Money Laundering Regulations 2007: supervision of Estate Agency Businesses

Contents

1. Money laundering and Estate Agency Businesses
2. Responsibilities of senior managers
3. Policies and procedures
4. Customer due diligence
5. Reporting suspicious activity
6. Record keeping
7. Staff awareness
8. Estate agents and property professionals
9. More information

1. Money laundering and Estate Agency Businesses

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 and selling it on, giving the criminal an apparently legitimate source of funds
- criminals may also hide behind complex company structures and multiple accounts to disguise the real purpose of a transaction and hide its beneficial ownership
- a more direct method may involve paying an estate agent or auctioneer a big deposit and reclaiming it later
- the money for a purchase may be the result of mortgage fraud

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.

Terrorist financing

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

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

- Proceeds of Crime Act 2002
- Terrorism Act 2000

- Money Laundering Regulations 2007

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.

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 businesses in the regulated sector, such as estate agents. This obligation extends across the whole business, so an Estate Agency Business which also does lettings must also submit suspicious activity reports for its lettings.

The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses, like estate agents, 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

The Money Laundering Regulations set out what relevant businesses like estate agents, must do to prevent their services being used for money laundering or terrorist financing purposes. This guidance focuses on the Money Laundering

Joint Money Laundering Steering Group publishes more information about businesses' obligations under the other relevant legislation.

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 on business as an estate agent unless they register with HM Revenue and Customs (HMRC).

This is explained in more detail later in this guide.

Penalties

If a person fails to comply with the regulations, they may face a civil or criminal prosecution. This could result in unlimited fines and/or a prison term of up to two years, or civil financial penalties.

2. Responsibilities of senior managers

Senior managers are personally liable if they don’t do everything they need to do to protect their business from money laundering and terrorist financing.

You’re a senior manager if you’re a director, manager, secretary, chief executive, member of the management committee or someone who carries out those functions, or any partner in a partnership or a sole proprietor.

<table>
<tr><td>

Senior managers core obligations

They must:

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

</td></tr>
<tr><td>

Action required:

- carry out a risk assessment identifying where their business is vulnerable to money laundering and terrorist financing
- prepare a policy statement and procedures to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments
- make sure there are enough trained people equipped to implement the policy adequately, and systems to help them
- monitor effectiveness and make improvements where required

</td></tr>
</table>

Your responsibilities

Senior managers are responsible for making sure that the business has risk based policies and procedures to help reduce the risk that criminals may exploit the business for financial crime. Your policies and procedures must address the level of risk that the business may encounter in different circumstances (see the section on policies and procedures). When higher risks are identified, you must take extra

measures (see the section on customer due diligence), and consider whether to report suspicious activity (see the section on reporting suspicious activity).

Policy statement

Your policy statement should make clear how you'll prevent money laundering and terrorist financing, by setting down your policies and procedures in writing.

Your policy will explain how you and the senior managers will assess risks to the business, notably how you and they will:

- identify, monitor and mitigate the risks of the business being used for money laundering or terrorist financing
- assign responsibilities to specific individuals and functions
- undertake due diligence checks and ongoing monitoring
- appoint a nominated officer or money laundering reporting officer to report suspicious activity to senior managers and the National Crime Agency (NCA)
- make sure the staff are trained to recognise risks and understand what they need to do, including the importance of reporting suspicious activity to the nominated officer
- maintain accurate, up to date record keeping and retention of records

The policy statement of a larger business should also have in it:

- a senior staff member taking responsibility for monitoring the effectiveness of the policy, including regular reviews to learn from experience
- individual staff responsibilities under the regulations
- training
- review and updating of policies and procedures
- auditing compliance with procedures
- the names of the nominated officer and any deputy

Appointing a nominated officer

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

You should make sure that your staff know the name of the nominated officer and receive training on when and how to report their suspicions to the nominated officer (see section on reporting suspicious activity).

Personal liability

You'll be committing a crime, if you don't comply with the regulations.
You may incur an unlimited fine and/or a prison term of up to two years if:

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

3. Policies and procedures

Senior managers core obligations

The senior managers must put in place appropriate policies and procedures that reflect the degree of risk associated with the business and its customers. These are:

- customer due diligence measures and ongoing monitoring
- reporting suspicious activity
- record keeping
- internal controls
- risk assessment and management
- monitoring and managing compliance
- the internal communication of these policies and procedures

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, product or transaction.

Action required

The points below are to be kept under regular review:

- carry out a formal, regular assessment of money laundering/terrorist financing risks, including market changes and changes in products, customers and the wider environment
- ensure internal procedures, systems and controls, including staff awareness, adequately reflect the risk assessment
- ensure customer identification and acceptance procedures reflect the risk characteristics of customers
- take further measures for higher risk situations
- ensure arrangements for monitoring systems and controls are robust and reflect the risk characteristics of customers
- carry out regular assessments of your systems and internal controls to make sure they are working

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

Risk based approach

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.

You'll need to:

- identify the risks of money laundering and terrorist financing that are relevant to your business, in other words, your business's risk profile
- assess the risks posed by your particular customers and any underlying beneficial owners (see the section on customer due diligence on who is a beneficial owner), services, financing methods, delivery channels and geographical areas of operation, including the location of the vendor, buyer, the property and the source of funds
- design and implement controls to mitigate these assessed risks
- monitor the effectiveness and implementation of the controls and make improvements where required
- record what has been done and why

Your risk profile

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

It's unlikely that a high street Estate Agency Business in a small market town will come across customers involved in terrorist financing. Customers may be more

likely to be evading tax or re-investing the proceeds of crime like fraud or theft to some extent.

A business in a metropolitan area with an international clientele presents a completely different risk profile. While this affects the individual customer's risk assessment, if you have many high net-worth customers or customers from a particular country or region, this will influence the business wide assessment.

In particular you should deal with 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.

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 customer 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
- passing off stolen property at auctions

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

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

The customer can also pose a risk in the following ways:

- how the customer 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, 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

Procedures and controls

Once you've identified and assessed the risks, you must ensure that you put in place appropriate procedures and controls to reduce these risks.

Procedures should also be easily accessible to staff and detailed enough to allow staff to understand and follow them easily. They should cover:

- the types of customers and transactions that you consider to be lower risk and qualify for simplified due diligence and those that are higher risk and merit closer scrutiny
- how to do customer due diligence, the identification of requirements for customers and beneficial owners, and how to do enhanced due diligence on higher risk customers
- any other patterns or activities that may show 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 NCA

Examples of risk based controls include:

- introducing a customer identification and verification programme that varies depending on the assessed level of risk
- requiring additional customer identity evidence in higher risk situations
- varying the level of monitoring of customer transactions and activities, depending on the assessed level of risk or activities that might be unusual or suspicious

This list is not exhaustive. You could also have other risk based controls, for more guidance go to the section on customer due diligence.

Identifying a customer or transaction as high risk doesn’t automatically mean that they are involved in money laundering or terrorist financing. Similarly, identifying a customer or transaction as low risk does not mean that they’re not involved in money laundering or terrorist financing.

Identifying suspicious activity

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.

New customers:

- checking the customer's identity is difficult
- the customer is reluctant to provide details of their identity or provides fake documents
- the customer is trying to use intermediaries to protect their identity or hide their involvement
- no apparent reason for using your business's services - for example, another business is better placed to handle the 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
- the property value doesn't fit the customer's profile
- the customer 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

Regular and existing customers:

- the transaction is different from the normal business of the customer
- the size and frequency of the transaction is different from the customer's normal pattern

- the pattern has changed since the business relationship was established
- there has been a significant or unexpected improvement in the customer's financial position
- the customer can't give a proper explanation of where money came from

Transactions:

- a property has multiple owners or is owned by nominee companies
- sale price significantly above or below market price
- an unknown third party appears at a late stage
- unusual speed or requests to expedite transactions unnecessarily
- a sudden or unexplained change in ownership
- the immediate resale (flipping) of property at a higher value
- a third party, apparently unconnected with the customer, 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 customer 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
- 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

Effectiveness of the controls

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

You should 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.

4. Customer due diligence

Core obligations

You must:

- do customer due diligence for all customers
- have systems to identify those who can't produce standard documents
- apply enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, specifically when the customer isn't physically present when being identified, and in respect of politically exposed persons
- not deal with certain persons or entities if you can't do due diligence, or the results aren't satisfactory
- have a system for keeping customer information up to date

The customer is the person or entity with whom the estate agency business forms a contractual relationship, often referred to as the client. For sales agents, it's usually the vendor, although in repossession it may be the lender. For buying agents, the customer is the buyer.

You must check that customers are who they say they are. This is often referred to as 'know your customer', or exercising customer due diligence. You must do customer due diligence on all customers, even if you knew them before they became your customers. This is because you must be able to show that you know all your customers.

Your business must undertake customer due diligence when:

- establishing a business relationship
- carrying out an occasional transaction, such as an auction
- it suspects money laundering or terrorist financing
- it suspects that information obtained for due diligence checks on a customer is not reliable or adequate

Customer due diligence means:

- identifying customers and verifying their identity (more details below)
- identifying the beneficial owner, where applicable, and taking adequate risk based measures to verify their identity
- obtaining information on the purpose and intended nature of the business relationship
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the customer's risk profile
- maintain records of these checks

Extent of customer due diligence

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

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

Timing

A customer's identity and where applicable the identity of a beneficial owner, should be verified before entering into a business relationship or occasional transaction.

You can make an exception to this practice only if both the following apply:

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

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

However, this exception doesn’t mean you can use it where it’s hard to verify a customer’s or beneficial owner’s identity.

Non-compliance

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

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

You must:

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

Business relationship

A business relationship is a business, professional or commercial relationship between an Estate Agency Business and a customer. The business will expect, on establishing the contact, the relationship to have an element of duration. The latest point at which you form a business relationship is when you agree a contract with the customer, either formally or informally.

Occasional transactions

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

The value of the transaction here means the gross value of the property transaction, not the value of your fees.

Politically exposed persons

Typically, a politically exposed person is one of the following:

- an overseas member of parliament
- a head of state or government
- a government minister and their relatives

A UK politician isn’t a politically exposed person.

Beneficial owners

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 relocation services
- a co-owner of a property who is not your customer

For a corporate body or partnership, a beneficial owner is any individual who:

- owns or controls over 25% of the shares or voting rights or in the case of a partnership, more than 25% of the capital or profits of the partnership
- exercises control over the management

For a trust, a beneficial owner includes:

- individuals with interests in 25% or more of the capital of the trust property
- individuals who exercise control over the trust
- the class of individuals that the trust acts for (for example 'homeless persons in London', 'deaf and blind persons', 'children living in the village of Ambridge' or 'someone’s children and grandchildren')

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

- individuals who benefit from 25% or more of the entity's property
- individuals who exercise control over 25% or more of the entity's property
- the class of individuals the entity acts for

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

In a sub-agency arrangement the beneficial owner is the vendor customer or, for relocation sub agents, the purchaser customer of the principal agent. Due diligence must be done accordingly.

If the sub-agent has contact with the principal agent's customer, the sub-agent may have to carry out 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.

Simplified due diligence

Sometimes your business may apply a simplified form of due diligence measures. In this case, you don't have to verify a customer's identity, nor a beneficial owner's identity. Also you don't need to ask for additional information about the nature or purpose of a business relationship.

Simplified due diligence applies if the customer is:

- a public authority in the UK
- a financial institution that is itself subject to Anti Money Laundering Supervision or equivalent regulation in another country

- situated outside the UK and is subject to equivalent Anti Money Laundering Supervision 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
- the customer is a European Community institution

You'll need to have evidence that a customer or service provided is eligible for simplified due diligence. You'll also need to conduct ongoing monitoring in line with your risk assessment.

You always need to conduct customer due diligence and ongoing monitoring if you suspect money laundering or terrorist financing.

Enhanced due diligence

This means that you may need to undertake further measures to assess the risks posed by certain transactions or customers.

You must do this when:

- a customer isn't physically present for identification face to face
- a customer is a politically exposed person, or an immediate family member or a close associate of a politically exposed person
- the nature of a particular situation can present a higher risk of money laundering or terrorist financing

Non face to face customers

If you can't identify a customer face to face, then you must do more due diligence to check their identity, for example:

- obtain additional information or evidence to establish the customer's identity

- take additional measures to verify the documents supplied, or require certification by a bank, financial institution, lawyer or notary
- ensure the first payment is made through a bank account in the customer's name

Identifying private individuals

You must obtain a private individual's full name and residential addresses.

If you verify the customer's identity by documents, you must see the originals and not accept photocopies, unless validated as described below, nor accept downloads of bills for example.

You should verify these using a government issued document with the customer's full name and photo, with either the customer's date of birth or residential address such as:

- a valid passport
- a valid photo card driving licence
- a national identity card
- a firearms certificate
- an identity card issued by the Electoral Office for Northern Ireland

Where the customer doesn't have one of the above documents, or the customer doesn't meet the criteria in your risk assessment, you may wish to ask for the following:

- a government issued document (without a photo) which includes the customer's full name and also secondary evidence of the customer's address, for example an old style driving licence or recent evidence of entitlement to state or local authority funded benefit such as housing benefit, council tax benefit, pension, tax credit

- secondary evidence of the customer’s address, not downloaded from the internet, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement

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

- spellings
- validity
- photo likeness
- whether addresses match

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

If you verify an individual’s identity electronically, you should do so from two separate online sources or use a service provider that does so. This check must use data from multiple sources collected over a period of time or incorporate checks that assess the strength of the information supplied. An electronic check from a single source (for example, a single check against the electoral roll) isn’t enough on its own to provide satisfactory evidence of identity.

An electronic records check establishes that an individual exists, not that your customer is that individual. You should therefore verify key facts that only the customer may know to establish who they say they are. For example, their place of birth, or how long they have been resident at an address.

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.

Individuals not resident in the UK

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. You can get the customer's address from:

- an official overseas source, such as an electoral register
- a recognised, well established directory
- a person regulated for money laundering purposes in the country where the person is resident, who confirms that they know the individual and confirms that the individual lives or works at the overseas address given

Where appropriate you can also accept written assurances from reputable persons or organisations that have dealt with the customer for some time.

If documents are in a foreign language, you must satisfy yourself that they do in fact provide evidence of the customer's identity.

Identifying organisations as customers

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

- the full name of the company
- registration number
- registered address
- country of incorporation

It will also be necessary to establish the beneficial owners of such entities.

Also for private or unlisted companies you must obtain the names of all directors (or equivalent), 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 verify the identity through reliable, independent sources that are relevant to that type of entity. For example:

- searching a relevant company registry
- confirming a company's listing on a regulated market
- obtaining a copy of the company's certificate of incorporation

You must also obtain evidence that individuals have the authority to act for that entity.

Beneficial owners

You must identify the existence of a beneficial owner and understand how they operate (the section on customer due diligence gives information on who is a beneficial owner). If you suspect or have identified that a beneficial owner controls or owns the customer, you should verify the beneficial owner's identity.

Where your customer is a private individual fronting for another individual who is the beneficial owner, you should obtain the same information about that beneficial owner as you would for the customer. You must verify the identity of a beneficial owner taking account of the level of risk associated with your business relationship with the customer. You should use any available public records of beneficial owners such as company registers, or ask the customer for relevant information. You should also ask for evidence of the beneficial owner’s identity based on documents, data or information obtained from a reliable and independent source or obtain the information in some other way.

Reliance on third parties

You must do due diligence before entering into a business relationship with a customer. As estate agents are usually the first professional to be instructed by a vendor or purchaser, 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 aren’t employed until the business relationship has got underway.

However, you can rely on certain regulated people to apply customer due diligence for you before entering into a business relationship with a customer on the conditions that they agree that you will rely on them, and they agree to provide you with the customer due diligence material if requested. The people you can rely on include:

- auditors
- insolvency practitioners
- external accountants
- tax advisers
- independent legal professionals
- authorised credit institutions
- financial institutions (excluding a Money Service Business)

If you rely on a third party you'll remain responsible for any failure to apply due diligence measures appropriately. You should ask what due diligence and other enquiries have been undertaken to ensure that they actually comply with the regulations. 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 due diligence checks and you should consider reliance as a risk in itself.

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

Reliance doesn't include accepting information from others to verify a client's identity for your own due diligence obligations, nor electronic verification, which constitutes outsourcing a service.

You mustn't 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.

Estate agents and property professionals cannot be relied upon by others for the purposes of customer due diligence.

5. Reporting suspicious activity

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 terrorist property exists. • The business's nominated officer must consider all internal reports. The Officer must make a report to the NCA as soon as it's feasible 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 seek consent from the NCA before proceeding with a suspicious transaction or entering into arrangements. • It's a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place.
Actions required: • enquiries made in respect of internal reports must be recorded • the reasons why a report was, or was not, submitted should be recorded • keep a record of any communications to or from the NCA about a suspicious transaction report

A suspicious activity report

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 terrorists. The term suspicion is meant to be applied in its everyday, normal sense. But if you're still not sure of the meaning of suspicious, then the courts have said that 'it is a possibility that is more than fanciful'.

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

As an estate agent in the regulated sector, you're also required to make a report if you have reasonable grounds for suspecting money laundering. This means that the facts you have about the customer and the transaction would cause a reasonable property professional in your position to have a suspicion.

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.

You must appoint a nominated officer to make reports. 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.

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

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

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

If a report is completed after a transaction has taken place, you'll be able to continue to do business with the customer subject to risk assessment procedures.

If a report is done before a completed transaction or the start of a business relationship, you must ask for the consent of the NCA to go ahead with the transaction. You should mark the report with 'CONSENT' and 'TRANSACTION NOT COMPLETE'. If urgent you can telephone the NCA to request consent.

Consent

It’s an offence for the nominated officer or sole trader to proceed with a transaction if the nominated officer or sole trader has asked for consent, but has not received it within 7 working days. This period starts from the day after submitting the report.

If you don’t get a response from the NCA after 7 working days, you can carry on with the transaction. If the agency refuses consent, you must not proceed with a transaction for up to a further 31 calendar days.

The NCA has published information on obtaining consent. Some of the key points include:

1. You only receive consent 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 consent 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)'.
2. The initial notice period is 7 working days from the date of the report. If consent is refused, the moratorium period is a further 31 calendar days from the date of refusal. If you need consent sooner, you should clearly state the reasons for the urgency and perhaps contact the NCA to discuss the situation. The agency can sometimes give consent in hours.
3. The NCA will contact you by telephone to notify you and will confirm in writing.

Receiving consent or no response from the NCA doesn’t mean you don’t have to verify a customer’s identity or that of any beneficial owners. The business must continue to comply with all the requirements of the regulations.

Making a report

You should make a report as soon as possible after you know or suspect that money laundering or terrorist financing is happening.

There is guidance about submitting a Suspicious Activity Report (SAR) within the regulated sector in the publications section of the NCA website.

The NCA has a secure, encrypted system for submitting reports. The NCA will provide information and registration details that lets you:

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

You can submit reports online and the NCA prefers this method. The main benefit of this is that you get an instant confirmation and reference number.
The system doesn't retain a file copy for your use, so you should keep a copy of your report.

Forms

The NCA issues report forms for you to fill in and send to:

UK FIU
PO Box 8000
London
SE11 5EN
(You will not receive an acknowledgement of a report sent this way)
Fax: 020 7238 8256

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

Tipping off

It’s 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 investigation may be carried out. It’s also an offence to falsify, conceal or destroy documents relevant to investigations.

Nobody may tell the customer 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 year’s imprisonment and/or a fine.

6. Record keeping

<table>
<tr><td>

Core obligations

You must retain:

- copies of, or references to, the evidence obtained of a customer's identity for five years after the end of the business relationship
- details of customer 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 an external report

</td></tr>
<tr><td>

Actions required

The points below are to be kept under regular review:

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

</td></tr>
</table>

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

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

You must also keep records of suspicious activity reports and any other internal or external reports and decisions.

You can keep records as original documents and photocopies of original documents in either computerised 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 against the criminals.

If someone else carries out customer due diligence for you, you must make sure that they also comply with these record keeping requirements.

7. Staff awareness

<table>
<tr><td>

Core obligations

You must:

- ensure relevant staff are aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation, know who the nominated officer is and what his responsibilities are, train in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity
- staff are trained at regular intervals, and record the details

The relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements.
</td></tr>
<tr><td>

Actions required

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
- 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
</td></tr>
</table>

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

Training

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.

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.

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.

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 customers' documents
- how to spot and deal with suspicious customers and activity
- how to make internal reports, including disclosures of suspicious activity
- record keeping
- the Money Laundering Regulations 2007; Part 7 of the Proceeds of Crime Act; and sections 18 and 21A of the Terrorism Act

Training may include:

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

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, depending on the level of risks.

You should think about keeping evidence of your assessment of training needs and the steps you've taken to meet those needs. For example, 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 or electronic training records
- an updated training schedule

8. Estate agents and property professionals

Anyone who engages in estate agency work must comply with the Money Laundering Regulations. HMRC supervise Estate Agency Businesses under these regulations. A person may not carry on estate agency business unless they register with HMRC.

The Money Laundering 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.

Estate agency work

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

This definition includes:

- high street 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 offices 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

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

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 Money Laundering Regulations 2007

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.

9. More information

You can contact HMRC by:

Telephone: 0300 200 3700.

Email: mlrcit@hmrc.gsi.gov.uk

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

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