

# Anti-Money Laundering Policy & Procedures

<b>Policy Owner:</b>	Executive Director of Finance
<b>Policy Lead:</b>	Risk & Assurance Manager
<b>Approved by:</b>	Audit Committee
<b>Approved date:</b>	February 2024
<b>Next review date:</b>	February 2027

## Contents

	Page
Purpose and scope of this policy	2
Policy	
• Policy	2
• Training	3
• Monitoring	4
Definitions	5
Equality, Diversity, and Inclusion	5
Data protection	5
Related legislation and regulations	5
Related policies and procedures	5
Customer engagement	5
Document revision history	6
Appendix A – policy statement	7
Appendix B – Anti-Money Laundering Procedures	8

## Purpose and scope of the policy

This policy enables us to meet the legal requirements in relation to preventing and detecting money laundering, ensuring our response is proportionate to the risk of money laundering and terrorist financing. The policy aims to make you aware of your responsibilities and the consequences of non-compliance with this policy.

This policy applies to all our employees. There is a focus on employees in the Development and New Business department where the highest risk has been identified due to the high value transactions being processed.

The estate agency activities undertaken within Development and New Business are subject to anti-money laundering supervision by HMRC. The policy sets out what must be done to enable us to comply with our legal obligations.

Within this policy the term employees refers to all colleagues, senior management, board members, temporary and contract staff.

## 1. Policy

- 1.1 Anti-money laundering legislation places responsibility upon us to combat money laundering and covers a wide range of financial transactions. It applies to all employees involved with monetary transactions.
- 1.2 There are three main offences which relate to money laundering:
  - Concealing: This includes concealing, disguising, converting, transferring or removing criminal property.
  - Arrangement: This means becoming concerned in an arrangement which you know, or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
  - Acquisition, Use or Possession: This means acquiring, using or possessing criminal property.
- 1.3 Any employee could commit an illegal offence under the money laundering provisions if they suspect money laundering and either become involved with it in some way and/or do nothing about it. Under the legislation it is a criminal offence to:
  - assist a money launderer.
  - ‘tip off’ a person suspected to be involved in money laundering that they are suspected or that they are the subject of police investigations.
  - fail to report a suspicion of money laundering and acquire, use, or possess criminal property.
  - deliberately interfere with police, or other law enforcement investigation into money laundering.

1.4 To meet the anti-money laundering requirements, we will:

- Complete a risk assessment to identify and assess where the business is vulnerable to money laundering and terrorist financing.
- Ensure policies, controls and procedures help reduce the risk that criminals may exploit the business for financial crime.
- Establish documented policy statement, controls, and procedures to demonstrate our management of the risks of money laundering and terrorist financing (Policy Statement - Appendix A)
- Carry out a regular (at least annually or upon material business activity changes) review of our activities and re-assess money laundering risks, updating policies and procedures as required.
- Communicate requirements and provide training to relevant employees (and/or contractor's employees) on the requirements of the legislation. Including the identification of suspicious transactions, identity verification and reporting procedures.
- Designate an officer as the Money Laundering Reporting Officer (MLRO), who will receive any report, keep records and if considered appropriate, make reports to the National Crime Agency (NCA). The MLRO is the Executive Director of Finance, and the Risk and Assurance Manager will act as deputy MLRO in their absence.
- Appoint a board member (the Executive Director of Finance) with responsibility for compliance with the regulations.
- Establish procedures for employees to report any suspicions to the Money Laundering Reporting Officer.
- Ensure employees dealing with money transactions comply with our procedures.
- Ensure sufficient resources are available to implement and monitor money laundering and terrorist financing requirements.

1.5 Appendix B sets out our detailed procedures.

## **2. Training**

2.1 The MLRO and deputy MLRO will ensure all employees are trained in and aware of anti-money laundering procedures, risks, the law, and their responsibilities relating to money laundering. This will include:

- Identity and source of funds checks
- How to recognise suspicious activity
- Internal reporting procedures

2.2 As a minimum the MLRO and deputy MLRO will ensure there is:

- Mandatory training for new employees.
- Annual mandatory refresher training for established employees.
- Targeted training for managers and employees in high-risk business areas / activities.
- Periodic publication of requirements to employees.

### **3. Monitoring**

- 3.1 We will routinely inform Audit and Risk Committee of all money laundering allegations and investigations (but not necessarily confidential details of any investigation).
- 3.2 The MLRO will ensure a register of all money laundering allegations and investigations is maintained.

## Definitions

- MLRO – Money Laundering Reporting Officer
- **Money laundering** is “a process that makes money with an illegal origin appear legal so that it may be used”.

## Equality, Diversity, and Inclusion

This policy will be delivered in accordance with our Equality, Diversity and Inclusion Policy. An Equality Impact Assessment was completed for this policy and considered as part of the approval process.

## Data protection

This policy will be delivered in accordance with our Data Protection Policy. A Data Impact Assessment was completed for this policy and considered as part of the approval process.

## Related legislation and regulations

- The Proceeds of Crime Act 2002
- Terrorism Act 2000
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations)
- Criminal Finances Act 2017
- The Fraud Act 2006
- The Bribery Act 2010
- Economic Crime Act 2022
- Policing and Crime Act 2017
- Sanctions and Anti-Money Laundering Act 2018

## Related policies and procedures

- Anti-Fraud, Tax Evasion & Bribery Policy and Fraud response plan
- Whistleblowing Policy
- Moat Policy on Payments and Benefits to Board Members and Staff
- Code of Conduct Policy
- Standing Orders and Terms of Reference
- Risk Management Policy & Framework
- Data Protection Policy & Data Security Breach Management Plan
- Acceptable Use Policy
- Disciplinary Policy

## Customer engagement

With the agreement of the Executive Team, we have not engaged with customers to develop this policy. Following approval of the policy customers will be provided with

information on the checks that we're required to undertake in relation to anti-money laundering.

**Document Revision History (Record of any changes made to the policy)**

<b>Date</b>	<b>Changes approved by</b>	<b>Details of changes made</b>

## **ANTI-MONEY LAUNDERING POLICY STATEMENT**

We are committed to ensuring our employees, senior management and board members comply with all legislation and appropriate guidelines designed to combat money laundering activity and the funding of terrorist or criminal activity in the areas in which we operate.

We will:

Carry out an annual risk assessment to identify and assess the risk of money laundering associated with our activities.

Appoint a designated Money Laundering Reporting Officer (MLRO) - this is the Executive Director of Finance.

Take reasonable steps to establish the identity of any person for whom it is proposed to provide any services.

Retain identification and transactional documentation as defined in the legislation.

Provide training to ensure all relevant employees are aware of their personal responsibilities, including the anti-money laundering procedures in respect of identifying clients, monitoring, record-keeping, remaining vigilant and reporting any suspicious transactions.

Ensure that policies, controls, and procedures are established to effectively manage and mitigate money laundering risks in our activities.

Ensure our policy is developed and maintained in line with evolving statutory and regulatory obligations, and advice from enforcement agencies.

Report to the relevant authority where there are reasonable grounds to suspect that a money laundering offence has been or is being committed.

Always ensure the protection of our employees and safeguard our organisation and reputation against the threat of money laundering and the funding of terrorist and criminal activities.

## **Appendix B - ANTI-MONEY LAUNDERING PROCEDURES**

### **1. Individual client identification procedures (customer due diligence)**

- 1.1 Client identification procedures apply when we carry out a “relevant” activity and before forming a business relationship or considering undertaking a one-off transaction.
- 1.2 Any employee involved in a relevant activity should ensure the customer(s) (sellers, buyers, individuals and/or companies) provide satisfactory evidence of their personal identity. This is customer due diligence, often referred to as ‘know your customer’ and must be carried out on all customers.
- 1.3 All new customers must be identified and responsibility for this rests with the individual processing the case. We must not proceed with a new applicant’s transaction unless this identification has been carried out.
- 1.4 For new customers two forms of identification must be obtained to confirm the person’s identity and address. Our preference is to obtain photographic ID.
- 1.5 We will accept proof of name and address for individuals in accordance with government approved identity lists (Appendix 1). Any refusal or reluctance to provide proof of identity must be reported to the MLRO.
- 1.6 Electronic identification will be verified through an electronic CDD verification product approved by the MLRO. Any ‘fail’ results returned for electronic verification checks must be investigated by the processing officer and satisfactorily evidenced by further manual verification before the transaction can proceed.
- 1.7 In the event of electronic verification being unavailable / inaccessible by customers staff should ask the customer to provide certified documents. Acceptable certified documents are listed in Appendix 2.
- 1.8 In exceptional circumstances, where a customer is not able to provide photographic proof of ID, the customer must provide a proof of name, two forms of proof of address from the approved lists (Appendix 1) and a photograph that has been certified by a solicitor in accordance with the guidance for certified documents in Appendix 2.
- 1.9 Staff must confirm the details collected using the standard customer identification form ‘Moat customer identification form.doc’ (Appendix 4) or in the customer file on CRM. The form must be scanned onto the client’s files alongside copies of the documents confirming identity and address.
- 1.10 If a customer cannot provide proof of identity, you must speak to the MLRO or deputy MLRO for guidance. Where we are unable to comply with customer due diligence requirements, we will terminate the transaction with the customer. Examples of issues with customer identification is provided in Appendix 6.

## **2. Reliance on third-party due diligence**

2.1 We will only place reliance on client identification (customer due diligence) performed by a third-party in the case of open market sales or land disposals.

2.2 Staff processing the transaction must request authority from the MLRO / deputy MLRO who will risk assess the third-party for suitability of reliance. This assessment will include:

- Confirmation that the third party is registered for Estate Agency Business Anti-Money Laundering Supervision with a regulatory body.
- Any available public disciplinary record regarding the standing of the firm.
- Any adverse experiences with the proposed third-party efficiencies in business dealing

2.3 If approved, third parties must agree to the reliance and complete the Reliance Agreement. (Appendix 7)

## **3. Sources of Funds**

3.1 Customers must be asked to provide evidence as to the source of their funds and copies of this evidence must be kept. This means understanding how that money has come into the customer's possession e.g. inheritance, gift, savings.

3.2 Supporting documentary evidence is required to demonstrate the source of funds. This may include payslips, evidence of the inheritance or gift. The evidence should also be checked against what you know about the customer for example, the customer claims the money comes from employment earnings but has claimed housing benefit for a substantial period.

3.3 We will only place reliance on sources of funds validation performed by a third-party where that third-party is an independent financial advisor registered with the Financial Conduct Authority.

3.4 Staff processing the transaction must request authority from the MLRO / deputy MLRO who will risk assess the third-party for suitability of reliance.

#### **4. Company identification procedures**

- 4.1 If purchasers are introduced by other companies or a company is purchasing homes from us e.g. outright sale, then staff must be satisfied that the company's identity is genuine. We will accept proof of identity for companies / legal structures in accordance with government approved identity lists (Appendix 3). Any refusal or reluctance to provide identity for a company must be reported to the MLRO.
- 4.2 If staff are being instructed by the officer of a company, the officer's identification will need to be confirmed in the same way as an individual client in addition to confirming the identity of the company.
- 4.3 This will also apply to any land disposals to other companies / charity organisations.
- 4.4 Transactions relating to land disposal will be subject to further risk assessment by the MLRO which will include:
  - Geographical location of site
  - Type of organisation
  - Available public company / charity information
  - Any available public disciplinary record regarding the standing of the firm
  - Any adverse experiences with the proposed third-party efficiencies in business dealings
  - Any further checks completed at the discretion of the MLRO

#### **5. Record Keeping Procedures**

- 5.1 We will comply with record keeping obligations to retain:
  - Copies of the customer contract and sale
  - Copies of the evidence of identity obtained for five years after the end of the business relationship
  - Details of transactions for five years from the date of the transaction
  - Details of actions taken in respect of internal and external suspicion reports (See Appendix 5)
  - Details of information considered by the MLRO in respect of any internal reports, where a suspicious activity report is not made
  - A written record of the money laundering risk assessment

- 5.2 The MLRO must be informed of the existence and location of such records.
- 5.3 Records must be clear and legible and demonstrate that we have met customer due diligence requirements. Records may be required for internal or external audit inspection, HMRC inspection or court proceedings.
- 5.4 We will ensure that documents are stored securely to protect data subjects from data loss. The retention periods noted above form part of our Data Retention Policy under the GDPR.

## 6. Internal Reporting Procedure

All staff are responsible for reporting **any** suspicion to the MLRO or deputy MLRO as soon as possible - even if the transaction is not completed. The transaction cannot continue until the MLRO approves this

**The customer must not be alerted that a suspicion has been raised. This is 'tipping off' and is a criminal offence**



Internal reports should be communicated to the MLRO via any communication channel, preferably in writing.

Reference to money laundering suspicions must not be reported on the customer file.

The MLRO will review the information available to decide if a Suspicious Activity Report (SAR) report is to be made to the National Crime Agency (NCA)



The SAR report will include details of how they know about or suspect money laundering or terrorist financing activity and as much relevant information about the customer and transaction



If a report is made before a transaction is completed or start of a business relationship, the MLRO will request a defence to a money laundering or terrorist financing offence from the NCA to proceed with the transaction



Where the MLRO decides not to file a report to the NCA, they will document their decision making on the internal reporting form and this will be recorded on the AML Register



The MLRO will inform the notifying officer of the outcome of the suspicion report and next steps to take with the customer

All suspicions will be recorded on Moat's AML Register

## 7. Other Procedures

- 7.1 The Proceeds of Crime Act 2002 covers all the day-to-day activities we carry out. Where a person knows or suspects that the proceeds of crime are being used in a transaction and that person assists, becomes involved or facilitates that transaction, a criminal prosecution against that person may occur. Any suspicious transactions should be reported to the MLRO.
- 7.2 We will establish other procedures of internal control and communication as may be appropriate from time to time for the purpose of preventing the receipt of the proceeds of crime or money laundering.
- 7.3 **Regular receipts** In the normal operation of our non-regulated activities, we accept payments from individuals and organisations e.g. in relation to rent, sundry debtors etc. If an employee has reasonable grounds to suspect that any monies received or payments made are the proceeds of crime or has other suspicions, they should report them to the MLRO.
- 7.4 **Cash receipts** If an amount is offered in cash of £1,000 or more, payment must only be accepted in line with established guidelines in this policy and other relevant departmental procedures.
- 7.5 **Refunds** Care will need to be taken with the procedures for refunds. For instance, a significant overpayment which results in a repayment will need to be properly investigated and authorised before payment.
- 7.6 In the event of any suspicious transactions, the MLRO should be contacted to investigate. The customer must not be informed (i.e. not 'tipped off').