officer by default, and must report suspicious activity to the National Crime Agency.
The nominated officer should be at an appropriate level of seniority in your business to make decisions on transactions.
You should make sure that your staff know the name of the nominated officer and any deputy and 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

3.14 You should consider whether the size and nature of your business means that you must appoint a compliance officer to ensure your compliance with the Regulations. You should take into account your risk assessment and exposure to money laundering and terrorist financing risk, the number of employees, number of premises, agent network, geographical area you operate in, type of customers, and the complexity of the business.
HMRC would not expect you to appoint a compliance officer where you are a sole trader where you carry out regulated activity from one premises, have no more than two or three staff and run an uncomplicated business model or organisation.
Businesses with, for example, more premises, use branches or agents, high turnover of customers, non-local or cross border trading and complex ways to deliver services will need a compliance officer. This is so that the business can ensure that, for example, training, record keeping and compliance requirements are observed and consistent throughout the organisation.

3.15 Where a compliance officer is needed, the business must:

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

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
  - review of how effective these are
  - recommend and carry out improvements
- ensure compliance throughout the business including subsidiaries and branches
- oversight of relevant staff screening.

3.16 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 with the Regulations including the receiving of documents from clients.

3.17 It is recommended that the compliance officer and nominated officer should not be the same person. This is because the responsibilities differ, the compliance officer needs to be

at a senior management level and needs to review how the business carries out its obligations, including the reporting of suspicious activity. However, in some businesses it may not be practical to have two individuals carrying out these functions and a compliance officer may have to act in the role of a nominated officer.
Given the importance of this role businesses may need to appoint a deputy compliance officer.

HMRC expects the compliance officer and nominated officers to be based in the UK. Where a business is part of a group of companies an individual can carry out these roles for other parts of the group. If each subsidiary has their own compliance officer then one person should have oversight of this.

Personal liability of officers

3.18 You will be committing a crime if you do not comply with the Regulations. You may incur an unlimited fine and/or a prison term of up to 2 years if:

- you agree to, or are involved in committing a crime
- a crime is committed because of your neglect.

Controls and procedures to put in place

3.19 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'll help to decide the level of due diligence to apply to each seller, buyer and beneficial owner. It's likely that there will be a standard level of due diligence that will apply to most sellers and buyers, based on your business's risk assessment.

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

- the types of seller, buyer and transactions that you consider to be lower risk and those that qualify for simplified due diligence and those that are higher risk and merit closer scrutiny
- how to carry out customer due diligence, the identification requirements for sellers, buyers and beneficial owners and how to carry out enhanced due diligence on higher risk persons

- any other patterns or activities that may signal that money laundering or terrorist financing is a real risk
- how to keep records, where and how long they should be kept
- how to conduct ongoing monitoring of transactions and customers
- clear staff responsibilities and the name and role of the nominated officer
- how policies and procedures will be reviewed
- how to report suspicious activity to the nominated officer, and how the nominated officer should make a report to the National Crime Agency.

3.21 Examples of risk-based controls include:

- introducing a customer identification and verification programme that varies depending on the assessed level of risk
- requiring additional seller or buyer identity evidence in higher risk situations
- reviewing low risk sellers and buyers and applying more due diligence where changes are apparent
- varying the level of monitoring of transactions and activities depending on the assessed level of risk or activities that might be unusual or suspicious.

3.22 This list is not exhaustive. You could also have other risk-based controls depending on the circumstances of your business.
Identifying a seller, buyer or transaction as high risk does not automatically mean that they're involved in money laundering or terrorist financing. Similarly, identifying a seller, buyer or transaction as low risk does not mean that they're not involved in money laundering or terrorist financing.

Effectiveness of the controls

3.23 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 procedures and controls, such as internal compliance audits, as this helps to keep them under regular review. You should have a process for monitoring whether they are working effectively, and how to improve them, for example to reflect changes in the business environment, such as new product types or business models.

Managing group subsidiaries

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

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

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

Managing a branch network

3.25 If you manage a branch network these are some of the questions to consider in addition to those previously covered. to help inform your risk assessment:

- how will you apply risk management procedures to a network of branches
- how will you manage and maintain records, what type of records
- if you selected a number of transaction files at random, would they all have a risk assessment and adequate customer due diligence for the seller , buyer and beneficial owners and will ongoing monitoring support the original assessment
- if you have applied simplified due diligence will the records show evidence for treating the seller or buyer as low risk
- do you have a system that will pick up where individuals, departments or branches are not implementing risk management procedures
- could you demonstrate that all staff have been trained on the Regulations and the business's procedures, and given ongoing training on recognising and dealing with suspicious transactions
- if asked, will staff know who the nominated officer is, what the firm's policies are and where they can be found.

4. Customer due diligence

Minimum requirements

4.1 You must:

- complete customer due diligence on all customers and beneficial owners before entering into a business relationship or occasional transaction
- complete due diligence on the other party to the property sale
- 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 limited company or trust
- apply enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, including when the customer is not physically present when being identified, and in respect of politically exposed persons
- 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 to keep the information up to date

4.2 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 so are in an ideal position to identify suspicious activity.

The customer

4.3 The customer is the person or entity with whom the estate agency business forms a contractual relationship, often referred to as the client, who can be a seller (that is the owner or owners of the property) or the person, or persons, who buys the property.

For sales agents, it is usually the vendor, although in the case of repossessions it may be the lender. A property finder will normally act for a buyer to find a property. An auctioneer may act for sellers, buyers and bidders.

4.4 An estate agency business enters into a business relationship with both parties to the transactions, i.e. the property seller and the property buyer. The person who is not a customer, in the commercial sense, 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.

Business relationship

With a customer

4.5 A business relationship is formed 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 estate agency business and the customer will not have a contract in writing.

An auctioneer may form a business relationship with its customers who are sellers, bidders and the buyer.

With the other party

4.6 In the case of sales agent, a business relationship is entered into with a buyer, who is not the customer, when the buyer's offer is accepted by the seller.

In the case of a relocation agent, property finder or investment broker, a business relationship is also formed with the seller, no later than at the point the buyer's offer is

accepted. In this case the buying agent may well be able to rely on the customer due diligence carried out by a sales agent (and vice versa) with their consent - see "Reliance on third parties".

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.

In most cases a property sale involves an element of duration so will be a business relationship.

Customer due diligence

4.7 You must carry out customer due diligence on your customer and the other party to the transaction which may be a seller or buyer. The level of due diligence will depend on your risk assessment of each person.
You must verify that both parties to the property sale 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.

4.8 You must undertake customer due diligence when:

- establishing a business relationship with a seller and buyer
- carrying out an occasional transaction with a customer
- money laundering or terrorist financing is suspected
- you suspect that information obtained for due diligence checks on a seller or buyer is not reliable or adequate.

4.9 Customer due diligence means:

- identifying all sellers and all buyers and verifying their identity (more details below)
- identifying all beneficial owners, where applicable, and taking reasonable measures to verify their identity to satisfy yourself that you know who they are
- obtaining information on the purpose and intended nature of the business relationship although in most cases this will be self-evident for estate agency businesses
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the seller and buyer, and the risk profile
- retaining records of these checks and update them when there are changes.

Timing

4.10 The customers' identity and where applicable the identity of beneficial owners, must be verified before entering into a business relationship or occasional transaction.
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

However, this exception is very limited as the verification must still be completed by the time the business relationship is entered into. Nor does this exception mean that you can use it where it is hard to verify a customer's or beneficial owner's identity.

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

4.11 An auctioneer should carry out customer due diligence on a bidder who is a customer before they receive a paddle and on the buyer before the hammer falls.

Timing in relation to the other party to a property sale

4.12 The other party's identity and where applicable the identity of beneficial owners must be verified before the contracts are exchanged.

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

In practice this means that customer due diligence should be carried out as early as possible on the other party. Selling agents 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.

4.13 Where the sales process involves sealed bids customer due diligence must be carried out before the bids are opened.

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

4.15 If the other party has agreed terms with a conveyancer or estate agency 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").

Extent of customer due diligence

4.16 The extent of customer due diligence measures depends on the degree of risk. It depends on the type of seller or buyer, business relationship, product or transaction and any geographical risk.
It goes beyond simply carrying out identity checks to understanding who you are dealing with. This is because even people you already know may become involved in illegal activity at some time, for example where their personal circumstances change or they face some new financial pressure. Your customer due diligence measures should reduce the risk of this and the opportunities for staff to be influenced.
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

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

- carry on estate agency work with, or for, the seller or buyer
- establish a business relationship or carry out an occasional transaction with the seller or buyer.

4.18 If you cannot comply with the customer due diligence measures, you must:

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

Ongoing monitoring of a business relationship

4.19 You must continue to monitor a business relationship after it is established. This means you must monitor transactions, and where necessary the source of funds, to ensure they are consistent with what you know about the seller or buyer and their risk assessment.
You must also keep the information you collect for this purpose up-to-date in line with your risk assessment. It should be checked periodically and expired documents replaced with copies of newly issued documents.

Occasional transactions

4.20 An occasional transaction is a transaction of €15,000 or more (or the sterling equivalent) that is not part of an ongoing business relationship. It also applies to a series of transactions totalling €15,000 or more, where there appears to be a link between transactions.
The value of the transaction here means the gross value of the property transaction, not the value of your fees.

Politically exposed persons

4.21 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

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

4.22 Politically exposed persons include:

heads of state, heads of government, ministers and deputy or assistant ministers	
members of parliament or similar legislative bodies	**includes** regional governments in federalised systems and devolved administrations, including the Scottish Executive and Welsh Assembly, where such bodies have some form of executive decision-making powers. **does not include** local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries.
members of the governing bodies of political parties	**member of a governing body** will generally only apply to the national governing bodies where a member has significant executive power (e.g. over the selection of candidates or distribution of significant party funds). **political parties** who have some representation in a national or supranational Parliament or similar legislative body.
members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances	in the UK: • this **includes** judges of the Supreme Court

	• **does not include** any other member of the judiciary
members of courts of auditors or boards of central banks	
ambassadors, and high ranking officers in the armed forces	**where persons holding these offices on behalf of the UK government** are at Permanent Secretary or Deputy Permanent Secretary level, or hold the equivalent military rank e.g. Vice Admiral, Lieutenant General or Air Marshal
members of the administrative, management or supervisory bodies of state owned enterprises	this only applies to for profit enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprises
directors, deputy directors and members of the board, or equivalent of an international organisation.	**includes** international public organisations such as the UN and NATO. **does not include** international sporting federations.

4.23 The definition includes family members such as spouse, partners, children (and their spouse or partner) brother, sisters and parents and known close associates.

4.24 Close associates are persons who have:

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

Beneficial owners

4.25 Beneficial owners are individuals who ultimately own or control the customer, or on whose behalf a transaction or activity takes place. Examples of beneficial owners may include:

- the vendor or purchaser customer of a principal agent 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.

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

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

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

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

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

4.28 For a trust, a beneficial owner includes:

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

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

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

- individuals who benefit from the entity's property

- where beneficiaries have not been established, the class of persons in whose main interest the entity or arrangement is set up or operates
- any individual who exercises control over the property.

4.31 For the estate of a deceased person in the course of administration, a beneficial owner means:

- the executor (original or by representation) or administrator for the time being of a deceased person in England, Wales or Northern Ireland
- the executor for the purposes of the Executors (Scotland Act) 1900 in Scotland.

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

4.33 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.
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.
Subject to the criteria in "Reliance on third parties", a sub-agents may be able to rely on the customer due diligence carried out by a principal agent.

Simplified due diligence

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

4.2 You will have to risk assess the seller and buyer and to establish that they are low risk.

4.3 This does not mean you do not have to do customer due diligence, and you are still required to verify seller, buyer and beneficial owner identity, but 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 beneficial owners identity:
    - during the establishment of a business relationship or
    - within a reasonable time, which HMRC would expect to normally be no more

than 14 days from the start of the business relationship or transaction (this does not mean exemption from customer due diligence and any delay to customer due diligence must not be prohibited by any other legal requirement you are subject to)

- if applicable verify the identity when transactions exceed a reasonably low level
- use one document to verify identity
- use information you have to determine the nature or purpose of a business relationship without requiring further information, for example, if your customer is a pension scheme you can assume what the purpose is
- adjust the frequency of customer due diligence reviews, for example, to when a change occurs

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

4.4 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 transactions to ensure that there is nothing unusual or suspicious
- it is not prevented by information on risk provided by HMRC or any other authority
- the seller or buyer is not from a high risk third country identified by the EU
- the buyer or seller is not a politically exposed person, or a family member or known close associate of one
- the buyer or seller 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
- the sale or purchase is not complex or unusually large, that is, over £1million although your risk assessment may indicate that a lower sum would be considered large in your geographical location
- the buyer or seller is not resident outside the UK
- the property is not buy to let
- if the buyer or seller is not an individual, that the legal entity is not registered or administered outside of the UK
- if the buyer or seller is not an individual, that there is no beneficial ownership beyond that legal entity.

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

4.6 Type of customer that may indicate lower risk are:

- 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 listed company that is subject to disclosure provisions
- beneficial owners of pooled accounts held by a notary or independent legal professional, provided information on the identity of the beneficial owners is available upon request
- a European Community institution.
- a pension scheme.

4.7 Geographical factors that may indicate a lower risk but not that the customer is low risk is where the customer is:

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

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

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

4.10 You must not automatically assume that a party to the sale 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. Your decision may be tested on the basis of the evidence that your business holds.

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

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

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

Enhanced due diligence

4.13 'Enhanced due diligence' applies in situations that are high risk, taking additional measures to identify and verify the seller and buyer's identity and source of funds and doing additional ongoing monitoring.

4.14 You must do this when:

- you have identified in your risk assessment that there is a high risk of money laundering or terrorist financing
- HMRC or another supervisory or law enforcement authority provide information that a particular situation is high risk
- a seller or buyer is from a high risk third country identified by the EU and FATF
- a person has given you false or stolen documents to identify themselves (consider making a suspicious activity report)
- a seller or buyer is a politically exposed person, an immediate family member or a close associate of a politically exposed person
- the transaction is complex or unusually large such as over £1 million

4.15 A branch or subsidiary of an EU 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 4th Directive may not be subject to enhanced due diligence if your risk assessment finds it is not high risk.

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

4.17 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
- an unusual or complex company structure given the nature of the type of business
- searches on a person or associates show, for example, adverse media attention, disqualification as a director or convictions for dishonesty

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

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

4.19 Geographical factors indicating higher risk:

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

Additional measures to take

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

- obtain additional information or evidence to establish the identity
- take additional measures to verify the original documents supplied
- ensure the first payment is made through a bank account in the name of the seller or

buyer

- take more steps to understand the history, ownership, and financial situation of the parties to the transaction
- in the case of a politically exposed person establish the source of wealth and source of funds
- carry out more scrutiny of the business relationship and satisfy yourself that it is consistent with the stated purpose.

4.21 If the original documents are not produced for verification 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"
- an official stamp of the person certifying
- signed and dated with a printed name of an authorising person in a bank or other financial institution or by a solicitor or notary
- occupation, address and telephone number.

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

Politically exposed persons risk

4.22 You must always apply enhanced due diligence on politically exposed persons, their family members or a known close associate of one. You must have appropriate risk management systems and procedures in place to determine whether a customer is a politically exposed person or a family member or known close associate of one. You should take account of:

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

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

- news agencies and sources
- government and parliament websites
- Electoral Commission: http://search.electoralcommission.org.uk/
- Companies House Persons of Significant Control:

https://beta.companieshouse.gov.uk/

- Transparency International: https://www.transparency.org/
- Global Witness: https://www.globalwitness.org/en-gb/campaigns/oil-gas-and-mining/myanmarjade/

You are not required to, but you may decide to use a commercial provider.

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

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

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

4.24 You must continue to apply enhanced due diligence when the politically exposed person has left the function or position and for a further period of at least 12 months. Any extension over 12 months will normally only apply to a politically exposed person you have assessed as higher risk.
For family members and close associates the obligation to apply enhanced due diligence stops as soon as the politically exposed person no longer holds the office unless there are other reasons for treating them as higher risk.

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

4.26 A politically exposed person who has a prominent public function in the UK should be treated as lower risk unless other factors in your risk assessment indicate a higher risk. The same treatment should be applied to family members or close associates of lower risk UK politically exposed persons.

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

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

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

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

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

4.30 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 with traits such as:

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

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

- lifestyle or wealth does not match what you know of their income source
- credible allegations of financial misconduct have been made in relation to bribery or dishonesty

- there is evidence they have sought to hide the nature of their financial situation
- has responsibility for or can influence the awarding of large procurement contract where the process lacks transparency
- has responsibility for or can influence the allocation of government grant of licenses such as energy, mining or permission for major construction projects

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

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

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

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

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

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

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

4.35 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

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

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

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

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

- 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 person's address, not downloaded from the internet, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement.

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

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

4.40 More information on official documents and how to spot counterfeits and forgeries is published by the Home Office in their 'Basic Guide to Forgery Awareness

and “Guidance on examining identity documents”:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536918/Guidance_on_examining_identity_documents_v._June_2016.pdf

The Nominated Officer, or other responsible person, should be aware of the issues within this and cascade relevant parts to staff as part of their training programme.

4.41 If you verify the seller or buyer’s identity by documents, you must see the originals and not accept photocopies, nor accept downloads of bills, unless certified (see paragraph 4.51) as described below:

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

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

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

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

4.44 Where a person acts under a power of attorney they are a customer, as well as the donor (or grantor). You should verify that they have the power to act in this role as well as carry out appropriate customer due diligence.

Electronic verification

4.45 An electronic records check carried out on limited information establishes only that an individual exists, not that the seller or buyer is that individual. For example, simply carrying out electronic verification to check 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 should ensure that the checks you use show that you have identified the customer, verified the identity and that they are, in fact, the same person that is using your services (to protect against impersonation). You should therefore verify key confidential facts, that only the seller or buyer may know to establish who they say they are. For example

testing background information such as their place of birth, how long they have been resident at an address with previous addresses when resident for a short period or education history. 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, such as verifying that a person's signature is genuine.

4.46 If you verify an individual's identity electronically, you should, for example:

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

The extent of the checks should satisfy the level of risk established in your risk assessment.

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

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

Individuals not resident in the UK

4.48 You should obtain the same types of identity documents for non UK residents as for UK residents.
If you have concerns that an identity document might not be genuine, contact the relevant embassy or consulate or use the link to PRADO below. If documents are in a foreign language, you must satisfy yourself that they do in fact provide evidence of the seller or buyer's identity. HMRC may require official translations when inspecting your customer due

diligence records.

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

Identifying organisations

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

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

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

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

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 any companies or trusts to establish the ultimate beneficial owners.

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

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

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

Obligation of customers to provide information

4.53 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.

4.54 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

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

4.55 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.

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

Beneficial owners

4.57 You must identify the existence of any beneficial owners (the section on customer due diligence gives information on who is a beneficial owner). You must verify the beneficial owner's identity so that you are satisfied that you know who the beneficial owner is. If it is a legal person you must take reasonable measures to understand the ownership structure.

4.58 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.

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

4.60 It is common for property to be owned by more than one person. You must identify any co-owners as these will be beneficial owners. The customer you are dealing with may be either an owner or is acting for the owners. You will need to carry out customer due diligence on the owners and any person acting on behalf of the owners. Ownership can be established through land registry and examining documents such as mortgage statements.

Reliance on third parties

4.61 You must do customer due diligence before entering into a business relationship with a seller or buyer. As estate agency businesses are usually the first professional to be instructed, 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. You can rely on the following persons to apply customer due diligence for you before entering into a business relationship with a seller or buyer:

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

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

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

- obtain immediately on request copies of the customer due diligence information from the third party
- ensure the third party retains copies of the customer due diligence information for five years from the date the reliance was agreed.

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

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

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

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

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

5 Reporting suspicious activity

5.1 Core obligations**:**

- Staff must raise an internal report where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that a terrorist finance offence may be committed.
- The business's nominated officer must consider all internal reports. The nominated officer must make a report to the National Crime Agency (NCA) as soon as it is practical to do so, even if no transaction takes place, if they consider that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, or financing terrorism.
- The business must consider whether it needs to seek a defence to a money laundering or terrorist financing offence (consent) from the NCA before proceeding with a suspicious transaction or entering into arrangements.
- It is a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place.

5.2 Actions required:

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

Suspicious activity reports (SAR)

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

5.4 The suspicion is that the funds or property involved in the transaction is the proceeds of any crime or is linked to 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 seller or buyer, will be relevant.

5.5 As an estate agency business in the regulated sector, you are also required to make a Suspicious Activity Report (SAR) as soon as possible after you know or suspect that money laundering or terrorist financing is happening. This means that the facts you have about the seller and buyer 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 regulated sector in the How to report SARs section of the NCA website. The NCA document "Guidance on Submitting Better Quality SARs" takes you through the information you should provide and the SAR glossary codes you should use.

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

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

The NCA also issues report forms for you to fill in but you will not receive an acknowledgement of a report sent this way.

For help in submitting a report or with online reporting to the NCA contact the UK Financial Intelligence Unit (UK FIU) helpdesk - Telephone: 020 7238 8282 or online at NCA.

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

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

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

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

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

Nominated officer

5.12 You must appoint a nominated officer to make reports (see suspicious activity reports) from within your registered business. The nominated officer (or a deputy) must make a report if they know or suspect that someone is involved in money laundering or terrorist financing.

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

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

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

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

A defence (consent)

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

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

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

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.

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

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

- You only receive a defence to the extent to which you ask for it. So you should clearly outline all the aspects of the transaction that could be affected. For example: 'We seek a defence to finalise an agreement for sale of property X and to then transfer property X into the name of (purchaser) and following payment of disbursements, pay the proceeds of the sale of the property to (seller)'.
- you can't ask for a general defence to trade with a person, only to carry out a particular transaction
- The initial notice period is 7 working days from the day after the SAR is submitted. If a defence is refused, the moratorium period is a further 31 calendar days from the date of refusal. If you need a defence sooner, you should clearly state the reasons for the urgency and perhaps contact the NCA to discuss the situation.
- The NCA will contact you and confirm in writing or by email.

Tipping off

5.21 It is a criminal offence for anyone to say or do anything that may 'tip off' another person that a suspicion has been raised, or that a money laundering or terrorist financing investigation may be carried out. It is also an offence to falsify, conceal or destroy documents relevant to investigations.

5.22 Nobody should tell or inform the person involved in the transaction or anyone else that:

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

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

Example of when you may consider making a SAR

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

- checking the seller or buyers identity is difficult
- the seller or buyer is reluctant to provide details of their identity or provides documents which may be fake
- the seller or buyer 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
- no apparent reason for using your business's services - for example, another business is better placed to handle the transaction
- 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
- they are keen to buy or sell quickly at an unusually low or high price for no legitimate reasons
- part or full settlement in cash or foreign currency, with weak reasons
- they, or associates, are subject to, for example, adverse media attention, have been disqualified as directors or have convictions for dishonesty.

Regular and existing customers

5.24 These are some of the questions 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 the customer cannot give a proper explanation of where money came from or their source of wealth or funds.

Transactions

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

- a third party, apparently unconnected with the seller or buyer, bears the costs, or otherwise pays the transaction costs
- an unusually big cash or foreign currency transaction
- the buyer will not disclose the source of the funds or the seller 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
- unusual source of funds.

6 Record keeping

Core obligations

6.1 You must retain:

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

6.2 You must also maintain:

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

Actions required

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

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

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

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

6.5 The records should be reviewed periodically to ensure, for example, that a fresh copy of expired documents is held. After the period above the records can be deleted unless you are required to keep them in relation to legal or court proceedings. You will not be required to keep them for more than twenty five years.

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

This evidence may be used in court proceedings.

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

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

7. Staff awareness

Core obligations

7.1 You must:

- ensure relevant staff are aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation, know who the nominated officer is and what his responsibilities are, 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 and the training given to staff
- ensure that a relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements.

Larger and more complex businesses must:

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

Actions required

7.2 The points below are to be kept under regular review:

- provide appropriate training to make relevant staff aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the business
- ensure that relevant employees have information on, and understand, the legal position of the business - individual members of staff and any changes to these positions
- regularly share risk assessment, policy, control and procedures information within the business and with branches and subsidiaries
- consider providing relevant staff with case studies and examples related to the firm's business
- train relevant staff in how to operate a risk based approach to assessing the risks of money laundering and terrorist financing
- set up a system to screen staff before they take up the post
- keep records of training given.

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

- tell your staff about your anti money laundering and counter terrorism financing obligations
- give them suitable (risk based) training on their legal obligations
- tell them how to identify and deal with the risks.

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.

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

Training

7.4 When you consider who needs to be trained you should include staff who deal with your customers, deal with money or help with compliance. Think about reception staff, administration staff and finance staff, because they'll each have a different involvement in compliance, and have different training needs.
The training process should therefore cover the whole end to end process from sales and receiving customers' instructions, through to valuation, dealing with offers and completion.

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

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

7.7 It should cover:

- the staff member's duties
- the risks posed to the business
- the business policies and procedures
- how to conduct customer due diligence and check sellers and buyer's documents
- how to spot and deal with suspicious persons and activity
- how to make internal reports, including disclosures of suspicious activity
- data protection requirements
- record keeping
- the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the

Payer) Regulations 2017; Part 7 of the Proceeds of Crime Act; and sections 18 and 21A of the Terrorism Act.

7.8 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.

7.9 A policy manual is useful to raise staff awareness and for reference between training sessions.

Staff training is necessary when staff join the business, move to a new job or when they change roles. They should also have ongoing training at least every 2 years or when a significant change happens, depending on the level of risks.

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

Training records include:

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

8. Estate Agency Business risk

8.1 An estate agency business in a metropolitan area with an international clientele presents a completely different risk profile to a high street business in a small market town. However, both may be targeted by criminals if they have little or no controls in place.

The environment you do business in affects the individual customer's risk assessment, if you have many high net-worth customers or deal with people from a particular country or region, this will influence the business wide assessment.

You should be aware of the risk of transactions being used for tax evasion, for example when property prices are manipulated 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 are intended to avoid Inheritance Tax. It's good policy to ask to see the tax advice that has prompted such a transaction.

8.2 Other areas of particular concern are:

- estate agency staff being offered bribes, for example in relation to valuations or planning applications
- where the source of funds may be a result of mortgage fraud by a seller or buyer or mortgage broker
- landlords not complying with their legal obligations
- 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 properties they have rented or persons selling properties they do not own.

8.3 The seller or buyer can also pose a risk in the following ways:

- how the person comes to the business, for example non face to face customers, occasional transactions, the pattern of behaviour and any changes to it and corporate customers, partnerships, or trusts
- if you undertake business in areas with a highly transient population
- the customer base may be unstable or have a high turnover
- where you act for international customers or customers you do not meet
- if you accept business from abroad, particularly tax havens, high risk third countries or countries with high levels of corruption, or where terrorist organisations operate

- where you act for entities that have a complex ownership structure or a cross border element
- payments that are made to or received from third parties or from overseas accounts.

Identifying a seller, buyer or transaction as high risk doesn't 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're not involved in money laundering or terrorist financing.

Identifying suspicious activity

8.4 Here are some warning signs of potentially suspicious activity. This is not a complete list and these signs aren't always suspicious. It depends on the circumstances of each case.

8.5 New or existing sellers and buyers:

- 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
- seller, buyer or professionals being evasive or reluctant to provide required CDD 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 cash exchanges directly between seller and buyer - perhaps including cash deposit
- poor explanation for the early redemption of a previous mortgage, especially where redemption incurs a penalty cost
- the customer or other party 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 buyer 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

- reluctance to employ a solicitor or other professional for conveyancing.

8.6 How a transaction is carried out or requests made by a seller or buyer 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 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 price significantly above or below market price
- the use of property management or investments companies who may not trade to make ownership less transparent
- an unknown third party appears at a late stage
- use of correspondent banking services where due diligence is less robust
- unusual speed or requests to expedite transactions unnecessarily possibly over or under value
- a sudden or unexplained change in ownership
- the immediate resale (flipping) of property at a higher value
- a third party, apparently unconnected with the seller or buyer, 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.

9. Estate agents and property professionals

9.1 Anyone who engages in estate agency work must comply with the Regulations. HMRC supervise Estate Agency Businesses under these Regulations. A business must not carry on estate agency business unless they are registered with HMRC.

9.2 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). Since 1 October 2012, the definition has included estate agents based in the UK who deal with overseas property, either exclusively or alongside other property services. It can also cover estate agents based abroad if they are doing business within the UK.

9.3 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.

Estate agency work

9.4 Under Section 1 of the Estate Agents Act 1979 estate agency work includes introducing/negotiating with people who want to buy or sell freehold or leasehold property (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 customer

9.5 This definition includes:

- 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
- letting or property management agents that offer estate agency services to landlord customers

- construction companies (house builders) with a sales office at a construction site, to the extent that they offer additional estate agency services beyond the sale of their own constructed or bought units
- in Scotland, a solicitors' property centre.

Exclusions

9.6 The definition of estate agency doesn't 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, which merely provide a platform for private sellers to advertise their properties and provide a means for sellers and buyers to contact and communicate with one another - this exemption applies only if you do nothing else covered by the general definition of estate agency work
- practising solicitors who carry out estate agency work as part of their role as a solicitor.

However, if a solicitor has a separate business which provides estate agency services, they will fall within the definition of an estate agent and must register with HMRC.

Letting agents

9.7 The Money Laundering Regulations don't cover letting agents or property management agents, unless they carry out estate agency work. For example, lettings agents who undertake the sale of leases for a premium (where the bulk of the rent is paid up front) fall within the definition of estate agency.

They still have to comply with the money laundering provisions of the Proceeds of Crime Act 2002, including the reporting duties of any nominated officer you may have appointed.

Estate agents' employees and the Regulations

9.8 Employees of estate agents who carry out estate agency work are not themselves individually supervised by HMRC. However, their employers will be responsible for their compliance with the Regulations.

Franchise business models

9.9 Franchise business models operate in the estate agency business sector. These 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.

9.10 Where a franchise agreement provides that a franchisee has substantial independence from the franchisor, 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 simply 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.

9.11 The same criteria will apply to local representatives of online estate agents who are carrying out their activities in the course of business.

9.12 The franchisor, where it is not merely the brand holder, must also ensure that they register if they are carrying out estate agency work.

10. More information

10.1 You can contact HMRC by:

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

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

Propertymark
Royal Institution of Chartered Surveyors
Association of Relocation Professionals
The Association of Residential Managing Agents
The Joint Money Laundering Steering Group

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

National Trading Standards Estate Agency Team