Ascend

# ANTI-MONEY LAUNDERING

# POLICY & PROCEDURE MANUAL

The author of this document FCS Compliance Ltd. has used its best endeavours to ensure the accuracy of the information and is not liable for any error, omission or the consequences of reliance upon the same by any party under any circumstances, including any loss or damage flowing from the effecting of this manual or Procedures. It is for each individual in this company to ensure that they are fully conversant with the law (i.e. the current legislation and Regulations and any common law) and is acting in compliance with that law. This manual is intended merely as a guide to AML Policies & Procedures of this Company.

This Company therefore actively encourages all of its staff to familiarise themselves with all the primary sources of law, including the Proceeds of Crime Act 2002 (as amended), Bribery Act 2010, Terrorism Act 2000 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. This manual or extracts from it may not be copied or circulated without the express permission of its author FCS Compliance Ltd.

**Published April 2024**

FCSCOMPLIANCE

# Chapter 1 – ABOUT THE MANUAL

## Purpose

The purpose of this document is to provide detailed procedures to ensure 'Ascend Estates Limited' is able to meet its legal obligation to deter, detect and disrupt money laundering or terrorist financing. The document:

- Outlines the legislation in respect of anti-money laundering (AML) or terrorist financing measures
- Explains the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and how these should be applied in practice [hereafter referred to as the "Regulations"]
- Gives details of the systems and controls necessary to lower the risk of our company being used by criminals to launder money.

## How to use it

All relevant employees upon joining the company must read and understand this 'Policy & Procedure' manual and refer to it when necessary. It is not designed to cover every eventuality but sets out the broad principles within which all relevant staff are expected to work.

## Responsibility

It is the responsibility of the Nominated Officer or Senior Manager of the company to maintain the manual and ensure it is kept up to date. However, it is the responsibility of all staff to request any amendments that appear to be required. Any such request should be forwarded to the Nominated Officer. In addition, all staff will receive the appropriate training on a regular basis in order to be updated of recent developments and trends in relation to AML.

## Distribution

An electronic copy of this 'Policy and Procedure Manual' will be retained by the Nominated Officer of the company and will be stored on the company's computer server and be easily accessible to all members of staff for reference. The manual will be replaced each time a new version is produced.

## Queries

Any queries as regards to the content of the manual should be addressed to the Nominated Officer. If the Nominated Officer is unable to provide an answer or explanation to the query they will seek advice from the appropriate person or body that has responsibility for the regulation of anti-money laundering issues such as HMRC, National Crime Agency or the external AML Consultancy company 'FCS Compliance Ltd'.

## Updates and amendments

The manual will be reviewed on a regular basis, at least annually and more often if warranted, such as changes in legislation, and the development of international standards. Any required updates and amendments will be prepared in conjunction by 'FCS Compliance Ltd' and approved by the Nominated Officer or Senior Manager of the company if that is not the same person. The amendments shall thereafter be incorporated into the manual and a revised copy e-mailed to all staff by the Nominated Officer. The cover e-mail will advise staff of the changes that have been made.

# Chapter 2 – ABOUT US

## Company Structure

Ascend Estates Limited was established in 2014 as an independent estate agency specialising in the sale and lettings of residential property, registered at office address Stafford Court, 145 Washway Road, Sale, M33 7PE, and trading from 6 offices located across Manchester, Leeds, Liverpool, and Wolverhampton. The company aims to market and sell property located across the whole of the UK, and currently employs 6 members of staff on the sales side of the business, 15 members of staff on the lettings side, and 76 members of staff in in office based administration. The company is registered with HMRC the Supervisor for Estate Agents for AML purposes, and is also registered with Propertymark NAEA (National Association of Estate Agents), ARLA Propertymark (Association of Registered Letting Agents), and the National Crime Agency (NCA) for the filing of Suspicious Activity Reports.

The company deals with a broad range of properties achieving prices up to £1,075,000 with the average value being in the region of £237,000. Although the company does operate a lettings department, it is yet to engage in a lettings transaction that exceeds the threshold of 10,000 Euros pcm (or its equivalent currency), where upon the transaction would fall within the scope of the Money Laundering Regulations (amendment) 2019 and any business relationship would be subject to the Money Laundering Regulations 2017 (”Regulations”). Nevertheless, the company remains cognisant of these requirements should it engage in a lettings transaction that does achieve this threshold.

Ascend Estates Limited has dealt with a number of clients that were foreign nationals. The company has had exposure to UK and overseas companies as customers, but has not had exposure to Trusts. To the best of its knowledge the company has not identified and individuals that would be classed as a ‘Politically Exposed Person’.

The company advertises the sale of property through its website www.ascendproperties.com, and it also uses online sales platforms to advertise property.

# Chapter 3 – MONEY LAUNDERING & REAL ESTATE

## Real Estate Introduction

The UK continues to comply with the 4th and 5th EU Anti-Money Laundering Directives (5AMLD) which were implemented in the UK in January 2020. The company recognizes its obligations under the applicable UK Anti-Money Laundering and Counter Terrorist Financing legislation and is committed to complying fully with those obligations. The UK Government has offered guidance specifically for Estate Agency Businesses which is approved by His Majesty's Treasury (HMT) which was updated in July 2023.

Real estate itself provides a means to launder and conceal ill-gotten gains while providing a layer of anonymity to individuals. Criminals can invest their monies into a legitimate asset that has the potential to appreciate over time while providing a means to generate income and liquidate into cash at a later stage. In addition, fluctuations in real estate market values vary by region and numerous factors impact property values making it easier to manipulate and difficult to monitor criminal mischief.

Latest estimates state that real estate in the UK valued at approximately £170 billion is held by more than 30,000 tax haven companies, and about £4.2 billion of property has been bought by public officials and politicians with suspicious wealth, of which 1,000 are 'Politically Exposed Persons' [1]. It is estimated UK real estate has long been a haven for investors seeking a stable political and business climate, and generally sound returns on their investment. The issue of identifying and dealing with persons who are classed as PEPs are explained in greater depth in this manual.

The UK National AML Risk Assessment published in December 2020 by the Home Office[2] stated that the abuse of property for money laundering purposes is now deemed as a HIGH risk and significantly the services of estate agents as a MEDIUM risk. The risk rating for both property itself and agents has been increased since the previous Risk Assessment in 2017 and this an indication of the attraction that real estate presents to those seeking to launder criminal proceeds due to its value. Therefore it is essential that real estate companies and professionals

1 https://www.transparency.org.uk/publications/faulty-towers-understanding-the-impact-of-overseas-corruption-on-the-london-property-market.

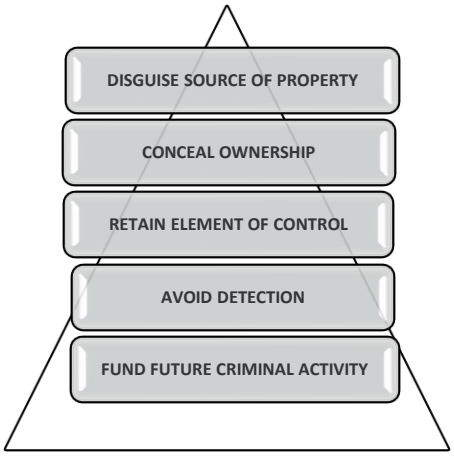
2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf

are aware of their duties and legal obligations to prevent them being concerned with this type of criminal activity.

## What is money laundering

Money laundering is the process by which criminals attempt to hide and disguise their criminally derived funds or assets to avoid detection, prosecution and confiscation. It is important to remember that despite its title money laundering is not restricted to money and can include property such as real estate, motor vehicles etc

## The five main objectives of money laundering or terrorist financing




## The need to prevent money laundering

Money laundering has potentially devastating economic, security, and social consequences. It provides the fuel for drug dealers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. If a company or an employee of the company is concerned with the laundering of criminal property it can have severe repercussions for the individual as well as the company including: -

- Criminal prosecution being brought against the individual, resulting upon conviction of imprisonment, a fine, or both
- Regulatory action taken against the company resulting in a financial penalty
- Defending a lengthy and complex civil action that will involve costly legal fees
- Reputational damage arising out of any criminal or civil action that could lead to loss of clients etc.

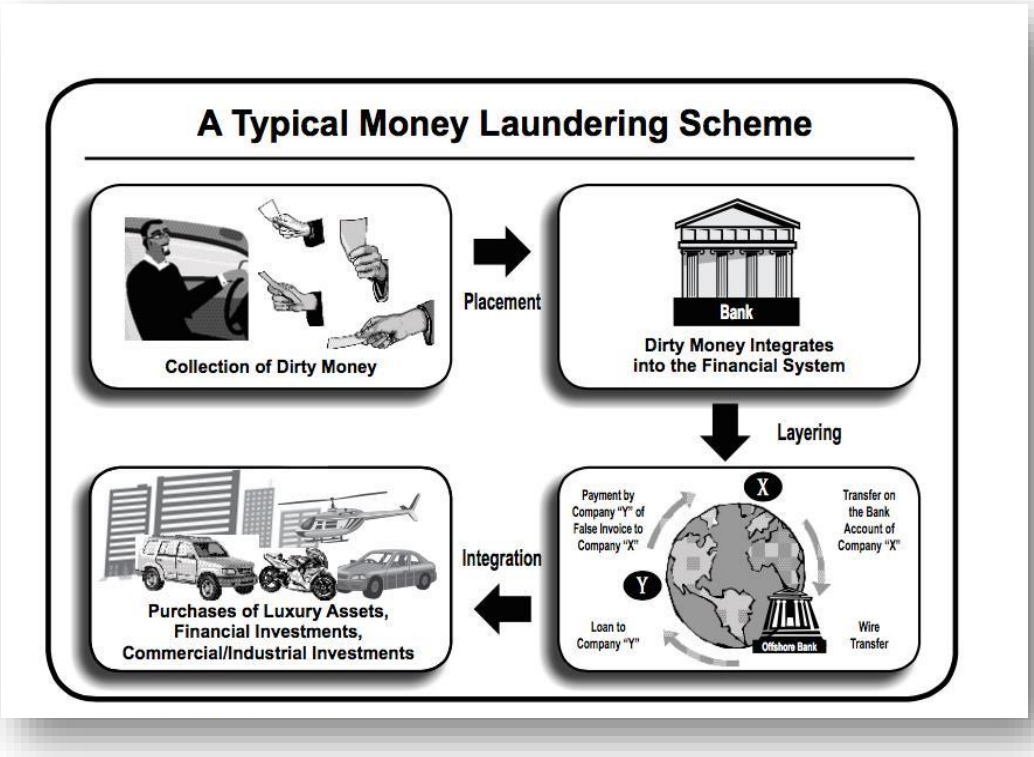
## The three-stage process

Traditionally money laundering is considered a three-stage process known as placement, layering and integration, although it should be borne in mind that it is not always the case and that laundering can be a far more straightforward process. Any involvement in dealing with criminal property at any stage may suffice.

- **Placement** - This is the initial phase of the process and it is usually where cash derived from criminal activity is infused into the financial system such as paying money into a bank account. Money launderers often attempt to conceal the origin of criminally derived cash by mixing it with legitimately derived cash. They do so by using the services of lawful business enterprises such as restaurants, taxi companies, bureaux de change etc. However, it is not always cash that is involved in the initial process, but the converting of the questionable asset obtained as a result of criminal activity into another form e.g. a motor vehicle or painting subsequently sold on.

- **Layering** – The objective of the layering phase is to disguise the proceeds of the criminality in sometimes complex transactions and transfers designed to disguise the audit paper trail and thus the source of the property. Quite often funds are transferred to accounts out of the original jurisdiction in which they were obtained. An example of this would be a launderer establishing several trading companies around the world which appear to trade with one another. Forged documentation can then be produced to justify a financial transaction taking place between the various entities.

- **Integration** – This is final stage of the laundering process and it is where illegal proceeds that have been placed and layered (and therefore 'cleaned') are re-integrated into the system. The main objective of the launderer at this stage is to reunite themselves with the criminal proceeds in a manner that does not draw attention or suspicion. The use of real estate is a common vehicle for money laundering and is often acquired at the integration stage, namely when funds are re-injected in the legal market after having gone through a series of intricate financial transfers that conceal their origin and beneficial owner. At this stage, the detection of the illicit origin of funds involved in the transaction is most difficult as they have already undergone the process of layering.




An example of when it is a far more straightforward process than the three stages previously described is when for instance there is no placement involved. This might include the scenario where there is a transfer of monies between two parties as bribery or a corrupt payment.

# Chapter 4 – SUMMARY OF THE 'PRIMARY' LEGISLATION

## Introduction

The principal legislation that concerns the offences of money laundering can be found within Part 7 of the Proceeds of Crime Act 2002 (POCA). The other main pieces of UK legislation concerning the prevention of money laundering or terrorist financing established an all-crimes approach, linking all acquisitive crimes which represent predicate offences to money laundering, failing to report knowledge or suspicions or reasonable grounds for knowledge or suspicions, 'tipping off' a person to the fact that a report has been made, and prejudicing an investigation.

The primary money laundering or terrorist financing legislation can be found within the:

- The Proceeds of Crime Act 2002, as amended by the Serious Organised Crime and Police Act 2005
- The Criminal Finances Act 2017
- Bribery Act 2010
- Terrorism Act 2000, as amended by the Anti-Terrorism, Crime & Security Act 2001.

The Terrorism Act 2000 establishes offences relating to:

- Facilitating, raising, possessing or using funds for terrorist purposes and for failing to report suspicions, tipping off and prejudicing an investigation
- Empowers authorities to make orders in connection with terrorist investigations
- Establishes a list of prohibited organisations with which a company may not deal.

## Definition of criminal property

Section 340 (3) of POCA 2002 defines criminal property as property that constitutes a person's *benefit* from *criminal conduct* or that it represents such a benefit (in whole or part and whether directly or indirectly) and:

- The alleged offender knows or suspects that it constitutes or represents such a benefit (section 340[3])
- The property which may comprise the benefit from criminal conduct is widely defined (S.340 [9] and [10]) to include:
- Money
- All forms of property or real estate
- Things in action and other intangible or incorporeal property.

A person obtains property if he obtains an interest in it.

## Criminal Conduct

Section 340 (2) of POCA defines criminal conduct as conduct which:

(a) Constitutes an offence in any part of the United Kingdom, or
(b) Would constitute an offence in any part of the United Kingdom if it occurred there.

The criminal offences giving rise to money laundering or terrorist financing are known as predicate offences and are as follows:

- *Theft*
- *Burglary*
- *Fraud*
- *Robbery*
- *Drug offences (possession, importation & supply)*
- *Corruption*
- *Bribery*
- *Extortion*
- *Tax Evasion*
- *People smuggling*
- *Counterfeit goods*
- *Sexual exploitation.*

## Money laundering offences – (Sections 327-329 POCA 2002)

- Acquiring, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property
- Entering into arrangements to facilitate laundering criminal or terrorist property
- Investing the proceeds of crimes in other financial products or in property or other assets
- Transferring criminal property.

The penalties for non-compliance are severe. For example:

- Somebody who knowingly assists a money launderer can be sentenced to 14 years in prison or fined or both.

## Failure to Disclose – (Section 330 POCA 2002)

As previously stated, the Proceeds of Crime Act 2002 places a legal obligation on every employee to report to their Nominated Officer any knowledge, suspicion or reasonable grounds to suspect money laundering or terrorist financing or terrorist financing.

The maximum penalty for failing to report is up to 5 years in prison, a fine, or both.

A separate offence of failure to disclose in respect of Nominated Officers exists where Nominated Officers who receive disclosures do not pass the information to the NCA when they:

- Know or suspect, or
- Have reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist financing.

The maximum penalty is up to 5 years imprisonment, a fine, or both.

However, an offence is not committed if a person makes an "authorised disclosure" to the company's Nominated Officer. As such, compliance with the company policy regarding reporting suspicious activity is vital.

## 'Tipping Off' – (Section 333A POCA 2002)

It is a criminal offence for anyone, following an internal disclosure to a Nominated Officer or externally to the NCA, to do or say anything that might either 'tip off' another person that a disclosure has been made to the NCA or to the company's Nominated Officer, and the disclosure to another person is likely to prejudice an investigation. This means that we must not tell a customer, or a known associate of that customer that a property sale was or is being delayed because we are carrying out an internal investigation, that we are reporting details of the customer's transactions or activities to the NCA; or that law enforcement is investigating the customer.

Reasonable enquiries of a customer concerning the background to a transaction or proposed transaction, as part of customer due diligence checks, will not usually give rise to a "tipping-off" offence, however once an actual SAR has been filed with the NCA best practice is to cease any further CDD checks made directly with the subject of the SAR, so as to prevent any likelihood of committing a 'tipping off' offence.

It is also an offence to make a disclosure that is likely to 'tip off' a customer that a money laundering or terrorist financing investigation is being undertaken or contemplated by law enforcement authorities. Therefore, any notification from law enforcement that they are

investigating a customer or former customer of the company for money laundering or terrorist financing matters should not be disclosed to the subject under any circumstances.

The offence carries a maximum penalty of 2 years' imprisonment, a fine, or both.

## Sanctions

In the UK, the regulation of financial sanctions is the responsibility of the 'Office of Financial Sanctions Implementation' ("OFSI") which is part of HM Treasury. The OFSI is responsible for:

- The implementation and administration of international financial sanctions in effect in the UK
- Licensing exemptions to financial sanctions
- Domestic designations under the Terrorist Asset-Freezing etc. Act 2010
- Directions given under Schedule 7 to the Counter-Terrorism Act 2008.

The OFSI maintain a consolidated list of all organisations and individuals who are the subject of sanction controls, and this database is publicly available and updated every 24 hours:

Financial Sanctions[3]

The UK and EU Sanctions may apply to individuals and legal entities

- In the UK or undertaking activities here, as well as
- To UK nationals and UK legal entities established under UK law, wherever their activities take place.

There is a duty to report to the OFSI as soon as practicable if one knows or has reasonable cause to suspect that a designated (sanctioned) person has committed an offence. The company must report any transactions concluded or attempts to use services, and may use the OFSI website below to 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: Financial Sanctions Implementation [4]

It is a criminal offence to breach a financial sanction without an appropriate licence or authorisation from the OFSI.

[3] http://www.hm-treasury.gov.uk/financialsanctionstreasury.gov.uk/financialsanctions
[4] https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

The offences imposed can be broadly described as:

- Dealing with the funds or economic resources of a designated person
- Making funds or economic resources, or in the case of terrorism financial services, available directly or indirectly to a designated person
- Making funds or economic resources, or in the case of terrorism financial services, available for the benefit of a designated person
- Knowingly and intentionally participating in activities that would directly or indirectly circumvent the financial restrictions, enable or facilitate the commission of any of the above offences.

This type of customer is high risk and therefore would require immediate referral to the NO for a decision as to whether the company is prepared to take on this type of customer and if required liaison with the OFSI in order to ensure there is no breach of the legislation, especially in light of the severe penalties for breaches.

Failure to comply with the UK sanctions lists could result in 7 years in prison, a fine, or both so therefore immediate referral to the NO is essential.

## Proliferation Financing

Section 18A.(1) Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 states:

*A relevant person must take appropriate steps to identify and assess the risks of proliferation financing to which its business is subject.*

Proliferation financing means the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, bio-logical, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation.

This company is aware of the need to mitigate the risks of the same within the business and have updated AML Policies & Procedures Manuals, and the firm wide AML Risk Assessment to reflect these. This specifically is in relation to high-risk jurisdictions such as The Democratic People's Republic of Korea and Iran but not exclusive to these countries. Although the risk for estate agents is low and likely to be indirect, consideration should be given when completing

customer due diligence to jurisdictions which have the potential for Proliferation Financing and how indirect funding can support these.

Proliferation Document[5]

5 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020695/National_risk_assessment_of_proliferation_financing.pdf

# Chapter 5 – SYSTEMS AND CONTROLS

## Policy Statement

Our company is committed to complying with all legislation that is designed to combat money laundering or terrorist financing. This includes ensuring that we have adequate controls to counter money laundering or terrorist financing as detailed in this document, and that we train staff appropriately. The risk of exposure to terrorist financing is considered to be very low, and therefore the policies and procedures of the company focus primarily on its prevention of money laundering. Nevertheless, the company is aware of its responsibilities and legal obligations in terms of reporting any suspicious activity relating to terrorist financing should such matters arise.

Although in December 2020 the UK Government assessed the estate agency businesses in general as a high risk of money laundering, after careful consideration of the risk factors specific to the size and nature of our business, we rate our own risk level as MEDIUM. The rating of MEDIUM is due in part to factors taken into account to reach this such as value of the average property and location, the company's potential exposure to the involvement of overseas based vendors and purchasers, especially those that are identified as a 'Politically Exposed Person' (which is very low). It is also due to the effectiveness of our procedures, controls and measures to manage and mitigate money laundering or terrorist financing risks. The company has not had exposure to legal entities such as trusts but has had limited exposure to overseas companies, and is aware that the task sometimes of "unwrapping" large, complex corporate or trust structures to establish beneficial ownership or controlling person(s) can be a significant risk factor given the level of anonymity these structures can provide.

Therefore, the company will apply a risk-based approach on all transactions and will keep its procedures and firm wide risk assessment under regular review at least annually, and certainly following any significant changes in: our business; the legal or regulatory landscape, such as the UK's latest national risk assessment, and HMT or HMRC guidance.

The company recognises the importance of staff promptly reporting suspicious activity and appointed a Nominated Officer and Deputy Nominated Officer to ensure compliance with the regulations and the effective reporting of money laundering or terrorist financing. The company is aware that the nominated officer should be of an appropriate level of seniority and therefore able to make decisions regarding the transactions taking place. In addition the company has procedures, which are detailed in this document, to undertake the appropriate level of Customer

Due Diligence measures, that includes the independent verification of the identity of our customers and to monitor ongoing activity in relation to them.

## Policies & Procedures

The policies adopted by the company in relation to AML/CTF are consistent with the ML regulations and latest government guidance and include:

- Statutory and Regulatory obligations to prevent money laundering or terrorist financing to be met in full and are to be applied as the minimum standard
- Appointing an individual to act as our Nominated Officer and to receive reports of suspicious activity
- The Nominated Officer/Senior Manager of the company will exercise positive action to minimise the risk that the company's services will be used for in relation to the laundering of funds associated with criminal activity, as defined by UK legislation
- Applying a risk-based approach for both the business as a whole and for individuals where qualifying transactions take place and where customer due diligence is applied
- If after the termination of a relationship following the reporting of suspicion of money laundering or terrorist financing to the appropriate reporting authority (the NCA), any further action that is required to be undertaken in relation to the customer shall be in conjunction with the relevant regulatory authorities and in accordance with the UK legislation to avoid any risk of the company or any of its employees committing a 'tipping off' offence.

The policies will be maintained through adopting the necessary procedures that include:

- The identities of all persons conducting business with the company are properly verified and sufficient information is gathered and recorded to permit the company to 'know its customer' and predict the expected pattern of business
- Consideration to decline potential new relationships that do not appear to be legitimate and where there is suspicion relating to criminal conduct on the part of the declined customer, such suspicion is reported to the Nominated Officer
- Ensuring employees report suspicious activity to the Nominated Officer or individuals with delegated responsibility
- Ensuring the Nominated Officer or individuals with delegated responsibility consider such internal reports in the light of available information and determine whether they give rise to knowledge or suspicion of money laundering or terrorist financing

- Established relationships are regularly monitored, to ensure that they fit the customer's profile, especially in respect of large or abnormal transactions
- Identifying and scrutinising complex or unusually large transactions, unusual patterns of transactions which have no apparent economic or visible lawful purpose and any other activity that could be considered as relating to money laundering or terrorist financing
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations
- All suspicions are reported promptly to the Nominated Officer and full cooperation is provided to the relevant reporting authority and the investigating authorities to the extent required by statute/regulation and to the extent permitted without breaching customer confidentiality
- Determining whether a customer is a 'Politically Exposed Person' (PEP) and if so putting in place appropriate CDD measures
- Determining whether the customer is subject to any Financial Sanctions.

## Roles and responsibilities of the Nominated Officer and staff members

The Nominated Officer (otherwise known as a MLRO) of the company is Christopher Norman (Head of Compliance) and the Deputy Nominated Officer is Fiona Ashworth (Finance Director).

The Nominated Officer's prime responsibilities include the following:

- Receiving internal suspicious activity reports (also known as 'disclosures') from within the company
- Considering each report, usually in conjunction with the employee who has made the report
- Evaluating the information and deciding whether the case should be reported to the NCA and making appropriate notes to explain the decision
- If appropriate, report the case to the NCA immediately or as soon as practicable, via the NCA's website, www.ukciu.gov.uk, and make appropriate notes on the internal SAR
- Ensure receipt of the report is acknowledged by the NCA's automated system
- Retain copies of the internal reports, the decisions taken on each report and the NCA response. All NCA documentation should be maintained separately from customer files to minimise the risk of 'tipping-off'
- Deal with any issues connected to the NCA 'Defence Against Money Laundering' regime.

In addition to the above the Nominated Officer will be responsible for:

- Developing necessary policies, procedures, training and education of staff. The Nominated Officer will be provided with copies of any current Guidance Notes to enable internal procedures to be kept up to date and the Nominated Officer will ensure that he or she is kept up to date with new money laundering or terrorist financing requirements and developments
- Developing and maintaining policy in line with the evolving statutory and regulatory obligations and experience/advice from enforcement agencies
- Representing the company to all external agencies and in any other third-party enquiries in relation to money laundering or terrorist financing prevention or compliance
- Ensuring all staff are given sufficient training in this area to ensure they are able to meet their legal obligations and responsibilities
- Ensuring that all parts of the company are complying with the stated policy and are therefore monitoring operations and development of the policy to this end
- All contact between the company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.

Regulation 21 of the “Regulations” sets out a requirement for the company to appoint a Money Laundering Compliance Officer (MLCO) responsible for ensuring that the company meets all of its requirements and obligations in relation to the “Regulations”. This role is in addition to the requirement to appoint a Nominated Officer, however the MLCO may also be the Nominated Officer provided they are of sufficient seniority.

The “Regulations” state that the following factors should be considered as part of the procedure to determine whether it is appropriate to apply those controls, and these include:

- Number of staff members in the company
- Number of offices in the company and where they are located (including whether the company has overseas offices)
- Customer demographic
- Nature and complexity of work the company undertakes
- Level of visibility and control that senior management has over client matters.

This company has decided that the MLCO role will be undertaken by Christopher Norman, the current Nominated Officer, and this is due to their level of experience and the fact that they are the Head of Compliance for the company. The company will ensure that the Nominated Officer and/or deputy nominated officer has access to resources and information to enable them to carry out that responsibility, and therefore the overseeing of full adherence to the "Regulations".

The staff of the company are responsible for:

- Familiarizing yourself with the 2022 AML Procedures, policies, systems and controls; Specifically,
- For reading this Manual
- Familiarizing yourself with the particular AML risks with respect to your role and responsibilities, especially if your role or responsibilities change.
- Familiarizing yourself with all AML procedures.
- Remaining vigilant to the possibility of money laundering or terrorist financing
- Reporting to the Nominated Officer all suspicions of money laundering or terrorist financing
- Complying fully with all money laundering or terrorist financing procedures in respect of customer identification, customer monitoring, record keeping, vigilance and reporting.

## Establishing a Risk Based Approach

The 2017 "Regulations" require the company to adopt a risk-based approach to the application of measures to prevent money laundering or terrorist financing. A risk-based approach requires regulated companies to identify, assess and understand anti-money laundering or terrorist financing risks and apply effective resources to mitigate those risks. Any measures to prevent the risks must be commensurate with the risk itself.

The risk-based approach starts with the identification and assessment of the risk that must be managed. To achieve this, the company is required to undertake an AML Risk Assessment in accordance with Regulation 18(1) of the "Regulations" to identify the risks that a company faces and the controls that need to be put in place to eliminate and identify any residual risks to minimise their impact.

The 'Joint Money Laundering Steering Group' [JMLSG] in the UK issued guidance [6] in adopting a risk-based approach and states that the core obligations of a company are:

[6] https://www.jmlsg.org.uk/guidance/

- Appropriate systems and controls must reflect the degree of risk associated with the business and its customers
- Determine CDD measures on a risk sensitive basis, depending on the type of customer, business relationship, product or transaction
- Consider situations and products which by their nature can present a higher risk of money laundering e.g. customer not physically present for identification purposes and business relationships and occasional transactions with Politically Exposed Persons [PEPs] or higher risk countries
- Financial sanctioned targets and additional measures that need to be taken.

## AML Risk Based Approach

In carrying out the risk assessment required, a "relevant person", which for this company is the Nominated Officer, must consider:

- Information made available to them by the supervisory authority and risk factors relating to:
- *Its customers*
- *The countries or geographic areas in which it operates*
- *Its products or services*
- *Its transactions, and*
- *Its delivery channels.*

In deciding what steps are appropriate, the 'relevant person' must consider the size and nature of its business and whether the company has overseas offices. The Risk Assessment should be reviewed at regular meetings and changes made where deemed necessary. A copy of the Risk Assessment template form can be found at **Appendix 1**. The significant issues within each risk factor that need to be considered are as follows:

**Customer Risk**

- Location of property in relation to the buyer e.g. is there a large unexplained geographic distance between the two?
- Unusual involvement of third parties
- Titling a residential property in the name of third party; for example, a friend, relative, business associate, or lawyer. Use of legal entities (corporations, LLPs or partnerships) that obscure the identity of the person who owns or controls them without a legitimate

business explanation (particularly relevant to enablers for designated (sanctioned) persons)

- High-ranking foreign political officials or their family members.

**Geographic Risk**

- The customer is resident in a jurisdiction that has a weak AML regime, supports or funds terrorism, or has a high degree of political corruption
- The source of the customer's funds originating from a country with weak or non-existent AML controls.

**Products & Services**

Companies selling residential property are potentially vulnerable to be exposed to money laundering as real estate remains an extremely attractive commodity for those seeking to launder funds. The potential to "hide" funds in the UK property market is attractive due to the status of owning UK property as well as the financial returns that can be achieved.

**Transaction Risk**

- Under or over-valued properties:
    - For example, is the property owner selling the property for significantly less than the purchase price?
    - Does the seller seem disinterested in obtaining a better price?
- Use of large amounts of cash:
    - Buyer brings actual cash to the closing
    - The purchase of a property without a mortgage, where it does not match the characteristics of the buyer
    - While rules and regulations governing the financial sector are designed to detect situations where large amounts of cash are being introduced, real estate practitioners should keep this factor in mind when evaluating whether a transaction seems suspicious
- Property purchases inconsistent with the individual's occupation or income:
    - Is the property being purchased significantly beyond the purchaser's means?

    - Immediate resale of the property especially if the sale entails a significant increase or decrease in the price compared to the prior purchase price, without a reasonable explanation.

- Speed of transaction (without reasonable explanation)
- Unusual source of funding:
    - Use of third-party funds to purchase a property where it doesn't make sense, i.e. third-party is not a parent, sibling, etc
    - Use of several different sources of funds without logical explanation e.g. funding coming from a business but property not being held in business' name, or purchase of property doesn't match the business' purpose
    - Use of digital currency  the use of digital currencies to purchase property should be considered a red flag due to the lack of regulation & especially so from high-net-worth individuals from high-risk countries.

- Purchases being made without viewing the property, no interest in the characteristics of the property
- Any other activities which demonstrate suspicious behaviour and do not make professional or commercial sense based on the agent's familiarity with the real estate industry and the normal course of business.

**Delivery Channels**

The use of intermediaries could potentially provide a greater risk due to the lack of "face to face" contact with the actual customer. Properties sold online as such can be problematic if there is no actual viewing undertaken by the purchaser and the practice of selling a property without a physical viewing poses a risk.

As part of the Delivery Channel, the knowledge and training in relation to AML matters that staff are provided with could be considered a potential risk if not of a sufficient standard, or no training is provided. The primary objective of AML training is to establish and maintain an appropriate level of competency to ensure that the staff fulfil their roles in protecting the company from money laundering. Compliance with statutory and regulatory obligations should flow as a by-product.

To achieve this, all members of staff should receive high quality regular formal training which is relevant to the role of the staff member either from the Nominated Officer or from an external contractor, and this should be delivered on a regular basis to achieve their AML objectives that will include:

- Encouraging staff to be vigilant at all times
- Making staff aware of their legal obligations
- Demonstrating why certain services are vulnerable
- Educating staff in the recognition of unusual or suspicious transactions
- Making staff aware of the organisation's AML policy and procedures
- Educating staff in the importance of quality CDD, and
- Identifying the Nominated Officer and the Deputy Nominated Officer and the reporting procedures.

A record must be kept of all persons who attend the training and the Nominated Officer should ensure that questions are asked of members of the company who do not attend the training, and this includes Senior Manager(s). As previously stated, those employees who do not make themselves conversant with the legislation leave themselves and the company wide open to regulatory, and even possibly criminal action by failing to meet their obligations. If the Nominated Officer feels it is appropriate, they will seek the guidance and advice of a suitably qualified AML external consultant in terms of both training and regulatory concerns.

In addition to the five main risk factors, any AML Risk Assessment must always consider the issue of PEPs and the SAR procedure, both of which are covered in greater detail in this manual. The sort of information required will be whether a company has had any PEPs as clients in the previous 12 months and how they have been managed, and whether any SARs have been filed with the NCA.

It is essential that any AML Risk Assessment is not seen as just a "tick box" exercise as this company needs to clearly set out how any inherent risk associated with the business is going to be mitigated through implemented policies and procedures.

## Risk Rating of Clients

One of the key methods in assisting in the identification and assessment of the money laundering risks the company faces is understanding the level of risk each individual customer i.e. client or purchaser pose to the business. To do this, the company must ensure that

appropriate controls are put in place to lessen these risks. Managing and mitigating the risks involves:

- Applying customer due diligence measures to verify the identity of customers
- Obtaining additional information on higher-risk customers
- Conducting on-going monitoring of the transactions and activity of customers with whom there is a business relationship, and
- Having systems to identify and scrutinise unusual transactions and activity to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing or terrorist financing may be taking place.

The “Regulations” state that we must determine the extent of our customer due diligence measures and on-going monitoring procedures on a risk-sensitive basis, depending on the type of customer, business relationship or transaction. Examples of risk-based control procedures may include:

- Requiring additional evidence of identity, source of funds and source of wealth information in higher risk situations
- Varying the level of monitoring of customer transactions and activities according to identified risk to identify transactions or activities that may be unusual or suspicious.

Therefore, each customer should be risk rated to give an indication as to whether the subject is deemed ‘Low’, ‘Medium’ or ‘High’ Risk in terms of money laundering, and the appropriate steps taken as set out in this policy and procedure manual.

The methodology concerned with risk rating the customer should be recorded with use of the template forms found for a seller and a purchaser at **Appendix 2 & Appendix 3**. The risk rating of customers should be undertaken at the time of establishing a business relationship and then reviewed at the exchange of contracts stage. Ongoing monitoring should continue for the duration of the business relationship to confirm no material changes have taken place regarding the status of the customer during the course of the business relationship. Ensure during the business relationship that any documents provided remain in date for the duration. Identifying a customer or transaction as being of a higher risk does not automatically mean that the customer or transaction is involved with money laundering or terrorist financing. Similarly, a customer or transaction seen as low risk does not mean that the customer or

transaction is not involved with money laundering or terrorist financing. Staff therefore need to be vigilant and use their experience and common sense when applying our risk-based criteria and rules.

An understanding of the risk posed by potential 'red flags' is essential in order to risk rate the client appropriately. Some of the factors that need to be taken into account when assessing the level of risk posed by a customer and or a transaction include, whether the buyer is located or domiciled in the UK or an overseas jurisdiction that has weak AML controls or higher levels of corruption or are funds originating from a UK financial institution or from a jurisdiction with weak or low AML controls. The potential use of complex opaque structures such as trusts or companies, especially those located offshore is another factor, and also whether the individual is a PEP. An understanding of the potential 'Red Flags' will assist in the risk rating process. It shall be for the members of staff to consider the risk posed by a customer, but consideration should be given to discussion with the Nominated Officer if in any doubt.

Therefore, the employee should consider for every customer and transaction the level of risk rating to attribute to:

- The Seller
- The Purchaser
- The Business Relationship.

The points below are the matters which are to be taken into account in determining the level of risk, but this is not an exact science and will require the employee's skills that include:

- Common sense
- Business acumen including commercial awareness
- Knowledge of the customer and their business
- Knowledge of the purchaser's source of funds
- Professional skills of information assessment & assimilation
- AML training
- Professional qualifications
- The use of third-party service providers through online verification.

The company must carry out regular assessments of the adequacy of its systems and controls to ensure that it manages the money laundering or terrorist financing risks effectively and is

compliant with the "Regulations". Therefore, it must ensure that appropriate monitoring processes and procedures are established and maintained to regularly review and test the effectiveness of our policies and procedures. The company must test the effectiveness of the checks we make and the areas and indicators of risk that we have identified.

The "Regulations" have removed the prescriptive list of entities that are subject to Simplified Due Diligence [SDD]. However, there are certain circumstances where it is clearly appropriate to apply SDD as the risk of money laundering is extremely low.

However it should be noted that if 'Simplified Due Diligence' is to be undertaken in relation to a customer because it is determined that they present a low risk, or even no risk of money laundering, this should still be recorded on the 'Risk Rating' form as it will evidence the fact that the risk has been considered and the rationale for reaching the final decision.

## Recognition of 'Red Flags'

There are a number of what could be deemed 'Red Flags' when it comes to money laundering, and it is likely that a combination of factors will give rise to suspicion rather than one isolated issue. The following list are just some of the issues to be aware of and are set out within what are considered the four main risk areas those being customer, transaction, geographical or delivery channel of products and services. The examples below are by no means exhaustive.

**Customer Risk**

- Customer produces copies rather than original ID documents
- Provides false or counterfeited documentation
- Delays giving you the verification you have requested for a transaction
- Is a business entity that cannot be found on the Internet
- Uses an 'alias' or is secretive about their personal information
- Uses a PO box or other type of unusual address instead of a residential or business postal address
- Seems very conversant with Money Laundering issues
- Is reluctant to or refuses to provide information that you have requested (e.g. relating to finances) before you can progress the transaction
- Does not want correspondence sent to their home address
- Not concerned that his instructions may lead them to suffer a loss or are a bad investment and there is no good reason for those instructions e.g. the purchaser who is unconcerned about paying over the odds for a property

- Reluctant to meet you in person
- Not possible to establish the identity of the beneficial owner or person who exercises control over a company
- Known to have convictions, or to be currently under investigation for, acquisitive crime or has known connections with criminals
- Use of intermediaries without good reason
- Avoidance of personal contact for no good reason
- Customer is a Politically Exposed Person (PEP)
- Customer is a family member or linked associate of a PEP.

**Transactional Risk**

- Transfers from countries that have weak or non-existent AML controls
- The parties attempt to disguise the real owner or parties to the transaction
- Reluctance to disclose information, data and documents that are necessary to enable the execution of the transaction
- Where there are confusing movements between a variety of funds, to and from a variety of accounts, in a variety of jurisdictions, for no clear purpose
- Payment out to a third party of a customer's money
- Funds coming into and going out of the UK using complex arrangements for no logical reason
- The request to use cash in a transaction
- Transactions with no apparent purpose and, which make no obvious economic sense
- The activity or transaction is inconsistent with what would be expected from the declared business
- Funds are received via several accounts from the purchaser for no good reason
- The purchaser tells you that funds are coming from one source and at the last minute changes the source of funds
- Disproportionate amount of private funding
- Large financial transaction, especially if requested by a recently created company, where it is not justified by the corporate purpose, the activity of the client or its group companies
- Attempts to conceal the identity of the remitter of the funds using instruments such as bank drafts
- Requests to make an "overpayment" for a property so as to potentially free up capital.

**Geographical Risk**

- The customer is resident or native to a jurisdiction that has weak or non-existent AML controls
- Resident or native to a jurisdiction that has high levels of corruption
- Transaction involves a country where underground or parallel banking is accepted business practice
- Transaction involves a country known for its highly secretive banking and corporate law
- Involvement in the transaction of a country that is the subject of sanctions or links to sanctioned countries
- Unusual use of offshore accounts, companies or other entities given the customer's instructions.

**Product or Services Risk**

- The client is a seller of a property that they do not reside at and there is no charge on the property
- Mortgages being redeemed soon after their completion
- Trust structures which may be used for the concealing of criminally derived assets
- The use of shell companies or corporate entities that do not have any business activities or recognisable assets themselves
- Immediate sale and then re-sale of the property for a markedly different price could be an indication of mortgage fraud and an attempt to launder the proceeds
- Mortgages being repeatedly repaid significantly prior to the initially agreed maturity date
- Finance provided by a lender other than a credit institution.

# Chapter 6 – WHAT IS SUSPICION, REASONABLE GROUNDS TO SUSPECT & KNOWLEDGE

## What is suspicion for the purposes of POCA

**The company recognises the importance of staff reporting suspicious activity as soon as reasonably practicable to its NO/MLRO, who is Christopher Norman.**

Suspicion is essentially a subjective issue and so is less than knowledge. Despite difficulties in defining the word suspicion, and because of its importance in English criminal law assistance can be sought from case law with the most significant being that of R v Da Silva [2006][7] in which Longmore LJ stated *"the defendant must think there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be "clear" or "firmly grounded or targeted on specific facts" or based upon "reasonable grounds".*

In addition, guidance from the JMLSG in 2020 confirms that suspicion is more subjective than knowledge and falls short of proof based on firm evidence. Suspicion has been defined by the courts as in the case of Da Silva as being beyond mere speculation and based on some foundation.

If an employee forms the relevant suspicion about a client or transaction, they are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. There is not a requirement to have evidence that money laundering or terrorist financing is taking place to have suspicion.

## I have concerns that don't amount to suspicion; what should I do

It is appropriate and indeed advisable that if you should you have a concern (which does not yet amount to a 'suspicion') arising in respect of a particular transaction, then you should routinely ask questions of the customer and take practical steps to learn enough about your customer and the source of any funds involved, and about the transaction as a whole. You should then sensibly be able to determine whether that concern constitutes a 'suspicion' and subsequently requires an immediate report to the Nominated Officer. You may also wish to discuss the issue with the Nominated Officer to assist you to reach your own conclusion.

## The Customer's response to further enquiries has increased my concern

If you have not yet done so, and the further enquiries of the customer increase your concerns

[7] https://www.casemine.com/judgement/uk/5a8ff7ab60d03e7f57eb10fb

to the point of 'suspicion', an employee should immediately make a report to the Nominated Officer. Be aware that the employee is not required to pursue "all lines of inquiry" just what is expected in terms of CDD according to the legislation i.e. ML Regulations.

### The Client's response to further enquiries has allayed my concern

If the concerns have reduced or diminished the staff member should always make a written note of their concerns, the answers the customer has given to the questions that they have raised by way of further enquiry, and why the member of staff is no longer concerned as a result of these answers. The written note should be signed and dated and given to the Nominated Officer for their records. This will protect the employee should there be any problems with this customer in the future in the context of money laundering or terrorist financing. Never place the notes on the actual customer file. However, it is important to remember that CDD is an ongoing process not just at the time of "onboarding" the client.

No one, regardless of their seniority, may dissuade a member of staff from making a suspicious activity report to the Nominated Officer in circumstances where he or she personally has knowledge or suspicion. The key things to remember is that a person does not have to wait until suspicion reaches some level of 'reasonableness'. In addition to subjective suspicion, under sections 330 and 331, a person can commit a criminal offence for failing to report money laundering or terrorist financing in circumstances where it was reasonable for them to have known or suspected it. A criminal prosecution under POCA does not require proof of any intent or any dishonesty on the part of the employee to bring about a prosecution.

As a result of the issues raised in a case involving HSBC v SHAH, where the customer who was the subject of a SAR sought to take civil action against the reporting institution, the Serious Crime Act 2015 affords companies a degree of protection in that it gives 'Exemption from civil liability for money-laundering disclosures'. The Act states:

*"In section 338 of the Proceeds of Crime Act 2002 (money laundering or terrorist financing: authorised disclosures), after subsection (4) insert—*

*"(4A) Where an authorised disclosure is made in good faith, no civil liability arises in respect of the disclosure on the part of the person by or on whose behalf it is made."*

However, the key point to remember is that the employee has formed the relevant suspicion and has adhered to the correct procedures when it comes to reporting those suspicions as set out in this manual and in accordance with POCA 2002.

## What are reasonable grounds to suspect

This aspect of criminal conduct only relates to persons in the "regulated sector" and reasonable grounds to know or suspect is in effect an objective test and met when an individual can demonstrate that facts or circumstances exist from which a reasonable person engaged in a business subject to money laundering regulations would have inferred knowledge, or formed the suspicion, that another person was engaged in money laundering or terrorist financing. The test will operate on the balance of probabilities, and as a defence to this aspect, staff must show that in the circumstances and as part of a 'Risk Based Approach', to know the customer and therefore the rationale for the activity, transaction or instruction.

The offence of 'Failing to Disclose' covers both a person's actual (subjective) knowledge or suspicion of money laundering or terrorist financing, and also applies a higher than normal objective test i.e. was it reasonable for you, someone working in a regulated company and therefore obliged under the "Regulations" to be properly trained to spot and report money laundering or terrorist financing, taking into account experience, qualifications etc, to have reasonable grounds to know or suspect money laundering or terrorist financing. The Court will take account of a person's experience and qualifications.

By applying a methodical and effective system to their everyday work in order to obtain and assess information about the customer and the transaction, an employee should be able to reach (at the least) a reasoned analysis or judgement of the situation. Even if the employee doesn't subjectively "suspect" a money laundering or terrorist financing transaction, consider whether or not a court might decide that objectively a person had reasonable grounds to have known or suspected money laundering or terrorist financing.

## What is knowledge

The issue of knowledge is more straightforward and accepted as actually knowing something to be true. It can also be inferred from a situation where the existence of money laundering should have been obvious to any reasonable and adequately trained employee. It has been asserted that there are five types of knowledge:

(i) Actual knowledge
(ii) Wilfully shutting one's eyes to the obvious
(iii) Wilfully and recklessly failing to make such inquiries as an honest and reasonable man would make

(iv) Knowledge of circumstances which would indicate the facts to an honest and reasonable man

(v) Knowledge of circumstances which would put an honest and reasonable man on inquiry.

# Chapter 7 – MONEY LAUNDERING, TERRORIST FINANCING & TRANSFER OF FUNDS REGULATIONS 2017

## Summary of the Regulatory offences

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ["Regulations"] came into effect on the 26th June 2017. The aim of the "Regulations" is to prevent money laundering or terrorist financing, and they set out the requirement for companies to establish and maintain appropriate and risk-sensitive policies and procedures relating to:

- Customer due diligence and on-going monitoring
- Reporting
- Training
- Dealing with Politically Exposed Persons ("PEPs")
- Record keeping
- Internal control
- Risk assessment and management
- The monitoring and management of compliance, and
- The internal communication of the policies and procedures.

## Customer Due Diligence

CDD encompasses 'Know your Customer' (KYC) but effectively goes further and should consider the source of funds for real estate purchases and rentals, and if deemed necessary in the case of higher risk customers, a source of wealth. When it is necessary to establish the source of funds the template form at **Appendix 4** can used by the purchaser for recording this information and supply documentation that supports the purchase funds e.g. mortgage offer, bank statement etc. However, the company will take a Risk Based Approach to the issue of funding and the company will ensure that the source of funds is in line with the risk profile of the purchaser. In summary, the basic steps of CDD include the steps below and are discussed further later in this Manual.

- Identify the customer
- Verify the customer's identity
- Understand the source of funds
- Understand the nature of the transaction, and

- For EDD, understand the source of wealth.

CDD must be undertaken before the establishing of a business relationship or undertaking a transaction on behalf of the customer and as previously described, measures should be applied on a risk-sensitive basis, depending on the type of customer, business relationship or nature of the transaction or activity. There are three accepted levels of Due Diligence:

- Simplified (SDD)
- Standard (CDD)
- Enhanced (EDD).

The "Regulations" require that the extent of CDD measures must be decided on a risk-sensitive basis, depending on the type of customer, business relationship, or transaction. It is important that all employees keep matters under review as CDD is on ongoing process and any change in the circumstances of the client relationship might affect what is required from the client in terms of CDD. The company must be able to demonstrate to any interested parties including the regulator HMRC that its due diligence measures are appropriate in view of the risk of money laundering or terrorist financing that the company faces, and employees must:

- Stay alert to any suspicious circumstances which may suggest ML, terrorist financing, or the provision of false CDD material
- Consider the risk profile of the client
- What other information the company may hold about this client, whether electronic verification would assist you and/or open-source research.

**Why the company should undertake CDD measures**

It is essential that the company is able to:

(a) Identify the customer and guard against ID theft
(b) Verify the identity of the customer using documentation, data or information from an independent reliable source
(c) Determine whether the customer is acting on behalf of another person, and if so, identify that other person and take reasonable measures to verify that person's identity
(d) In the case of a legal person e.g. a company you must identify the natural person who ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the share or voting rights in the legal person or any person who exercises control over the management of the company

(e) In the case of a legal arrangement, the trustee, settlor or other person who exercises ultimate effective control over the legal arrangement, and in the case of a foundation, a natural person who otherwise exercises ultimate effective control over the foundation

(f) Obtain all information on the purpose and intended nature of the business relationship, and

(g) Take reasonable measures to establish the source of funds.

**When the company should undertake CDD**

- When establishing a business relationship and prior to undertaking any transactions
- Where there is a suspicion of money laundering or terrorist financing or terrorist financing
- Where there are doubts about previously obtained customer identification information
- At appropriate times to existing customers on a risk-sensitive basis.

In practical terms the establishing of a business relationship for the seller i.e. the client is when the instructions are received to market the property concerned and a contract is signed, If it is necessary not to interrupt the normal conduct of business and there is little risk of money laundering or terrorist financing then you can make an exception to when customer due diligence is carried out. However use of this exception will be very limited and should only be used during the course of setting up the business relationship.

In relation to the timing of obtaining the documentation for identification purposes, if the seller is met in person then it must be obtained at the time of receiving the instructions to market the property, and for the purchaser at the time an offer is put forward by the purchaser and accepted by the seller. If the customer cannot be met “face to face”, and original ID documentation cannot be produced, because for example they are resident overseas, then a certified copy of the ID must be obtained from the customer at the time of establishing the business relationship as described above.

If the customer is a business, the relevant person must collect proof of registration or an extract of the register, before a business relationship is established, to show the business:

- Is subject to the requirements of Companies Act 2006, Part 21 A
- Is subject to the requirements of Limited Liability Partnerships (Register of People with Significant Control) Regulations 2016

- Is subject to the requirements of Scottish Partnerships (Register of People with Significant Control) Regulations 2017, or
- Is otherwise subject to registration under Part 5 of the Regulations.

Where your customer is a company, unregistered company, limited liability partnership, eligible Scottish partnership, trust, or an overseas entity, you must either collect an extract of the register which contains full details of the information held or establish (from inspection of the register) that there is no information held at that time. This must be done before establishing a business relationship, and as part of ongoing monitoring.

**How CDD should be undertaken**

CDD generally is a cumulative process with more than one document or data source being required to verify all of the necessary components. A list of the identification documents or data that can be used for CDD purposes can be found at **Appendix 8**.

In practice, if the customer is seen in person then original and current documentation can be provided and a copy obtained. The copy will then be "certified" by the company employee confirming the fact that they have had sight of the original and the date that the original document was produced. If the customer cannot be seen in person, then a copy of the approved documentation should be requested that has been certified by an appropriate person. The certification should confirm the fact that the appropriate person has met the customer in person, and original documentation has been provided for identification purposes e.g. passport. It should also confirm the fact that the customer bears a true likeness to the person whose photograph appears in the document produced and the appropriate person should also record the date of the certification.

Online verification through a third-party service provider is another method of obtaining information from database searches and are used to uncover ML risks such as PEPs, high-risk jurisdictions, clients on sanctions lists, clients who have been subject of criminal prosecution or investigation, among many other data points retrieved from publicly available information through open-source research. This and open-source adverse medial checks can be used to supplement the customer due diligence process and additionally supports a risk based approach for each client.

Appropriate persons for the purposes of certifying documents are as follows:

- Credit or financial institution which is an authorised person i.e. the FCA regulated entity

or individual

- Auditor
- Insolvency Practitioner
- External accountant (not employed directly by the client)
- Tax advisor
- Independent legal professional
- Doctor
- Minister of Religion.

As best practice if a certified document is produced then a check should be made with the supervisory body to confirm that the appropriate person is suitably qualified to undertake the certification of documents e.g. for a legal professional the Law Society or SRA website. For appropriate persons who are resident overseas then open-source research should be undertaken to confirm their suitability to undertake the certification of documents.

The actual level of CDD undertaken should be recorded through use of the template forms at **Appendix 2** for the 'Seller' and **Appendix 3** for the 'Purchaser' and every employee must complete the form in respect of the CDD undertaken and attach to it a copy of the identification provided by the client or the purchaser.

If a third party or intermediary is representing either the client or purchaser, and therefore there is no direct 'face to face' contact with the customer, then it is essential that the same level of identification and verification is undertaken in respect of the third party to confirm their identity and their authority to represent the customer and the relationship between the various parties involved in the transaction.

As clearly set out in the "Regulations" if an employee doesn't obtain CDD at all, or in the timeframe required by the money laundering regulations, they must cease to undertake any further work on behalf of the client or purchaser as this will potentially constitute a breach of the "Regulations" and can lead to regulatory or criminal action being instigated against them, and or the company. In addition to ceasing to act for a lack of CDD, the employee may also have to go on to consider whether this lack of CDD causes them to be suspicious, and therefore file a SAR under the Proceeds of Crime Act 2002.

If the obtaining of the CDD is to be delayed in accordance with the "Regulations" consideration should be given to seeking written authorisation from the Nominated Officer for such a delay. If

the customer is unhappy or unwilling to provide CDD, you should refer the matter immediately to the Nominated Officer.

It is essential that every member of the company explains to the customer that there is a legal requirement to carry out CDD for all customers, so that they are aware of the company's obligations and therefore they fully understand the reasoning behind any request for information. Correspondence sent to both the seller and the purchaser at the time of establishing a business relationship will contain information that clearly sets out what the company's obligations are in relation to the money laundering legislation. A copy of the wording set out in the AML Policy letter **Appendix 5** can be incorporated partly or in its entirety in the 'Heads of Terms' that is sent to the client or purchaser as part of the terms of business.

It is imperative that everyone in this company diligently keeps all matters under constant review as CDD is an ongoing process and any change of circumstances in the customer relationship might affect what is required from the customer in terms of CDD.

Every employee must:

- Stay alert to any suspicious circumstances which may suggest ML, terrorist financing, or the provision of false CDD material
- Always look at the risk profile of the customer
- Consider what other information the company may hold about this customer, particularly if it relates to the customer's overall Risk Profile or to new CDD
- Consider whether electronic verification would assist you.

Inadequate CDD standards and controls can result in serious customer and counterparty risks for the company in relation to reputational and legal risk resulting in potential significant financial cost to the company and legal action being taken against the relevant person.

## Simplified Due Diligence

The Money Laundering Regulations 2017 did away with the defined list of entities that are considered to present a low risk of money laundering or terrorist financing and can be subject to Simplified Due Diligence. However, as a guideline certain circumstances SDD may be applied such as:

- A public authority or publicly owned body in the UK

- A financial institution that is itself subject to anti-money laundering supervision in the UK or equivalent regulation in another country
- A company whose securities are listed on a regulated market
- Beneficial owners of pooled accounts held by a notary or independent legal professional, provided information on the identity of the beneficial owners is available upon request
- A European Community institution
- A pension scheme that does not allow assignment of interests.

A check must be completed to confirm that the entity is eligible for Simplified Due Diligence (e.g. search of the relevant company register or confirmation of the company's listing on a regulated market, regulated entity register (e.g. the FCA). Written confirmation must be obtained that the person instructing has the authority to do so and the person must be identified by:

- Full business name and registered number
- Country of incorporation
- Address of the legal entity.

In undertaking Simplified Due Diligence the company is seeking to confirm its existence through the use of company documents which can be achieved through Companies House and open-source searches and also crucially the fact that the entity is a regulated entity itself i.e. subject to the "Regulations" themselves.

## Enhanced Due Diligence

A referral to the Nominated Officer and Senior Management should be sought prior to commencing a business relationship with a customer considered "high risk" such as a PEP (see Chapter 8), and where there is a requirement to undertake EDD. This might also apply to an existing customer who are not in themselves considered high risk but the transaction their undertaking is, such as the transfer of funds from or to a high-risk jurisdiction.

You must complete EDD when:

- You have identified in your risk assessment that there is a high risk of money laundering or terrorist financing
- HMRC or another supervisory or law enforcement authority provide information that a particular situation is high risk in published material or where, for example, a law enforcement interest has been registered with the Land Registry. In particular, further

information relating to super-prime properties and other high-risk areas can be found within the National Risk Assessment

- A client or any party relevant to the transaction is established in or operates from a high risk third country identified by the FATF or a high risk third country identified by the UK
- A person has given you false or stolen documents to identify themselves (immediately consider making a suspicious activity report)
- A client is a politically exposed person, an immediate family member or a close associate of a politically exposed person
- The transaction is complex and unusually large, or there is an unusual pattern of transactions, such as, in the case of legal entities, it has more than 2 levels of ownership, though this is dependent on what the business identifies as irregular based on their experiences
- The purchase, sale, or tenancy agreement is for an unusually large amount for your type of business, location or for the individual
- A residential property is a super prime property. What a business identifies as super prime would be reflective of factors such as the region and the competitiveness of the market, usually within the top 5% of the local market values, or
- During the course of completing due diligence, the business identifies a client is a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in that EEA state.

EDD procedures for new customers that are assessed as posing higher risk must be undertaken before or during the formation of that relationship and there should be no concession to delay the timing of obtaining the identity information and the verification of it. If satisfactory EDD is not obtained, the business relationship is to proceed no further, and the relevant person should consider making an internal disclosure.

Source of funds is concerned with the funding of the transaction, for example an immediate source from which property has derived e.g. a bank account in the name of Mr 'X'. Knowing who provided or will provide the funds and the account or product from which they have derived is necessary in every case. The source of funds requirement refers to where the funds are coming from in order to fund the relationship or transaction. Source of funds will sometime be a bank account that can be directly related to the purchaser. Where this not the case, for example when a third party is involved, the relevant person may take a risk-based approach and where

appropriate make further enquiries about the relationship between the ultimate underlying owner of the funds and the purchaser and consider beneficial ownership requirements. In addition, consideration must be given to verifying the identity of the ultimate underlying owner i.e. the provider of the funds. The source of funds form at **Appendix 4** can be utilised for this process.

Source of wealth is distinct from source of funds and describes the origins of a purchaser's financial standing or total net worth i.e. those activities which have generated a purchaser's funds and property. Information sufficient to establish the source of income or wealth must be obtained for all higher risk customers (including higher risk domestic PEPs and all foreign PEPs) and all other relationships where the service being requested makes it appropriate to do so because of its risk profile. For customers that are initially subject to EDD enhanced monitoring is a necessity, and the procedures that need to be adopted such as scrutiny of transactions are clearly set out and must be adhered to at all times.

## Companies

Businesses are required to put in place measures to identify the existence of beneficial owners. In verifying the beneficial owner's identity, the agent should be satisfied that they know who the beneficial owner is and understand how they operate. Beneficial owners are the individuals who ultimately own or control the customer or on whose behalf a transaction or activity is being conducted.

In the case of corporate bodies and partnerships, a beneficial owner is any individual who:

- Owns or control more than 25 per cent of the shares or voting rights or in the case of a partnership more than 25 per cent of the capital of profits of the partnership, or
- Exercises control over the management of the company.

In terms of documentary evidence for companies the required documentation should consist of the following:

- Certificate of Incorporation
- Memorandum & Articles of Association
- Register of Shareholders
- Register of Directors.

In addition there are occasions when it might be necessary to ask for further information regarding the company and these documents might include copy bank statements or a copy of the audited accounts to confirm the company's financial status if it is purchasing a property. If the company has been recently incorporated and has therefore not filed any accounts a company should consider obtaining references from the appointed accountants or certified copies of bank statements to confirm its existence. The use of companies to purchase and sell property has been a favoured method of those seeking to launder criminal funds, as they understand the difficulty they sometimes present to companies in terms of identifying the person(s) with ultimate control of the business.

If this company forms a business relationship with a legal person i.e. a company as a customer then it will request the documents be supplied to us as opposed to downloading any documents directly from Companies House. The obligation on the part of the customer to provide those documents is set out in Regulation 43 of the "Regulations". The only occasion when it is considered satisfactory to rely upon the information contained on the Companies House website is if it is appropriate to undertake Simplified Due Diligence in respect of the customer when the requirement is just to identify the customer as it is deemed the risk of money laundering is low. The following entities that this might apply to is set out in the section on undertaking SDD. It might be applicable to use open- source internet searches to assist in the process of identifying whether a business is suitable for SDD.

## Trusts

A trust is a way of managing assets (money, investments, land or buildings) for people. In practice they are an arrangement or construct where Party 'A' transfers ownership of assets to Party 'B', who manages them for the benefit of another Party 'C'. The parties concerned and their role in a trust are as follows:

Party 'A' – The 'Settlor' – The person(s) who put the assets into the Trust

Party 'B' – The 'Trustee' – The person(s) who manages the Trust

Party 'C' – The 'Beneficiary' – The person(s) who benefit from the Trust.

### What the settlor does

The settlor decides how the assets in a trust should be used – This is usually set out in a document called the 'Trust Deed'. Sometimes the settlor can also benefit from the assets in a trust and this is called a 'settlor-interested' trust and has special tax rules.

### What trustees do

The trustees are the legal owners of the assets held in a trust. Their role is to:

- Deal with the assets according to the settlor's wishes, as set out in the trust deed or their will
- Manage the trust on a day-to-day basis and pay any tax due
- Decide how to invest or use the trust's assets.
- If the trustees change, the trust can still continue, but there always has to be at least one trustee.

### Who are the Beneficiaries

There might be more than one beneficiary, like a whole family or defined group of people. They may benefit from:

- The income of a trust only, for example from renting out a house held in a trust
- The capital only, for example getting shares held in a trust when they reach a certain age
- Both the income and capital of the trust.

Trusts have been recognised as a corporate vehicle used by corrupt individuals to hide illicit funds. Like companies, the lack of transparency around who controls and benefits from trusts is abused to mask the identity of those who have criminal wealth to hide.

Trusts provide unparalleled secrecy, allowing individuals to disguise the ownership of assets while still benefitting from them. This creates huge legal barriers to creditors or anyone else seeking to make a claim against these assets. These features are significant additions to the simple anonymity that can be achieved by setting up an anonymous shell company.

In practice it can be relatively straightforward to identify the trustees of a trust as this is the organisation or individual(s) that an Estate Agency company is likely to have direct dealings with in terms of instructions to sell or purchase a property on behalf of a trust. However, the role of the settlor can be pivotal in terms of the funds used to establish a trust in the first instance. Therefore, all reasonable steps and measures must be undertaken to establish not just the trustees and beneficiaries but also the settlor.

Most Trusts are currently required to register with HMRC and Estate Agents are required to obtain a copy of the trust register when completing customer due diligence. The copy should be cross-referenced with the trust documents received and the Trustees notified if any discrepancies become apparent in order that the correct details can be re-registered.

However, by adopting a Risk Based Approach it will depend to certain extent as to when and where the trust was established and its purpose as to how much risk the trust poses in terms of money laundering or terrorist financing. Clearly each case must be judged on merit, but it is essential that when dealing with a trust its purpose is understood and those who have ultimate control of it are identified.

## Register of Overseas Entities

The register of overseas entities (ROE) as administered by Companies House requires overseas entities who want to buy, sell or transfer property or land in the UK, to register with Companies House and tell Companies House who their registrable beneficial owners or managing officers are.

### Requirement to report discrepancies in register

If the customer is a business, the relevant person must collect proof of registration or an extract of the register, before a business relationship is established, to show the business:

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

From 1 April 2023, where your customer is a company, unregistered company, limited liability partnership, eligible Scottish partnership, trust, or an overseas entity, you must either collect an extract of the register which contains full details of the information held or establish (from inspection of the register) that there is no information held at that time. This must be done before establishing a business relationship, and as part of ongoing monitoring.

The information required is as follows:

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

**If you identify a material discrepancy while undertaking CDD or ongoing monitoring, these must be reported as soon as possible.**

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

- Be linked to money laundering or terrorist financing, or
- Conceal details of the business of the customer.

**Discrepancies are in the form of:**

- A difference in name
- An incorrect entry for nature of control
- An incorrect entry for date of birth
- An incorrect entry for nationality
- An incorrect entry for correspondence address
- A missing entry for a person of significant control or a registrable beneficial owner
- An incorrect entry for the date the individual became a registrable person.

**A material discrepancy must be reported to**:

- Companies House – If it relates to a company, an unregistered company, a limited liability partnership or an eligible Scottish partnership or an overseas entity
- HMRC – If it relates to a trust.

## Reliance on a Third Party

Regulation 39 of the 'Regulations' state that a company can rely upon the CDD undertaken by another "Relevant Person" who for the purposes of the 'Regulations' are those individuals or entities operating within the regulated sector and therefore subject to the 'Regulations' as set out in Regulation 8, and they include the following:

- Credit and financial institutions
- Auditors, insolvency practitioners, external accountants and tax advisers
- Independent legal professionals
- Trust or company service providers
- Estate agents
- High value dealers
- Casinos.

In order to rely upon the CDD undertaken by a third party, certain conditions must be in place as follows:

- The “third party” must be a “relevant person” for the purposes of the ‘Regulations’ as set out in Regulation 8
- There is an arrangement between both parties for the CDD to be relied upon by the “requestor” and therefore in other words the “third party” i.e. the provider of the CDD has to consent in effect
- The “third party” must provide the documents obtained as part of the CDD process to the “requestor”
- The documents used for identification and verification documents must be provided to the “requestor” immediately upon request
- The documents that the “third party” has in their possession must be retained in line with the ‘Regulations’ i.e. 5 years from the date that reliance was agreed upon
- The “requestor” remains liable for any failures by the relevant person for failure to apply satisfactory CDD measures.

The important point to note is that if this company relies on a “third party” for the purposes of CDD then it will remain responsible for any failure to apply due diligence measures appropriately. This is particularly important when relying on a person outside the UK. Reliance upon another person to undertake our customer due diligence checks could be considered a risk in itself and a risk assessment should therefore be completed if the reliance request is refused then this company will document and provide a clear audit trail of the steps undertaken to obtain the customer due diligence.

In practice this company will always seek to conduct its own CDD in relation to both the seller and the purchaser unless there are circumstances where it is felt that it is practical to place reliance on a “third party”. However, the key issue is that this company will only ever rely upon the CDD conducted by a third party if it is satisfied that the “third party” has undertaken a level of CDD that meets the conditions set down by the “Regulations”. If there is any doubt or concern relating to the level of CDD that has been conducted, then this company will always undertake its own CDD in relation to both seller and the purchaser.

The document found at **Appendix 6** can be used to confirm there is a written agreement in place with another “relevant person” for the reliance on CDD undertaken by that “third party”. A copy of the form should be provided to the “third party” so that they are fully aware of their own

obligations when it comes to the retention of documentation used for CDD purposes. It is essential to point out that if there is a refusal on the part of the third party holding the CDD this company has to show that it has attempted to obtain the CDD undertaken and therefore a written record must be retained of any request made to the third party.

If a third party or intermediary representing the customer supplies documentation for CDD purposes directly to this company on behalf of the customer, it is important to remember that this company is not seeking to place "reliance" upon it but just to receive documents this way and undertake the necessary due diligence itself.

The issue of reliance will be most relevant when a company has a sub agency or joint-sole agency agreement in place or has formed a business relationship with a Property Finder or Relocation Agent. In these circumstances it must be remembered that the CDD will have to be obtained from the buyer or seller with whom a business relationship is not directly formed as well as the other property professional themselves as defined by Section 1 of the Estate Agents Act 1979. The practical steps that need to be taken in each scenario are as follows:

**Sub-Agency Agreement**

The 'main agent' i.e. the selling agent must undertake CDD on the seller and the 'sub-agent' must undertake CDD on their client i.e. the buyer. The main agent then should seek the CDD undertaken on the buyer by the sub-agent and vice versa. Both the 'main agent' and 'sub-agent' should also undertake Simplified Due Diligence on each other as they are forming a business relationship in line with the "regulations". This SDD should just consist of the existence of the firm, the registered office, list of company officials i.e. directors and confirmation of their registration with HMRC for AML purposes.[8]

**Joint Sole Agency Agreement (split fee)**

This will occur where two agents are selling the same property and agree to split the fee when a buyer is found. In this scenario both agents are required to undertake the CDD on the seller their client. However, it is acceptable for just one of the agents to carry out the CDD and the other agent to place reliance upon the CDD undertaken to avoid potential duplication of the process.

[8] https://www.gov.uk/guidance/money-laundering-regulations-supervised-business-register

Whichever party then finds the buyer is required to carry out the due diligence on the buyer with the other agent looking to place “reliance” upon it. Both agents are then required to undertake due diligence on each other as previously stated in the sub-agency agreement.

**Property Finder, Buyer or Relocation Agent**

This situation is very similar to the sub-agency agreement in that the main agent i.e. the selling agent will undertake CDD on the seller with the property finder undertaking CDD on their client the buyer. Both sides should seek to obtain the CDD undertaken by the counterparty to the transaction as well on each other as previously stated.

## Data Protection & Record keeping

**Data Protection**

Consistent with our Data Protection Policy, this company is committed to complying with all legal and regulatory record keeping requirements and as such, the NO/MLRO has designed a system for us to store separate from the routine client files the documents and information obtained to satisfy the AML CDD requirements in accordance with Regulation 40 of the ML Regulations (AML Records).

Some of the information and documents collected may include personal data. Personal data obtained by the company may only be processed for the prevention of money laundering and terrorist financing or where use of the data is allowed by other legislation or after obtaining the consent of the data subject. It is strictly against our policy and the law to use personal data obtained in the process of applying this Policy for competitive or commercial purposes.

The company will retain records obtained to satisfy the customer due diligence requirements for AML purposes that we hold on customers and transactions in accordance with Regulation 40 of the “Regulations”. These records will consist of documents and information that may be crucial in any subsequent investigation by bodies such as the NCA, the Police, or HMRC. They will enable the company to produce a sound defence against any suspicion of involvement in money laundering or terrorist financing or charges of failure to comply with the Regulations.

This company must keep evidence of customer’s records for five years from the date on which the transaction is complete, or that the business relationship has come to an end. Records relating to CDD for the prevention of money laundering or terrorist financing can only be kept beyond 5 years under the following conditions:

- Consent of the customer
- By or under any enactment
- Court proceedings
- Reasonable grounds for believing needed to be retained for legal proceedings.

Nominated Officer records relating to external reports made to the NCA, internal reports not disclosed to the NCA and details of on-going law enforcement enquiries must be retained indefinitely or at least until the company has received confirmation from the NCA or law enforcement that the records concerned are no longer required.

It is vital that all documents and data relating to the AML process including client and purchaser risk rating, CDD forms and copies of documents used for the verification of ID are kept separate from the normal client file correspondence. This will prevent the client inadvertently being provided with a copy of the AML records if they request any other information or copies of documentation from the file.

However, if any issues arises during the relationship with the customer that gives rise to a suspicion of money laundering or terrorist financing, and results in a referral to the Nominated Officer then the sub folder containing the CDD documents should be retained separately and securely by the Nominated Officer together with any correspondence or documents generated as a result of the money laundering or terrorist financing issue such as the internal SAR, e-mails or records of telephone conversations with the client or purchaser that relate specifically to the AML issue. It is essential that the decision-making process surrounding the business relationship is formally documented and retained in the AML file that has been generated.

## Training

The primary objective of AML training is to establish and maintain an appropriate level of competency to ensure that the staff fulfil their roles in protecting the company from money laundering or terrorist financing. Compliance with statutory and regulatory obligations should flow as a by-product.

In order to achieve this, all members of staff will receive high quality bespoke formal training which is relevant to the role of the staff member either from the Nominated Officer or from an external contractor.

Regulation 24 of the “Regulations” does not specify how regularly staff need to receive AML training, however HMRC have stated that they expect all frontline staff and those responsible for

the financial aspect of the business to receive some formal training every 2 years. Therefore this company will seek to ensure that new members of staff will receive some form of formal training as soon as practicable after being appointed, and existing members of staff should receive some form of refresher training on a regular basis.

The objectives of any AML training include:

- Encouraging staff to be vigilant at all times
- Making staff aware of their legal obligations
- Demonstrating why certain services are vulnerable
- Educating staff in the recognition of unusual or suspicious transactions
- Making staff aware of the organisation's AML policy and procedures
- Educating staff in the importance of quality CDD
- Identifying the Nominated Officer, Deputy Nominated Officer, and reporting procedures
- Reference to industry guidance and other sources of information, e.g. the NCA.

The Nominated Officer as they may become involved with on-going monitoring of business relationships and other internal control procedures, might require different training, tailored to their particular function. It is an essential element of this proper formal training that everyone must read and understand the contents of this manual. Every member of staff should complete an acknowledgement that they have complied with the requirement to read the Manual and re-read when a potential money laundering or terrorist financing issue is identified.

In the event of any lack of clarity or ambiguity, it is the employee's responsibility to raise those issues with the Nominated Officer and to ensure appropriate further discussions and if necessary further training. If the Nominated Officer feels it is appropriate, they should seek the guidance and advice of a suitably qualified AML external consultant in terms of both training and regulatory concerns.

The Nominated Officer will be responsible for provision of up-to-date resources and materials in respect of money laundering or terrorist financing, and such resources will be available to members of staff.

Training itself must cover all of the key aspects of the AML regime and will include the topics:

- What is money laundering and issues for the Real Estate Sector
- Proceeds of Crime Act 2002
- Money Laundering Regulations 2017

- Recognition of 'Red Flags'
- Politically Exposed Persons
- Financial Sanctions.

As previously stated, the training itself can either be provided "in-house" through engaging the services of an external company that specialise in this field, online training or employees will attend an external AML course provided by an external contractor. Any significant updates to the AML legislation that require additional training can be provided by the Nominated Officer of the company.

A Training record must be kept of all persons who attend either internal or external training and a training attendance template form can be found at **Appendix 10**. Employees who do not make themselves conversant with the legislation leave themselves and the company wide open to regulatory, and even possibly criminal action by failing to meet their obligations.

# Chapter 8 – SUSPICIOUS ACTIVITY REPORTING PROCEDURE

## National Crime Agency

The NCA is the UK 'Financial Intelligence Unit' and as such has responsibility for collating and disseminating all of the Suspicious Activity Reports (SARs) submitted by the regulated sector. It also has responsibility for receiving all 'Defence Against Money Laundering' [DAML] requests from regulated companies to undertake transactions which the reporting company have considered to be suspicious in terms of money laundering or terrorist financing.

## Internal reporting procedure

Once a member of staff forms the suspicion or knowledge or has reasonable ground to suspect that money laundering or terrorist financing is taking place either by the client or the purchaser, or a transaction or relationship that either is concerned with, then they should notify the Nominated Officer immediately. This can be done verbally initially but must always be supported by a written internal report. The template form at **Appendix 9** should be used by a member of staff for the filing of an internal SAR as this will ensure the correct information is supplied to the Nominated Officer on every occasion that there is suspicion of money laundering and will allow the Nominated Officer to fully evaluate what is being alleged.

Once the employee has made the internal report to the Nominated Officer, they have complied with the money laundering legislation, namely section 330 of POCA. Upon receiving an internal report from a member of staff the Nominated Officer should undertake an evaluation process which should be documented. The 'evaluation records' formalise the evaluation process and prevent ad-hoc decision making. Nominated Officer evaluation records also have the advantage of providing the company with a valuable evidential record of the evaluation process that demonstrates the seriousness with which the company take their money laundering or terrorist financing obligations.

The Nominated Officer evaluation record should include:

- Nature of report received, and reasons given for it
- Details of internal and external CDD information that has been obtained and considered
- Summaries of discussions with colleagues
- Details of any further information obtained from the reporting employee
- The decision and reason for the course of action undertaken.

The Nominated Officer evaluation record should be maintained together with the internal SAR. Therefore, the Nominated Officer will not simply make an external report to the NCA based on the information provided without conducting their own investigations into the information provided and this will include verification of the CDD already provided together with further enquiries to ascertain any further information that will assist the decision-making process and whether to refer the matter to the NCA or not.

Any decision to make an external report to the NCA should be commented upon by a Senior Manager and noted on the money laundering client file. This will ensure that all levels within the company are aware of the money laundering or terrorist financing risk exposure and address any issues that are forthcoming as a result of the action undertaken.

It is possible that the Senior Manager will have to liaise directly with the customer if the situation is taken to exit the relationship and they therefore need to be fully aware of the facts surrounding the matter.

## Suspicious activity reporting to the NCA

Once the requisite level of suspicion or knowledge has been formed that the company is concerned with a money laundering or terrorist financing issue, the Nominated Officer or Deputy Nominated Officer must complete and file a 'Suspicious Activity Report' (SAR) with the NCA. The SAR will detail the exact nature of the customer relationship and the transaction or activity that has given rise to the suspicion of money laundering or terrorist financing.

The value of SAR's has been shown to:[9]

- Provide information and intelligence to law enforcement that is predominantly used in relation to financial crime and money laundering or terrorist financing
- Provide information that assists in ongoing operations such as telephone numbers, addresses, alias identities, companies, investment activity, bank accounts and other assets
- Help identify organised criminal schemes, for example mortgage and boiler room frauds, enabling detection and prevention activity including the issue of alerts to businesses at risk from such activity
- Multiple SARs on the same subject or company can identify new targets for operational activity

[9] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports

- Information leads to the recovery of the proceeds of crime by assisting in restraint orders, confiscation orders and cash seizures
- Provide intelligence about criminal methods, contribute to the UK's understanding of crime and inform strategies to reduce the impact of crime
- Can help establish a geographical picture or pattern of the vulnerability of a particular sector or product and can be used in the analysis of suspicious activity before and after a specific event e.g. a terrorist incident.

There are two objectives for filing a SAR with the NCA. The first reason might be for intelligence purposes i.e. informing the NCA of what is suspicious activity in terms of money laundering or terrorist financing.

The second purpose of filing a SAR is that in addition to informing the NCA of the activity concerned, the reporting organisation might be seeking permission to continue with the transaction and is requiring what is called a 'Defence Against Money Laundering' (DAML) in respect of the main offences under Section 327 - 329 POCA 2002.

The responsibility for liaising directly with the NCA rests with the Nominated Officer or Deputy Nominated Officer, and any requests for further information or documentation should be forwarded directly to them and this will include the service of any court orders.

## Defence Against Money Laundering' (DAML) & Timescales

As stated above the company might on occasions be required to submit a SAR request to the NCA in order to continue undertaking a transaction on behalf of a customer or continuing with a business relationship. This DAML request will be done online using the same SAR form. This scenario will occur when the customer is still wishing to engage the services of this company and as stated the company is seeking permission to continue with the business relationship.

However, it should be borne in mind that the NCA will not provide what should be considered as "consent" for an actual transaction because they will not be in a position to clarify whether the funds are in effect "clean" and not the proceeds of criminal activity.

This fact is outlined by them in their SAR guidance [10]:

*"the term 'consent' is frequently misinterpreted. Often it is seen as seeking permission or that where requests are granted that this is a statement that the funds are clean or that there is no criminality*

[10] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports

*involved. This is not the case. Additionally, reporters sometimes seek 'consent' where they have been unable to complete customer due diligence. The process is not a substitute for taking a risk-based approach or for fulfilling your regulatory and legal responsibilities, including those under the Money Laundering Regulations 2017."*

The NCA further state that such misinterpretation and conduct risks undermining efforts to prevent money laundering or counter terrorist financing. As such the granted letters from the NCA no longer use the term 'consent' and instead use the terms 'Defence Against a Money Laundering offence'.

Once received the NCA will acknowledge the DAML request and then have 7 working days in which to respond to the request. During that time, the company can under no circumstances conduct any transactions on behalf of the customer or inform them that a disclosure has been made to the NCA otherwise the employee will be potentially guilty of 'Tipping Off' under section 333A of POCA 2002.

The DAML period of 7 working days will commence the next working day after the NCA have acknowledged the request. Therefore, as an example, if a DAML request is filed and acknowledged at 2pm on a Tuesday the 7 working days will commence from 9am the following day, on the Wednesday.

After the DAML period has elapsed, if the NCA have not responded with a decision, then the company should make a decision as to whether they want to carry on with the business relationship. This scenario is very unusual, and a company can normally expect to receive a response from the NCA. However, because there was suspicion of money laundering leading to a DAML request in the first instance, the customer relationship should be monitored very closely, and accurate records kept of all instructions or communications between the employee and the customer.

If further issues arise which result in suspicion of money laundering or terrorist financing being formed, consideration should be given to filing an additional SAR and seeking a further DAML.

The most likely course of events is that prior to end of the 7 working day period from when the SAR was filed, the NCA will contact the company with one of two responses. The first response will be that based upon the information supplied to them, they do not object to the transaction continuing and they are effectively providing the company with a statutory defence to the s.327-s.329 offences under POCA. The worded response will be to the effect of:

*"We confirm that with effect from XXXXX you have a criminal defence to one of the principal money laundering offences under sections 327, 328 and 329 POCA in relation to the acts specified in your disclosure and any updates made to that disclosure. This decision has been made by the NCA in accordance with Home Office Circular 29/2008".*[11]

However, in their correspondence they will make it clear in that it does not excuse the company from its obligations under the "Regulations" notably in respect of undertaking CDD satisfactorily. Therefore, before continuing the relationship with the customer the company must be satisfied that it has taken all reasonable steps and measures to comply with the "Regulations".

The alternative response from the NCA could be a refusal to continue undertaking any work on behalf of the customer, and therefore effectively a suspension of the business relationship. If this is the case, then there is what is called a "moratorium period" of 31 days from the date of the refusal for the transaction to proceed. During the "moratorium period" the NCA must take action, either through seeking a Freezing or Restraint Order from the courts in relation to the funds that are subject of the suspicious activity in question. It should be noted that the 31 days includes weekends and Bank Holidays.

Once the initial 31-day period has lapsed, and upon application to a Crown Court Judge, the "moratorium period" can be extended for periods of 31 days at a time, up to a maximum of 217 days in total i.e. 6 x 31-day extensions to the initial period.

Again, under no circumstances can the customer be informed during the "moratorium period" that a disclosure has been made to the NCA otherwise the employee could be guilty of 'Tipping Off'.

There might be occasions when information comes to light after a transaction has been undertaken or a business relationship has ended which causes the employee to form a level of suspicion or knowledge of money laundering or terrorist financing relating to the customer. If this is the case it is essential that the same reporting procedures are followed and if necessary, a report is filed with the NCA as this will protect the company from any comeback some time down the line.

[11] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports

It is important that the SAR sets out what information has come to light subsequent to the transaction/business relationship ending, and why suspicion of money laundering or terrorist financing was not formed at the time.

# Chapter 9 – HIGHER RISK CUSTOMERS

## Politically Exposed Persons (PEPs)

The "Regulations" define a PEP as an individual *'who is entrusted with prominent public functions, other than as a middle-ranking or more junior official'.*

Due to their public position/occupation and the associated increased exposure to bribery and corruption, PEPs potentially present a higher risk of money laundering or terrorist financing. The level of risk associated with any PEP, family member or close associate (and the extent of EDD measures to be applied) must be considered on a case by-case basis.

Those individuals who would be classed as PEPs include:

- Heads of state, heads of government, ministers and deputy or assistant ministers
- Members of parliament or of similar legislative bodies
- Members of the governing bodies of political parties
- 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
- Members of courts of auditors or of the boards of central banks
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces
- Members of the administrative, management or supervisory bodies of State-owned enterprises
- Directors, deputy directors and members of the board or equivalent function of an international organisation.

In addition to the PEP, 'family members' and 'known close associates' are captured within the legislation and the Regulations defines these as:

"family member" of a politically exposed person includes:

- A spouse or partner of that person
- Children of that person and their spouses or partner
- Parents of that person
- Siblings of that person.

"known close associate" of a politically exposed person means:

- An individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relations with a politically exposed person

- An individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a politically exposed person.

For the purpose of deciding whether a person is a known close associate of a PEP, a relevant person need only have regard to information which is in its possession, or to credible information which is publicly known.

The "Regulations" now crucially include domestic PEPs as well as foreign nationals and this will include Members of Parliament. The FCA published in July 2017 guidance as to the level of seniority within the judiciary and the armed forces[12]. The company will adopt a Risk Based Approach when it comes to the level of CDD required for a domestic PEP. It is possible that certain characteristics such as source of wealth will be easier to identify and confirm with a domestic PEP and the extent of the EDD undertaken will be considered on a case-by-case basis.

Foreign PEPs as defined, should always be considered as high risk and therefore subject to EDD and any introduction into the company must always be referred to the Nominated Officer. EDD might involve establishing a source of wealth in addition to the source of funds relating to the actual property transaction. In terms of source of wealth there are four main factors that should be considered:

- Current income
- Family estates
- "Explained" (independently verified) source of wealth and funds from previous positions
- Business undertakings.

Clients initially subject of EDD require enhanced monitoring of the business relationship and this might include an increasing number of controls, timing and pattern of transactions. Decisions relating to PEPs should be recorded accurately and set out the decision-making process concerned with the initial "on-boarding" of the customer and the ongoing management of the client.

Ongoing monitoring might consist of scrutiny of transactions undertaken throughout the course of the relationship to ensure that they are consistent with knowledge of customer, business and risk profile.

[12] https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering

At the time of forming a business relationship the company will use online verification services provided by Veriphy to ascertain whether an individual is a PEP.

If there are concerns that give rise to a suspicion that a client is a PEP, but we have no data source service provider confirmation of the fact, we may use the PEP Questionnaire found at **Appendix 7**. It is accepted that this represents self-declaration and consideration should be given to open-source research in addition to the manual checking process.

The use of the CDD & Risk Analysis template forms at **Appendix 2 & 3** of the manual provides the employee with adequate opportunity to record the customer as a PEP and therefore potentially high risk, and highlight the procedures undertaken to manage and mitigate the exposure to that risk. A person is still classed as a PEP, twelve months after ceasing the role that categorised them as a PEP in the first instance. However, this period can be extended at the discretion of the Nominated Officer or Director of the company if they deem the person still presents a higher risk beyond their official classification as a PEP.

## Higher Risk Jurisdictions

There are three main reasons why a country might be classed as higher risk, either a country with weak or non-existent anti-money laundering controls, connections with terrorism or historically it has higher levels of corruption. There are three lists of countries that have been identified as posing a higher risk in terms of money laundering and therefore where EDD should apply. The first is the EU Commission, the second is the Financial Action Task Force (FATF) and the UK via HM Treasury is the third organisation to publish its own list of high-risk countries.

All three published lists vary slightly in terms of the jurisdictions identified as higher risk, as their criteria for reaching their conclusion might differ, but there has been more of an alignment when it comes to the countries concerned. The lists change regularly, so it is important to check them at the time of a pending transaction.

It may be worth referring to the following websites for up to date information relating to higher risk countries: Know Your Country[13], and FATF List[14]. These can be used as a reference tool for obtaining up to date information as regards to individual jurisdictions when it comes to FATF mutual evaluations.

[13] https://www.knowyourcountry.com/
[14] http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2022.html

## Financial Sanctions

In the UK, the regulation of financial sanctions is the responsibility of the 'Office of Financial Sanctions Implementation' ("OFSI") which is part of HM Treasury. The OFSI is responsible for:

- The implementation and administration of international financial sanctions in effect in the UK
- Licensing exemptions to financial sanctions
- Domestic designations under the Terrorist Asset-Freezing etc. Act 2010
- Directions given under Schedule 7 to the Counter-Terrorism Act 2008.

The OFSI maintain a consolidated list of all organisations and individuals who are the subject of sanction controls, and this database is publicly available and updated every 24 hours:

OFSI Database[15]

Financial sanctions may apply to individuals, entities and governments, who may be resident in the UK or abroad. Certain financial sanctions may also prohibit providing or performing other financial services, such as insurance, to designated individuals or governments. It is a criminal offence to breach a financial sanction, without an appropriate licence or authorisation from the Office of Financial Sanctions Implementation.

A company is prohibited from carrying out certain activities or behaving in a certain way if financial sanctions apply and will depend on the exact terms of the EU or UK legislation which imposes the financial sanction in the given situation. The penalties for a breach of financial sanctions were initially contained within Terrorist Asset- Freezing Act 2010 but these have now been amended by the Policing & Crime Act 2017.

The offences imposed can be broadly described as:

- Dealing with the funds or economic resources of a designated person
- Making funds or economic resources, or in the case of terrorism financial services, available directly or indirectly to a designated person
- Making funds or economic resources, or in the case of terrorism financial services, available for the benefit of a designated person
- Knowingly and intentionally participating in activities that would directly or indirectly circumvent the financial restrictions, enable or facilitate the commission of any of the above offences.

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

This type of customer is extremely high risk and therefore would require immediate referral to the Nominated Officer to report to the OFSI that a designated person is attempting to use the EAB service. The Nominated Officer will then be in a position to make  a decision as to whether the company is prepared to take on this type of customer and if required liaise with the OFSI with regard to a potential licence that may be in place for the designated person the licence would need to ensure there is no breach of the legislation, especially in light of the severe penalties for breaches.

Failure to comply with the UK sanctions lists could result in 7 years in prison, a fine, or both so therefore immediate referral to the Nominated Officer is essential.

The company may use the OFSI website above to 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. The company may file a Terrorist SAR in relation to a designated person.

# Chapter 10 – ANTI-BRIBERY & CORRUPTION

## What is Bribery

The Bribery Act 2010 is the principal legislation covering bribery and corruption offences. Bribery is related to money laundering or terrorist financing, professional ethics, and good corporate governance.

A bribe is defined widely as a financial or other advantage and is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage. A bribe can be of low or high value.

Matters such as promotional expenses and hospitality must be analysed in the context of the Bribery Act, although transparency, proportionality, and the companies' procedures, are likely to be taken into consideration by prosecuting authorities. There are four offences under the legislation which are:

- General offences of 'Active Bribery' (bribing another) and Passive Bribery (being bribed)
- Commercial offences of 'Bribing a foreign official' and 'Failure of commercial organisations to prevent bribery'.

It is the company's policy to conduct all of its business in an honest and ethical manner and the company will take a zero-tolerance approach to bribery and corruption and is committed to acting professionally, fairly and with integrity in all our relationships and business dealings wherever we operate and to implementing and enforcing effective systems to counter bribery. This policy applies to all of the company's employees.

The company and its employees will uphold all laws relevant to countering bribery and corruption. The company remains bound by the laws of the UK, including the Bribery Act 2010, in respect of its conduct both at home and abroad.

The purpose of this policy is to:

- Set out our responsibilities, and of those working for the company, in observing and upholding our position on bribery and corruption, and
- Provide information and guidance to those working for the company on how to recognise and deal with bribery and corruption issues.

Bribery and corruption are punishable for individuals by up to ten years' imprisonment and if found to have taken part in corruption an employee could face an unlimited fine and face damage to this company's reputation.

Therefore, it is essential the company takes its legal responsibilities very seriously. In order to do this it will ensure that it:

- Limits corporate hospitality to events with adequate commercial rationale
- Discourages the giving or receipt of cash gifts.

The following are examples of both types of behaviour associated with bribery:

**Offering a bribe**

An employee offers customers tickets to a major sporting event, but only if they agree to do business with us.

This would be an offence as they are making the offer to gain a commercial and contractual advantage. The employee may also be found to have committed an offence because the offer has been made to obtain business for the company. It may also be an offence for the potential customer to accept their offer.

**Receiving a bribe**

A customer gives a relative of an employee a job but makes it clear that in return they expect them to use their influence in their organisation to ensure that this company continues to do business with them. It is an offence for a supplier to make such an offer.

It would be an offence for an employee to accept the offer as they would be doing so to gain a personal advantage.

## Hospitality and Gifts

This policy does not prohibit normal and appropriate hospitality (given and received) to or from third parties and the giving or receipt of gifts.

Normal and appropriate hospitality and gifts would include where the hospitality or gift:

- Is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits
- Complies with local law

- Is given by this company not in your name
- Is only offered or accepted with the prior approval of the Nominated Officer
- Does not include cash or a cash equivalent (such as gift certificates or vouchers
- Is appropriate in the circumstances. For example, in the UK it is customary for small gifts to be given at Christmas time
- Taking into account the reason for the gift, is of an appropriate type and value and given at an appropriate time
- Is given openly, not secretly
- Is not offered to, or accepted from, government officials or representatives, or politicians or political parties, without the prior approval of the Nominated Officer.

## What is not acceptable

It is not acceptable for an employee (or someone on their behalf) to:

- Give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given
- Give, promise to give, or offer, a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure
- Accept payment from a third party that they know or suspect is offered with the expectation that it will obtain a business advantage for them
- Accept a gift or hospitality from a third party if they know or suspect that it is offered or provided with an expectation that a business advantage will be provided by this company in return
- Threaten or retaliate against another worker who has refused to commit a bribery offence or who has raised concerns under this policy
- Engage in any activity that might lead to a breach of this policy.

## Staff responsibilities

All staff must ensure that they read, understand and comply with this policy. The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for this company or under its control. All employees are required to avoid any activity that might lead to, or suggest, a breach of this policy.

Staff must notify the Nominated Officer or a Senior Staff member as soon as possible if they believe or suspect that a conflict with this policy has occurred or may occur in the future. For

example, if a third party or potential third party offers an employee something to gain a business advantage with us or indicates that a gift or payment is required to secure their business. Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct.

If an employee is a victim of bribery or corruption, they must notify the Nominated Officer or Senior Manager as soon as possible.

# Appendices

# 1. ANTI-MONEY LAUNDERING RISK ASSESSMENT

# AML RISK ASSESSMENT

As part of a 'Risk Based Approach' in relation to AML / CTF, this company will perform a Risk Assessment in order to establish and maintain appropriate risk-sensitive policies and procedures. The Risk Assessment will be used to identify the inherent risk it faces as a result of the business it is engaged in, and then to adopt policies and procedures to mitigate those risks that will be approved by a Senior Manager(s).

The Risk Assessment in accordance with Regulation 18 of 'The Money Laundering Regulations 2017' takes into account the following risk factors:

i. Customers

ii. Countries or geographic areas

iii. Products or Services

iv. Transactions

v. Delivery channels

The AML Risk Assessment must be undertaken on a regular basis and especially if there are significant changes to the inherent risks that the company is exposed to. It is recommended that the information ascertained by undertaking the Risk Assessment is reviewed at least annually.

## Instructions

- Complete the assessment by considering whether the specified risks affect your practice and ticking YES or NO as appropriate.
- Should your answer identify a risk, then proceed to outline the risk level and action or control measures you are currently implementing, or proposing to implement, to manage the risk by using the additional form if necessary.
- Should a risk not be applicable, please modify the template accordingly, or mark the risk as N/A. Should a risk or risks affect your company that are not identified, add these to the appropriate section and complete them in the same manner.
- The AML Policy & Procedures should be used as guidance in order to identify the definition of PEPs, Beneficial Owners, Enhanced Due Diligence etc.

| AREA AND NATURE OF RISK | YES | NO | ACTION or CONTROL IMPLEMENTED (describe actions taken, or propose to take, to mitigate the risks) | Risk Level: High/Med/ Low |
|---|---|---|---|---|
| **CLIENT ACCEPTANCE AND ONGOING MONITORING** | | | | |
| **1. Client Risk Rating** Does the company conduct a risk rating assessment of every new client and a when a change occurs in the business relationship of existing clients. | | | | |
| **2. Non-face-to-face customers**: Have any clients or client representatives not been met face-to-face/not been physically present for identification purposes (for example, you are providing services by email/telephone, or providing services through an agent) | | | | |
| **3. Politically exposed persons (PEPs):** Do you ascertain whether your clients are PEPs? Do you have any clients who are PEPs | | | | |
| **4. Complex business ownership structures**: Do any clients have complex business ownership structures with the potential to conceal underlying beneficiaries (for example, trusts or legal entities established to hold assets, or entities based offshore) | | | | |
| **5. Beneficial owners**: Do you take all reasonable measures to identify beneficial owners and, where applicable, verify their identity | | | | |
| **6.** Client due diligence: Do you have standard client due diligence and enhanced client due diligence procedures for client acceptance and the ongoing monitoring of clients | | | | |

| | | | | |
|---|---|---|---|---|
| **7. Enhanced due diligence (EDD):** Have EDD measures been applied to all relevant clients (i.e. non-face-to-face clients, clients who are PEPs, and clients that have been assessed as higher risk) | | | | |
| **8. Longstanding and well-known clients:** Do you have up to date CDD information recorded for any longstanding and well-known clients | | | | |
| **9. Reliance**: Do you use any agents or intermediaries or rely on CDD that has been performed by another party | | | | |
| **10. Ongoing monitoring**: Have you conducted ongoing monitoring of all client relationships, including scrutiny of transactions, ensuring consistency of activity with the known client profile, and ongoing consideration of the business and risk profile | | | | |
| **11. Ongoing monitoring (EDD):** Have you conducted more stringent ongoing monitoring as appropriate, on a risk-sensitive basis, for client relationships that are higher risk | | | | |
| **12. Reapplying CDD/EDD:** Do you reapply CDD/EDD as appropriate, on a risk-sensitive basis (for example, when the nature of the business relationship changes and when the structure of the client changes or periodically) | | | | |

| **COUNTRIES OR GEOGRAPHIC AREAS** | | | | |
|---|---|---|---|---|
| 13. **High risk locations**: Are any clients based in, or conducting business in or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of bribery, corruption, terrorist activity, organised crime or drug production/distribution | | | | |
| 14. **Links with overseas real estate companies**: Does the company have a relationship with an overseas registered real estate company and if so in what capacity | | | | |
| 15. **Financial Sanctions**: Does the company have any clients who are the subject of financial sanctions or are known to have a business relationship or association with a jurisdiction that is the subject of sanctions | | | | |

| **PRODUCTS AND SERVICES** | | | | |
|---|---|---|---|---|
| 16. **Cash based clients**: In respect of clients who are Legal Persons is the company aware of companies that handle large amounts of cash takings, or receive payments from customers that are predominately in cash | | | | |
| 17. **Client services**: Do any clients request the purchase or sale of real estate that have no apparent economic or visible purpose, or conduct business in unusual circumstances (for example, requesting the sale of a property that is considerably undervalued) | | | | |
| 18. **Terms of engagement**: Do your terms of engagement outline the scope of services to be provided and outline your AML/CTF legal and regulatory obligations | | | | |
| 19. **Charities & NPOs**: Does the company have any charities or Non-Profit Organisations as clients and have all reasonable measures been undertaken to establish the Trustees of such organisations or those have significant control over them | | | | |

| **TRANSACTIONS** | | | | |
|---|---|---|---|---|
| 20. **Complex transactions**: Do you have any clients engaged in large or complex transactions | | | | |
| 21. **Source of funds**: Are there clients or services where the source of funds has not, or cannot be ascertained and verified | | | | |
| 22. **Cash payments**: Does your practice accept payments in cash or payments in advance for services yet to be provided | | | | |
| 23. **Banking facilities**: Does the company use internet banking facilities in order to undertake transactions | | | | |
| 24. **International transactions**: Is the company required to either remit or receive payments from overseas jurisdictions | | | | |
| 25. **Correspondent Banking**: Does the company use correspondent Banks to undertake such transactions and is EDD considered in relation to those transactions. | | | | |

| **DELIVERY CHANNELS** | | | | |
|---|---|---|---|---|
| 26. **Client markets**: What are the target client markets and segments e.g. are they mainly domestic | | | | |
| 27. **Online services**: Are any of the services provided by the company conducted solely online without the requirement for direct contact with the client | | | | |
| 28. **Client contact**: Are a high percentage of the business relationship with a client conducted on a non- face to face basis | | | | |
| 29. **Intermediaries**: Does the company use introducers or intermediaries and what is the nature of their relationship with the company | | | | |

| | | | | |
|---|---|---|---|---|
| 30. **Use of intermediaries**: If intermediaries are used are they a regulated person subject to AML regulations consistent with the UK regime and are there any indications that the intermediary level of compliance with AML regulation is inadequate such as sanctions in relation to AML / CTF obligations. | | | | |
| 31. **Independent verification**: Does the company use a reliable and independent source in order to undertake CDD | | | | |
| 32. **Client introductions:** Have any clients been introduced to the company by other organisations within the regulated sector (e.g. estate agents, accountants etc.) | | | | |
| **STAFF TRAINING** | | | | |
| 33. **AML Policies & Procedures:** Does the company have a current AML policies and procedures manual that is in an electronic format stored on the company's computer system and also a paper format both of which are accessible to all members of staff. | | | | |
| 34. **AML Manual content** : If the answer to the above is yes does the manual clearly set out the roles and responsibilities of all members of staff in relation to AML / CTF including the legislation and the procedure for reporting suspicious transactions and activity by a client. | | | | |
| 35. **Training provision:** Has the Nominated Officer undertaken appropriate training to understand and meet their AML/CTF obligations, with adequate records maintained (for example, materials read, events and conferences attended, relevant dates, content covered) | | | | |

| | | | | |
|---|---|---|---|---|
| 36. **Training refreshers:** Has the Nominated Officer undertaken training on a periodic basis to refresh their understanding of and how to meet their AML/CTF obligations, with adequate records maintained (for example, materials read, events and conferences attended, relevant dates, content covered) | | | | |
| 37. **Staff training provision:** Has training been provided to all relevant staff, with adequate records maintained (including the date, attendance (with signatures), and content covered) | | | | |
| 38. **Staff training refreshers:** Is training provided on a periodic basis to refresh the knowledge of all relevant staff, with adequate records maintained (including the date, attendance (with signatures), and content covered) | | | | |
| **SYSTEMS AND REPORTING LINES** | | | | |
| 39. **Money Laundering Reporting Officer (NOMINATED OFFICER):** Has a Nominated Officer been formally appointed with their responsibilities formally outlined? (Note: sole practitioners will be regarded as the Nominated Officer) | | | | |
| 40. **Suspicious Activity Reporting (SAR)**: Is there a formal process in place for internal and external SARs, including the reporting template to use, training on how to identify and report suspicious activity, and appropriate record keeping | | | | |
| 41. **Reporting to the National Crime Agency (NCA):** Have SARs been reported to the NCA for all suspicions and knowledge of ML/TF? If any internal SARs were deemed not suspicious, and not disclosed to the NCA, have appropriate records been kept documenting your reasons for not disclosing | | | | |

| | | | | |
|---|---|---|---|---|
| 42. **Record keeping:** Is there an adequate record keeping system and process in place for all relevant information to be maintained for at least 5 years | | | | |
| 43. **Senior Manager(s)**: Is a Senior Manager / Director informed of all instances when a PEP is engaged as a client and are they asked to comment upon the onboarding of such a client | | | | |
| 44. **External SAR**: Is a Senior Manager(s) / Director asked to comment in writing on every occasion that a SAR is made to the NCA | | | | |
| 45. **Any other issues**: Do any other issues or activities relevant to your practice and not referred to in the Risk Assessment pose a risk of ML/TF | | | | |
| Name of Company: | | | | |
| Name of Nominated Officer or authorised person (please state role) undertaking the Risk Assessment: | | | | |
| Date Risk Assessment was undertaken: | | | | |
| *Signature of Nominated Officer or person undertaking the Risk Assessment and Date: | | | | |

**On signing this risk assessment, the Nominated Officer or authorised person acknowledges that HMRC, as designated AML/CTF supervisor, may examine this document. The Nominated Officer or authorised person also undertakes responsibility to ensure that all risk controls outlined are to be implemented and monitored on an ongoing basis.**

# 2. ‘SELLER’ CUSTOMER DUE DILIGENCE & RISK ANALYSIS FORM

# ‘SELLER’ CUSTOMER DUE DILIGENCE & AML RISK ANALYSIS

**Explanatory Note**

This form will be completed by the estate agent once instructions have been received to market a property i.e. at the time of establishing a business relationship and prior to the Estate Agent undertaking any transactions on behalf of the client.

The form consists of 5 sections that will be completed where relevant as part of the CDD process:

1) Property & Instruction Details
2) Natural Person
3) Legal Person (Company) or Legal Arrangement (Trust, Charity, NPO)
4) Politically Exposed Person
5) Client Risk Analysis & Money Laundering Rating

Section 1 will be completed with the details of the property being sold and details of the person or organisation instructing the agent. Section 2 or 3 will record whether the client actually selling the property is a person, company or trust.

In Section 3 if the Beneficial Owner is identified as another ‘Legal Person’ i.e. company then that will be recorded but the “ultimate” Beneficial Owner will be identified and recorded.

In Section 4 which relates to a PEP the ‘client’ can be either be a Natural Person as per Section 2 or the Beneficial Owner as recorded in Section 3.

| SECTION 1 – PROPERTY & INSTRUCTION DETAILS | |
|---|---|
| Address of property being sold | |
| Title holder as per Land Registry | |
| Agreed Sale Price | |
| Is client a Natural Person, Legal Person (Company) or Legal Arrangement (Trust) | |
| Is the instructing person as per the Estate Agent referral the seller | |
| If answer to above is 'NO' state full name of person instructing and relationship to seller | |

| SECTION 2 – NATURAL PERSON | |
|---|---|
| Full name of the client | |
| Date of birth | |
| Home address if different from property being sold | |
| Contact e-mail | |

| **SECTION 3 – LEGAL PERSON (COMPANY)** | |
|---|---|
| Name of the company | |
| If registered in UK company number | |
| If registered overseas country where incorporated | |
| Has the Register of Overseas Entity document been provided | |
| Registered Office address | |
| Full details of company documentation provided e.g. certificate of Incorporation, Memorandum / Articles of Association, List of directors, share register, PSC register | |
| Full Details of the Beneficial owner(s) of the company e.g. name, address, date of birth **(**If BO is another company then details will be recorded but in addition the ultimate owner i.e. person will be identified and recorded) | |
| Full details of the "ultimate" Beneficial Owner of the company (Full name, address, date of birth, occupation etc) | |
| Full details of documentation provided to confirm the identity of the Beneficial Owner(s) e.g. passport number, date of issue, expiry etc | |

| SECTION 3 - LEGAL ARRANGEMENT (TRUST) | |
|---|---|
| Full name of the Legal arrangement | |
| Is the Legal Arrangement a Trust, Charity or Not for Profit Organisation | |
| Where was the Legal Arrangement established | |
| For a Trust state the documents provided to confirm existence of the Trust e.g. Deed of Trust | |
| Has the Trust registration document been provided | |
| Full name of the Beneficial Owner of the Trust i.e. Settlor, Trustees and Beneficiaries | S:<br><br>T:<br><br>B: |
| Details of the documentation provided to confirm the identity of the Beneficial Owner(s) e.g. passport number, date of issue, expiry etc | S:<br><br>T:<br><br>B: |
| If the Legal Arrangement is a Charity or NPO has the person with significant control been identified and please state full name and date of birth | |
| Details of the documentation provided to confirm the identity of the person with significant control e.g. passport number, date of issue, expiry etc | |

| SECTION 4 – POLITICALLY EXPOSED PERSONS | |
|---|---|
| Due to their position or status is the client currently considered a 'PEP' | |
| What is the exact position held by the client that classifies them as a PEP (includes position, jurisdiction, dates held from and to) | |
| Is the client a close family member i.e. husband / wife, parent or child of a person who is considered a 'PEP' | |
| Has EDD been undertaken including the request for additional supporting documentation from the client | |
| Has the MLRO and a Director of the Estate Agent been informed that the client is a 'PEP'. | |

## SECTION 5 - 'SELLER' RISK ANALYSIS & MONEY LAUNDERING RATING

The factors posed below should be considered when assessing the risk of the client and/or the transaction. The notes column is used to summarise assessment of risks involved where the issue is applicable to the client/transaction being considered. Not all questions will be relevant or applicable to all situations. Conversely, the questions outlined are non-exhaustive and there may be other pertinent risk factors which should be taken into account, dependent upon the nature of the client/transaction being considered.

| CLIENT RISK | NOTES |
|---|---|
| **STATUS OF CLIENT**<br>• Has the client been introduced by a 3rd Party? Is R.39 reliance being used?<br>• Is the instruction channelled through a 3rd party? If so, why?<br>• Is the client a Politically Exposed Person?<br>• If client is not a natural person has the ID&V of beneficial owners and directors / controllers been confirmed? | |
| **FACE TO FACE CONTACT**<br>• Has the agent met with the client face to face or is it a non-face to face transaction?<br>• If non-face to face, is there a legitimate reason for this? | |
| **LOCATION OF CLIENT**<br>• Where is the client based? Locally /UK/EU/other international location?<br>• Is the client based in a high-risk jurisdiction or resident in/links to a sanctioned country? | |
| **ID & ADDRESS VERIFICATION**<br>• Has the client provided acceptable standard ID or *acceptable* non-standard ID?<br>• Has Land Registry search confirmed the title holder of the property?<br>• Full details of identification document e.g. Passport number, date of issue, expiry etc. If certified has the status of certifier confirmed?<br>• Has the client provided an address verification?<br>• Details of documentation provided to confirm place of residence of the client (e.g. utility bill, finance agreement, bank statement etc)<br>• If using R.39 reliance (obtaining certified copies of ID & address verification), has the authenticity/professional status of the certifier been confirmed?<br>• Has the client been cooperative in the process or have they delayed providing ID and address verification/ appeared reluctant to do so? | |
| **TRANSACTION TYPE**<br>• Could the type of transaction be at a higher risk of money laundering?<br>• Does the transaction make sense or is it overly complex given the underlying nature of the business being conducted? | |

## MONEY LAUNDERING RISK RATING

This analysis will be undertaken at the beginning of the business relationship and repeated if the estate agent becomes aware of any material changes to the status of the client during the course of the business relationship. This may result in the analysis being reviewed and may require further CDD to be undertaken. Assessment of risk will take both client and transaction risk into consideration and will dictate whether Simplified, Standard or Enhanced Client Due Diligence (CDD) is required.

| INITIAL ASSESSMENT OF RISK (Business relationship): | LOW | MEDIUM | HIGH |
|---|---|---|---|
| | SIMPLIFIED CDD<br>STANDARD CDD | STANDARD CDD<br>ENHANCED CDD | ENHANCED CDD |

Please note below reasons for your assessment:

| SIGNED BY: | DATE: |
|---|---|
| | |

# 3. ‘PURCHASER’ CUSTOMER DUE DILIGENCE & RISK ANALYSIS FORM

# ‘PURCHASER’ CUSTOMER DUE DILIGENCE & AML RISK RATING

**Explanatory Note**

The form consists of 5 sections that will be completed where relevant as part of the CDD process:

1) Property Details
2) Natural Person
3) Legal Person or Legal Arrangement
4) Politically Exposed Person
5) Purchaser Risk Analysis & Money Laundering Risk Rating

Section 1 will be completed with the details of the property being purchased and Section 2 or 3 will detail the name of the entity actually purchasing the property.

Section 4 which relates to a PEP, the ‘purchaser’ can be either the person making the offer in Section 2 or the Beneficial Owner as listed in Section 3.

| SECTION 1 – PROPERTY DETAILS | |
|---|---|
| Address of property being purchased | |
| Agreed purchase price | |
| Is purchaser a Natural Person, Legal Person (Company) or Legal Arrangement (Trust) | |

| SECTION 2 – NATURAL PERSON | |
|---|---|
| Full name of the purchaser(s) | |
| Date of birth | |
| Home address | |
| Contact e-mail | |

| **SECTION 3 – LEGAL PERSON (COMPANY)** | |
|---|---|
| Name of the company | |
| If registered in UK company number | |
| If registered overseas country where incorporated | |
| Has the Register of Overseas Entity document been provided | |
| Registered Office address | |
| Full details of company documentation provided e.g. Certificate of Incorporation, Memorandum / Articles of Association, List of directors, Share register | |
| Full Details of the Beneficial owner(s) of the company e.g. name, address, date of birth<br>**(**If BO is another company then details must be recorded but ultimate Beneficial Owner i.e. person must be identified and recorded) | |
| Details of the documentation provided to confirm the identity of the "ultimate" Beneficial Owner(s) e.g. passport number, date of issue, expiry etc | |

| SECTION 3 - LEGAL ARRANGEMENT (TRUST) | |
|---|---|
| Full name of the Legal arrangement | |
| Is the Legal Arrangement a Trust, Charity or Not for Profit Organisation | |
| Where was the Legal Arrangement established | |
| For a Trust state the documents provided to confirm existence of the Trust e.g. Deed of Trust | |
| Have the Trust provided a copy of their registration | |
| Full name of the Beneficial Owner of the Trust i.e. Settlor, Trustees and Beneficiaries | S:<br><br>T:<br><br>B: |
| Details of the documentation provided to confirm the identity of the Beneficial Owner(s) e.g. passport number, date of issue, expiry etc | S:<br><br>T:<br><br>B: |
| If the Legal Arrangement is a Charity or NPO has the person with significant control been identified and please state full name, date of birth etc | |
| Details of the documentation provided to confirm the identity of the person with significant control e.g. passport number, date of issue, expiry etc | |

| SECTION 4 – POLITICALLY EXPOSED PERSONS | |
|---|---|
| Due to their position or status is the purchaser currently considered a 'PEP' | |
| What is the exact position held by the purchaser that classifies them as a PEP (includes position, jurisdiction, dates held from and to) | |
| Is the purchaser a close family member i.e. husband / wife, parent or child of a person who is considered a 'PEP' | |
| Has EDD been undertaken including the request for additional supporting documentation from the purchaser | |
| Has the MLRO and a Director of the Estate Agent been informed that the purchaser is a 'PEP'. | |

## SECTION 5 - 'PURCHASER' RISK ANALYSIS & MONEY LAUNDERING RISK RATING

The factors posed below will be considered when assessing the risk of the Purchaser and/or the transaction. Please use the notes column to summarise assessment of risks involved where the issue is applicable to the Purchaser/transaction being considered. Not all questions will be relevant or applicable to all situations. Conversely, the questions outlined are non-exhaustive and there may be other pertinent risk factors which should be taken into account, dependent upon the nature of the Purchaser/transaction being considered.

| PURCHASER RISK | NOTES |
|---|---|
| **STATUS OF PURCHASER**<br>• Has the Purchaser been introduced by a 3rd Party? Is R.39 reliance being used?<br>• Is the Purchaser a Politically Exposed Person?<br>• If the Purchaser is not a natural person but rather a legal entity, has the ID & V of beneficial owners and directors / controllers been confirmed? | |
| **FACE TO FACE CONTACT**<br>• Has the agent met the Purchaser concerned face to face?<br>• If non-face to face, is there a legitimate reason for this? | |
| **LOCATION OF PURCHASER**<br>• Where is the Purchaser based? UK/EU/other international location?<br>• Is the Purchaser based in a high-risk jurisdiction or resident in/links to a sanctioned country? | |
| **ID & ADDRESS VERIFICATION**<br>• Has the purchaser provided acceptable standard ID or *acceptable* non-standard ID?<br>• Full details of identification document e.g. Passport number, date of issue, expiry etc. If certified has the status of certifier confirmed?<br>• Details of documentation provided to confirm place of residence of the purchaser<br>• If using R.39 reliance (obtaining certified copies of ID & address verification), has the authenticity/professional status of the certifier been confirmed?<br>• Has the purchaser been cooperative in the process or have they delayed providing ID and address verification/ appeared reluctant to do so? | |
| **TRANSACTION TYPE**<br>• Could the type of transaction be at a higher risk of money laundering?<br>• Does the transaction make sense or is it overly complex given the underlying nature of the business being conducted? | |

| | |
|---|---|
| **SOURCE OF FUNDS**<br>• How does the purchaser intend to pay for the purchase of the property?<br>• Is the source of funds clear and identifiable?<br>• Details of documentary evidence provided to confirm the source of funds e.g. mortgage letter, bank statement<br>• Are funds from a recognised financial/credit institution or personal funds?<br>• Is any funding coming from overseas and if so where, who, connection?<br>• If third party involved what are the details of the third party and the connections between them and the purchaser<br>• Details of documentary evidence provided in relation to the third party<br>• Does the value of the property purchase fit the profile of the purchaser e.g. occupation, source of wealth etc | |

## MONEY LAUNDERING RISK RATING

This analysis will be undertaken at the beginning of the business relationship i.e. when an offer to purchase has been accepted by the seller. If the estate agent becomes aware of any material changes to the status of the purchaser during the course of the business relationship, then the analysis will be reviewed and may require further CDD to be undertaken. Assessment of risk should take both purchaser and transaction risk into consideration and will dictate whether Simplified, Standard or Enhanced Purchaser Due Diligence (CDD) is required.

| | | | |
|---|---|---|---|
| INITIAL ASSESSMENT OF RISK<br>(Business relationship): | LOW<br><br>SIMPLIFIED CDD<br>STANDARD CDD | MEDIUM<br><br>STANDARD CDD<br>ENHANCED CDD | HIGH<br><br>ENHANCED CDD |
| Please note below reasons for your assessment: | | | |
| SIGNED BY: | DATE: | | |

# 4. SOURCE OF FUNDS STATEMENT

## SOURCE OF FUNDS STATEMENT

As part of the Customer Due Diligence process in line with the 2017 Money Laundering Regulations estate agents are required to ascertain the source of funding for any property purchased. Therefore, as standard procedure we request all purchasers complete the questions below in order for us to comply with our legal obligation when it comes to anti-money laundering. The information relates to the proof of funds (evidence that you have the required funds) and source of funds (where and how you have acquired such funds). If we cannot obtain satisfactory information relating to proof and source of funding we will not be in a position to complete our Customer Due Diligence procedure and therefore the purchase of the property concerned might be at risk.

| | |
|---|---|
| **PROPERTY TO BE PURCHASED** | |
| **PURCHASE PRICE** | |
| **SOURCE OF FUNDS**<br><br>(Please give as much detail as possible. If for example you have acquired funds from a particular source (e.g. sale of house, drawdown from an investment, sale of an asset/shares, bonus from work, dividend payment and will also include details of any gifted payments from for example family members) | |
| **DOCUMENTATION TO SUPPORT SOURCE OF FUNDS**<br><br>(Please indicate the documentation that corroborates with the information given as the source of funds statement e.g. bank statements, mortgage offer letter. This documentation will need to be provided to the sales agent and a copy will be retained on your file in line with the ML Regulations). | |
| **FULL NAME** | |
| **SIGNATURE** | |

# 5. AML POLICY LETTER FOR CLIENT & PURCHASER

## Anti-Money Laundering Policy

This company is required to comply fully with the Money Laundering Regulations 2017 ("Regulations") and as such we are required by law to get satisfactory evidence of the identity of our clients and/or any third parties involved in your matter. This information must be provided at the outset which means for vendors at the time the instructions are received to market and sell your property and for purchasers at the time that your offered to buy is accepted by the seller. If this information is not provided as agreed, your transaction may be delayed, or we may have to withdraw our services from the sale of the property.

For an individual person, we require to see two current forms of identification, one of which will include photographic evidence such as a current passport or photographic driving licence and the second form will include a document that provides a satisfactory proof of address such as a bank statement or utility bill which is no more than 3 months old. The estate agent involved in your transaction can discuss this issue with you in further detail if you do not have a current passport or photographic driving licence and we have to accept alternative forms of ID.

The requirements for corporate entities such as companies or partnerships are more complex and you will be required to provide documentation e.g. certificate of incorporation, articles of association etc that confirm whom the beneficial owner is of the company or the person(s) with significant control over it. The beneficial owner of a company whether through direct or indirect ownership or control, including through bearer share holdings is someone who has more than 25% of the shares or voting rights in the company or any person who exercises control over the management of the company. In the case of Trusts this might include full details of the Settlor and or the Beneficiaries.

Original documentation will be the required for verification purposes wherever possible but if copies are provided, they must be independently verified by a professional person such as a solicitor and accountant and the photocopy marked up accordingly. In all cases and in line with the 'Regulations', the company will retain copies of your ID in either paper or electronic form up to a period of 5 years after the date we have ceased the business relationship. In addition, we also reserve the right to use the services of third parties including on-line credit check companies to carry out identity verification of any client.

The company may from time-to-time request further documentation beyond what was originally requested should we deem it appropriate in order to meet our obligations as regards to the "Regulations".

For previous clients, it is important that the company conducts a check to confirm that there has been no change in your circumstances such as a change of address or name or, in the case of a corporate entity there is a change of identity, structure or beneficial ownership. However, it is requested that the client notify the company should there such a change and provide us with the relevant identification or evidence.

In addition to verification of the client the company will have to verify the source of any funds that are being used for the property purchase. Funds received on your behalf from a third party require the same levels of identification and verification checks as the customer themselves. For example, if you are paying for the property by way of a mortgage you might be required to provide written confirmation. If it is a "cash" purchase proof of funds in the form of a bank statement might be requested.

In addition to verification of the source of funds there are occasions when the company must be satisfied as to the source of wealth of any client instructing us, and we may need to ask you for an explanation of that source.

This company has a professional and legal duty to keep your affairs confidential. However, it is important to note that should the company have any evidence or form a suspicion that a client is in any way concerned with money laundering or terrorist financing we are under a legal obligation as set out in the Proceeds of Crime Act 2002 to make a formal report to the National Crime Agency (NCA) who are responsible for collating all reports of potential money laundering. The company is explicitly prohibited from notifying you of the fact that any such report has been made and because of such a report the company might have to suspend work on your matter for a period, and/or even terminate the relationship. If this is the case, then we cannot legally notify you of this fact or the outcome of such a report.

# 6. CDD RELIANCE ON A THIRD PARTY

## "RELIANCE" IN ACCORDANCE WITH REGULATION 39 OF THE MONEY LAUNDERING, TERRORIST FINANCING AND TRANSFER OF FUNDS (INFORMATION ON THE PAYER) REGULATIONS 2017

In accordance with Regulation 39 a regulated company subject to the Money Laundering Regulations 2017 ["Regulations"] may place reliance on the Customer Due Diligence undertaken by a "relevant person" as defined by Regulation 8 of the "Regulations".[16]

The conditions that need to be met in order to comply with Regulation 39 are as follows:

i. There has to be an agreement in place between both parties that the "requestor" can place reliance upon the CDD undertaken by a third party and therefore the third party must consent to the reliance.
ii. The documentation and information obtained for CDD purposes must be provided to the "requestor"
iii. ID & V records and any other relevant information relating to the identity of the customer, customer's beneficial owner, or any person acting on behalf of the customer must be supplied to the "requestor" immediately upon request
iv. The documents must be retained by the third party in line with Regulation 40 of the ML Regulations i.e. retained for 5 years etc
v. The "requestor" remains liable for any failure to apply appropriate measures

## WRITTEN AGREEMENT FOR RELIANCE ON CDD

This is a written agreement confirming the reliance placed upon CDD undertaken by a "relevant person" by another company in the regulated sector that is subject to the "Regulations". This written arrangement confirms that all conditions as set out above relating to Regulation 39 of the "Regulations" will be met in full by all parties to this agreement and that CDD has been conducted in accordance with Regulation 28 of the "Regulations".

Name of organisation providing the CDD:

Address:

Name of organisation placing reliance upon the CDD:

Address:

[16] http://www.legislation.gov.uk/uksi/2017/692/pdfs/uksi_20170692_en.pdf

**INDIVIDUAL PERSON**

Full name:

Date of birth:

Home address:

**LEGAL PERSON (COMPANY)**

Name:

Company number or other registration number:

Address of registered office, and if different, its principal place of business:

Full Name of Beneficial Owner: Date of Birth:

Address:

Full Name of Beneficial Owner: Date of Birth:

Address:

Full Name of Beneficial Owner: Date of Birth:

Address:

**LEGAL ARRANGEMENT I.E. TRUST, CHARITY OR NPO**

Full name of Organisation:

Jurisdiction where established:

Name of person exercising control over the organisation;

Position held:

**THIRD PARTY ACTING ON BEHALF OF THE CLIENT**

Full name:

Date of birth:

Home Address:

Relationship to the client:

---

All parties accept that all documentation and information to support the undertaking of CDD in line with the "Regulations" should be forwarded to the "Requestor" as soon as practicable and copies of the Identification and verification documents that have been independently verified should be provided immediately upon request.

Signed on behalf of the organisation providing the CDD:

Name:

Position held:

---

Signed on behalf of the organisation placing reliance upon the CDD:

Name:

Position held:

---

# 7. PEP QUESTIONNAIRE

## "POLITICALLY EXPOSED PERSON" QUESTIONNAIRE

In accordance with Regulation 35 of the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 this company is required to check if a client, or anyone connected with a client, might be a "Politically Exposed Person" (known as a "PEP"). If a client is a PEP the company might have to undertake additional anti-money laundering procedures. Please answer the questions below, and if necessary add any explanation at the end.

| Have you been entrusted with a prominent public function as listed below | Yes | No |
|---|---|---|

Answer "YES" if now or in the recent past (certainly in the last 12 months) you have held any roles, in any country:

- Member of parliament
- Member of the governing body of a political party
- Appeal court judge
- Member of the court of auditors or the board of a central bank
- Diplomat or high-ranking officer in the armed forces
- Member of the administrative, management or supervisory body of a State-owned enterprise
- Senior officer or director of an international organisation
- Head of state, head of government, minister or deputy or assistant minister

| Does a member of your family hold such a function as listed above? | Yes | No |
|---|---|---|

☐ Your spouse or civil partner

☐ Your parents, or the parents of your spouse or civil partner

☐ Your children

| Does a close associate of yours hold such a function as listed above? | Yes | No |
|---|---|---|

Answer "YES" if any of the following hold any of the roles listed above:

☐ Someone with whom you have a close business relationship

☐ Someone with whom you have joint beneficial ownership of a legal entity or a legal arrangement (e.g. a company or a trust)

☐ Someone for whose benefit a legal entity or a legal arrangement has been set up in respect of which you have sole ownership

If you have answered "YES" to any question, please provide further details here:

Signed:..... Name:.....Date:.....

# 8. IDENTIFICATION & VERIFICATION DOCUMENT CHECKLIST

## Individual – Non-UK Resident/ UK Resident

'CDD' is required for each person involved in the purchase or sale of a property:

The following documentation is required:

| | |
|---|---|
| **Identification – Passport or Photo Driving Licence/Overseas Identification**. This should be a photograph of the official document. The documents must be certified if you have **NOT** met the individual in person. | |
| **Proof of Address –** Utility Bill/Council Tax/Bank Statement. This must be dated within the last 3 months. The document must be certified if you have not seen the original. | |
| **Determine whether this party is a Politically Exposed Person 'PEP' or subject to financial sanctions.** | |
| **For sellers only: Proof of ownership of the property through the land registry title** | |
| **For purchasers only: Source of funds** | |

## Companies

The following documentation is required for your records:

| | |
|---|---|
| **Certificate of Incorporation** | |
| **Memorandum & Articles of Association** | |
| **Copy of current share register** | |
| **Confirmation of registered office and trading address (if different)** | |
| **List of Directors** | |
| **Identity of the ultimate Beneficial owner(s)' or person(s) who appear to be exercising control over the organisation** | |
| **For sellers: Proof of ownership of the property through the land registry title** | |
| **Copy of the Registration of PSC for LLPs** | |
| **Copy of Register of Overseas Entity if company outside of the UK** | |

## Trusts

The following documentation is required for your records:

| | |
|---|---|
| **Deed of Trust** | |
| **Identification, proof of address and Politically Exposed Person ('PEP') form for the Settlor, Trustees & Beneficiaries of the Trust** | |
| **For sellers: Proof of ownership of the property through the land registry title** | |
| **Copy of the Registration of the trust with HMRC** | |

## Enhanced Due Diligence

A referral to the Nominated Officer (MLRO) and Senior Management should be sought prior to commencing a business relationship with a client considered "high risk" such as a PEP and where there is a requirement to undertake Enhanced Due Diligence (EDD). 'EDD' consists of the following:

- ✓ **Considering whether additional identification information needs to be obtained.**
- ✓ **Considering whether additional aspects of the identity need to be verified.**
- ✓ **The taking of reasonable measures to establish Source of Wealth of the customer and any beneficial owner.**
- ✓ **Considering what on-going monitoring should be carried out.**

## Methods used to conduct identification and verification

**Natural Person**

**Identification of the person**

These are some of the methods that can be used:

- Passport bearing a photograph of the individual which is current and valid
- Driving Licence or Provisional Driving Licence bearing a photograph of the individual which is current and valid
- Birth certificate
- Current EEA member state identity card
- Firearms certificate or shotgun licence
- Photographic registration cards for self-employed individuals and partnerships in the construction industry

**Proof of the current place of residence**

- Driving licence – If not being used as proof of identity
- Council tax bill
- Utility bill or statement, or a certificate from a utility's supplier confirming an arrangement to pay services on pre-payment terms
- Bank, building society or credit union statement or passbook containing current address
- A recent original mortgage statement from a recognised lender
- Solicitor's letter confirming recent house purchase or land registry confirmation of address
- Local council or housing association rent card or tenancy agreement
- HMRC self-assessment statement or tax demand
- House or motor insurance certificate
- Statement from a member of the firm or other person in the regulated sector who has known the client for a number of years attesting to their identity - bear in mind you may be unable to contact this person to give an assurance supporting that statement at a later date

It is essential that at least **two** documents from the above list are obtained i.e. one from each. The first document must be from the list to confirm identification of the client and a second document to confirm proof of their current place of residence.

**Legal Persons**

The following are some of the methods that can be used:

- Certificate of Incorporation, Memorandum & Articles of Association which must be either a certified copy or sourced directly from an independent public registry
- Bank statement or utility bill which is not more than 6 months old and is received in the post by the customer
- Latest Annual Return which must be in date and sourced directly from an independent public registry in an equivalent jurisdiction
- Audited financial statements which display the company name, directors and registered address which must be signed by the reporting accountant.
- Prepared accounts by a reporting accountant which display the company name, directors and registered address and which are signed by the reporting accountant
- Conducting and recording an enquiry by a business information service, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted
- Undertaking a company house search, including confirmation that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated
- Use of independent data sources including electronic sources
- Copy of the Registration of a Person with Significant Control (PSC)

**Legal Arrangement**

- Trust Deed (or relevant extracts of the trust deed) and any subsequent deeds of appointment and retirement (or equivalent) and it must be a certified copy
- Bank statement which includes the Trustees mailing address and is no more than 6 months old and is received in the post by the customer
- Use of independent data sources, including electronic sources
- Copy of the Registration of a Trust with HMRC

# 9. INTERNAL SUSPICIOUS ACTIVITY REPORT

## INTERNAL SUSPICIOUS ACTIVITY REPORT

The company will adopt this internal Suspicious Activity Report (which may be updated from time to time by the Nominated Officer).

It is the responsibility of each staff member to have access to the current internal Suspicious Activity Report form. This can be found as a document on the company's computer system. For further information or in the event of any difficulty obtaining / understanding / completing this form you must refer immediately to the Nominated Officer who will take the appropriate action.

A copy of this report should never be placed on the client file as should the client obtain the file and see this document you may be guilty of "tipping off" the client. You must ensure that the documents that should accompany the Suspicious Activity Report are attached to it and submitted to the Nominated Officer. The Nominated Officer will decide which of these it is appropriate to retain, and which should be placed on the transaction file at the conclusion of any NCA investigation.

Keep an accurate record of the date you submitted your Suspicious Activity Report to the Nominated Officer.

The Nominated Officer will notify all staff immediately of:

i) The client's details where there is any intended / anticipated Suspicious Activity Report

ii) The date any Suspicious Activity Report is filed with the NCA

iii) The date of any response (if any) by the NCA as to actual or deemed "appropriate consent" (allowing this company to continue acting for the client)

iv) Any lack of "appropriate consent" from the NCA and how this company (and you) should respond accordingly

v) The date you may continue to act on the file

THE SUSPICIOUS ACTIVITY REPORT FORM SHOULD BE RETAINED WITH THE:

- CDD Form for New Clients
- Risk Analysis Form
- Copies of relevant correspondence

## SUSPICIOUS ACTIVITY REPORT

(Use separate continuation sheets if required)

| | |
|---|---|
| Report submitted by: | |
| Date & Time received by the NOMINATED OFFICER: | |
| Does the report need to be fast tracked: If 'Yes', please specify why: (including all relevant dates presently anticipated e.g. exchange of contracts, completion, Court or other Tribunal hearings, mediation, movement or transfer of funds etc) | |
| Suspect's Full Name: | |
| Title - Mr, Mrs, Ms, Miss, Dr etc | |
| Date of Birth: | |
| Address (home): | |
| Telephone Numbers:<br><br>Home-<br>Work-<br>Mobile- | |
| Employer if known: (Full Details) | |
| Type of Employment: | |

| | |
|---|---|
| Work Address: | |
| Bank Account details<br><br>Branch:<br>Sort Code:<br>Account No.: | |
| Associated persons / entities with the Suspect: (Full Details) | |
| Full Details of the Connection/Association: | |

| | |
|---|---|
| **If suspect a Company** | |
| Full Company Name: | |
| Registered No.: | |
| Country Registered: | |
| Registered Office: | |
| Type of Business: | |

| **Suspicion** | |
|---|---|
| Reasons for knowledge / suspicion (full details) | |
| Full details of any concerns regarding monies connected with the client / this matter generally: | |

| | |
|---|---|
| Name of Person Reporting (Block Capitals): | |
| Signed: | |
| Date: | |
| Signature of Nominated Officer: (acknowledging receipt) | |
| Date: | |
| Action taken and reason(s) (e.g. referral to the NCA or decision not to file external SAR): | |
| | |
| ADMINISTRATION OF SAR CHECKLIST:<br><br>1. CDD Form for new and existing clients attached<br>2. Risk Analysis Form attached<br>3. Relevant correspondence attached | |

# 10. TRAINING RECORD

## Anti-Money Laundering Training Attendance Form

| **Location of Course:** | | | |
|---|---|---|---|
| Date of Training:<br>**(DD MM YYYY)** | | **Duration:** | |
| **Name of Trainer:** | | **Company:** | |
| **SURNAME** | **FIRST NAME** | **POSITION** | **NOMINATED OFFICER SIGNATURE** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |