Wheatley Group

Making homes and lives better
wheatley-group.com

Group Anti-Money Laundering and Counter-Terrorism Financing Policy

Approved by Group Audit Committee on 4 August 2021

Contents

1. Introduction

2. Aims

3. Background

4. Money Laundering Reporting Officer (MLRO)

5. Customer Due Diligence Measures

6. Suspicious Activity Reporting

7. Terrorist Financing Offences

8. Training

9. Record Keeping

10. Policy Review

1. Introduction

1.1. Wheatley Housing Group and all its Subsidiaries ('the Group') are committed to ensuring that it has adequate controls to counter money laundering activities and terrorist financing activities.

1.2. The Group is required under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations), as amended by 2019 and 2020 Regulations to put in place appropriate systems and controls to prevent money laundering and terrorist financing. This Policy contains the procedures that we have developed in order to comply with these obligations.

1.3. The Regulations require that an organisation has a Nominated Officer to ensure that there is up-to-date knowledge of issues relating to Anti-Money Laundering and Counter-Terrorist Financing throughout the organisation, implement appropriate policies and procedures and receive reports of suspicious activity. The Nominated Officer (Money Laundering Reporting Officer) for the Group is the Director of Assurance.

1.4. This Policy shall apply across the Group and is intended to ensure a standardised approach.

2. Aims

2.1 The purpose of this Policy is to ensure all staff are aware of the key regulations surrounding the detection and prevention of money laundering activities and terrorist financing activities; and their role as set out within these regulations. The regulatory environment with regards money laundering activities and terrorist financing activities is as follows:

- The Proceeds of Crime Act 2000 ("POCA");
- The Money Laundering Regulations 2017 ("MLR"); and
- The Terrorism Act 2006.

2.2 This Policy aims to:

- ensure staff are aware of what constitutes money laundering activities and terrorist financing activities;
- identify the Group Money Laundering Reporting Officer (MLRO);
- set due diligence measures to aid in the detection of money laundering activities and terrorist financing activities;
- provide staff with the methods for raising reports where they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing; and
- ensure records are complete and retained for the required period of time.

3. Background

3.1 Money laundering is the process by which funds derived from criminal activity are given the appearance of being legitimate by being exchanged for clean money. That means that the proceeds of any acquisitive crime are 'cleaned up' by various means and then fed back into the financial system after a transaction or transactions designed to disguise the original source of the funds.

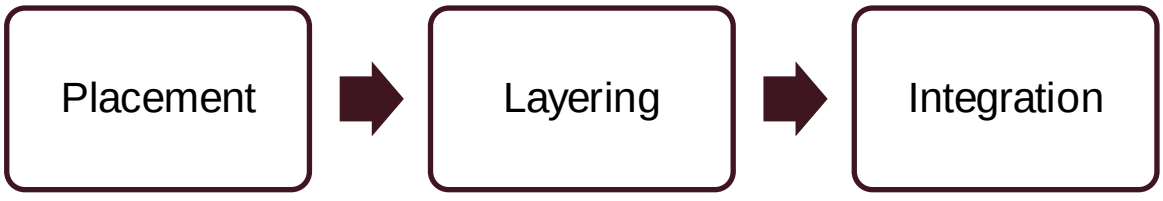
3.2 Terrorist financing is providing or collecting funds, from legitimate or illegitimate sources, to be used to carry out an act of terrorism. Money laundering activity includes:

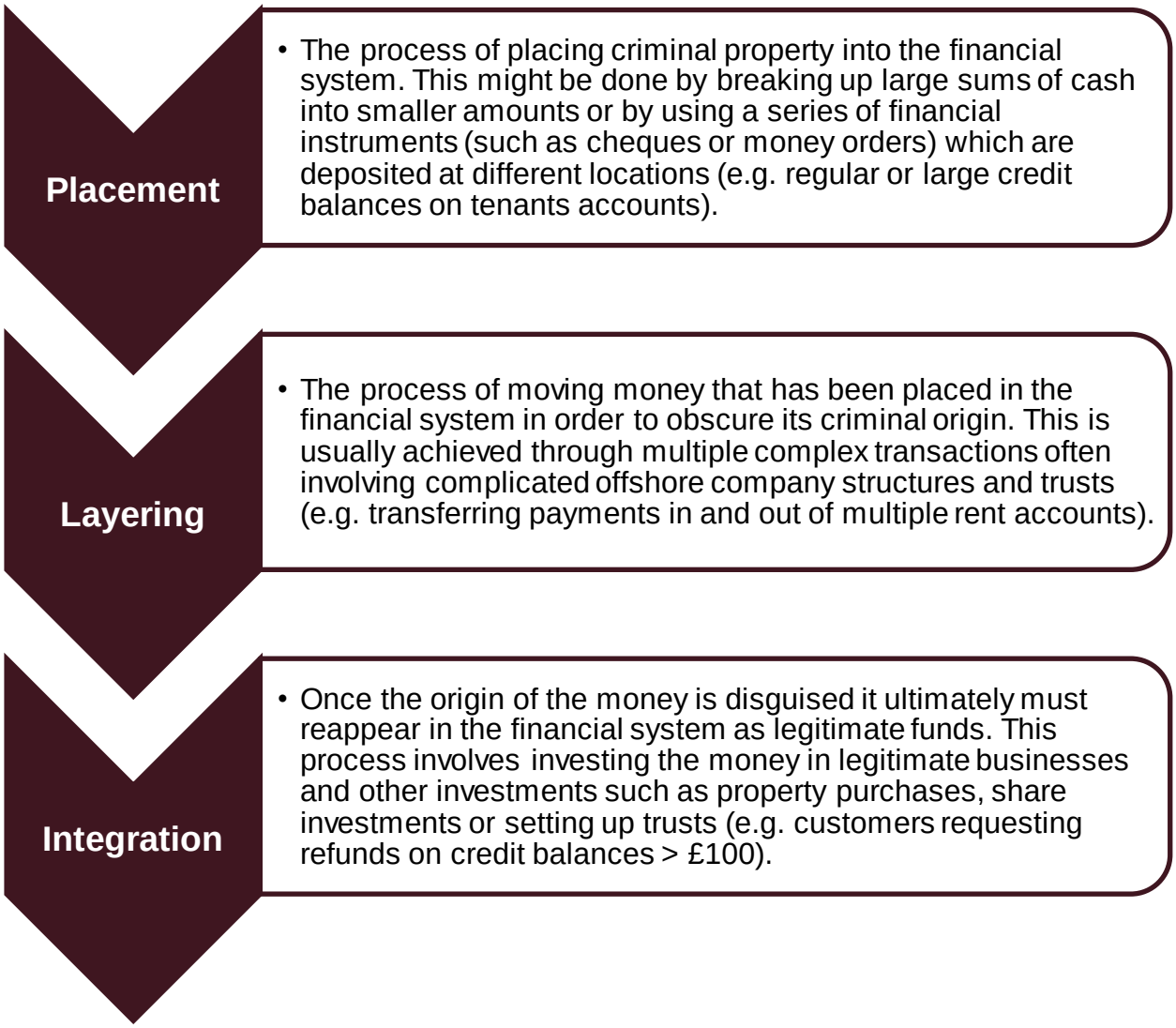
- acquiring, using or possessing criminal property;
- handling the proceeds of crimes such as theft, fraud and tax evasion;
- being knowingly involved in any way with criminal or terrorist property;
- entering into arrangements to facilitate laundering criminal or terrorist property;
- investing the proceeds of crimes in other financial products;
- investing the proceeds of crimes through the acquisition of property/assets; and
- transferring criminal property.

3.3 The Group facilitates a large volume of transactions (some of which can be significant e.g. payments to subcontractors, treasury draw downs, large rent payments).

3.4 The anti-money laundering (AML) and counter-terrorist financing (CTF) regime is designed to prevent our services being used by criminals. You have obligations under the AML/CTF regime to spot and report money laundering and terrorist financing. Failure to meet these obligations can lead to criminal penalties, substantial fines and untold damage to your own and the Group's reputation.

3.5 Typically, money laundering involves three stages:





3.6 For us the placement and integration stages are the most likely but the Group could potentially be involved in any stage. The potential for money laundering has been considered and addressed when developing the Group's new delivery mechanisms under the home working operating model.

3.7 Typical signs of money laundering and terrorist financing are:

- Obstructive or secretive customers;
- Customers based a long way from us with no apparent reason for using us;
- Complex or unusually large transactions;
- Money transfers where there is a variation between the account holder and signatory;
- Payments to or from third parties where there is no logical connection to the customer; and
- Overpayment of money due and credit balances returned to customers.

4. Money Laundering Reporting Officer ("MLRO")

4.1 As part of the required anti-money laundering controls, we have in place a Group MLRO. The Group's MLRO is the Director of Assurance.

4.2 If anyone knows or suspects that another person is money laundering or financing terrorism, they must notify the MLRO as soon as is practicable (by completing a Suspicious Activity Report). The MLRO will review the information they have received and decide if it needs to be reported to the National Crime Agency ("NCA"). If the MLRO decides there are reasonable grounds to suspect money laundering the MLRO must inform the NCA at the earliest possible opportunity.

5. Customer Due Diligence Measures

5.1 All staff should adhere to due diligence identification procedures on every occasion. This will mitigate the risks of the business being used to launder money or fund terrorism.

5.2 All customers must be identified fully with two forms of valid identification. This must include photographic evidence of identity and evidence of their residence e.g. a council tax or utility bill dated in the last three months.

5.3 Should a face-to-face meeting not take place, nor electronic ID verification from independent and reliable sources be obtained, then enhanced due diligence procedures will need to be adopted. This includes asking for additional information or evidence to establish the customer's identity, and ensuring that the documents supplied are certified. It would also be prudent to ensure that the first payment is made to/from a bank account in the customer's name. Enhanced due diligence is also required when a client is established in a high-risk third country or a relevant transaction involved a client in a high risk third country.

5.4 If the verification of the customer's identity is via documents this should be based on:

- A Government issued document with the customer's full name and photograph with either the customer's date of birth or residential address such as:
    - Valid passport;
    - Valid photocard driving licence;
    - National identity card
    - Any other photographic ID, such as a bio-metric residence test.
- **OR**, a government issued document (without a photo) which includes the customer's full name and supported by secondary evidence:
    - Old style driving licence;
    - Recent evidence of entitlement to state or local authority-funded benefit such as housing benefit, council tax benefit, pension.

- Supported by secondary evidence such as

    - A utility bill;
    - Bank or building society statement;
    - Most recent mortgage statement from a recognised lender

    (Secondary evidence should ideally be no older than three months prior to the date of the check).

5.5 For customers who are not private individuals, such as corporate customers and private companies, the Group must obtain information that is relevant e.g. company registration number, registered address and evidence that the individual(s) has the authority to act for the company – a search at Companies House will identify the directors and company secretary. If we become aware of any discrepancies between the information held by Companies House and our own records (based on the Companies House definition of a person of significant control), this must be reported to Companies House.

6. Suspicious Activity Reporting

6.1 Any customer activity outside the normal or expected activity should be considered unusual and must be investigated. Understanding our customers is crucial. Unusual activity or transactions outside established norms should be considered as a potential indicator of suspicious activity. Investigations should establish the reasons for the unusual activity or transaction. This may either remove or confirm your suspicion. If it is confirmed, you must report it to the MLRO. Failure to do so is an offence that could result in five years imprisonment.

6.2 Reports must be made by staff to the MLRO as soon as practicable when they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing. This report should be via an internal Suspicious Activity Report ("SAR").

6.3 After due consideration of the SAR, the MLRO may request further information to aid their decision. The MLRO will then make a decision as to whether there are grounds to make a report to the NCA via a SAR.

6.4 All reports of suspicious activity will be treated as confidential and securely stored, regardless of whether they are reported onto the NCA or not. In respect of Internal Reports where it is decided not to report to the NCA, the MLRO will fully document the rationale behind any such decisions and retain those records.

6.5 Staff should guard against alerting a suspected launderer once they have made their report to the MLRO. Where staff are unsure of how or whether to proceed with a transaction, advice should be sought from the MLRO.

7. Terrorist Financing Offences

7.1 Terrorists need funds to plan and carry out attacks. The Terrorism Act 2000 ("TA 2000") criminalises both participation in terrorist activities and terrorist financing. In general terms, terrorist financing is:

- The provision or collection of funds
- From legitimate or illegitimate sources
- With the intention or in the knowledge
- That they should be used in order to carry out any act of terrorism
- Whether or not those funds are in fact used for that purpose

7.2 The TA 2000 establishes a similar pattern of offences to those contained in POCA 2002, i.e Principal terrorism offences of:

- Fundraising
- Use or possession
- Arrangements
- Money laundering
- Failure to disclose offences
- Tipping-off offences

7.3 All offences carry heavy criminal penalties. While the terrorist financing and money laundering regimes are different, they share similar aims and structures and run together in UK legislation. Many of the provisions of POCA 2002 and TA 2000 mirror one another and the definitions are deliberately matched.

7.4 Both POCA 2002 and TA 2000 run parallel to the Regulations.

8. Training

8.1 Employees will be made aware of this Policy and training and support will be provided where applicable.

9. Record Keeping

9.1 The following records are required to be kept for 5 years:

- Copies of, or references to, the evidence obtained of a customer's identity for five years after the end of the customer relationship, or five years from the date when the transaction was completed.
- Supporting records relating to a customer relationship or occasional transaction for five years from the date when the transaction was completed.

9.2 At the end of the five-year period you must delete any personal data in those records unless:

- you are required to retain records containing person data under an enactment or for the purposes of court proceedings or you have reasonable grounds for believing the records need to be retained for legal proceedings, or

- you have the consent of the person whose data it is.

9.3 The purpose for keeping these records is to demonstrate the business's compliance with the regulations and to aid any resulting investigations.

10. Policy Review

10.1 This Policy may only be changed or varied with the specific authority of the Group Board or Group Audit Committee.

10.2 We will review this Policy every 3 years. More regular reviews will be considered where, for example, there is a need to respond to new legislation/Policy guidance. Reviews will consider legislative, performance standard and good practice changes.

10.3 We will publish this Policy on our website. A hard copy is available on request. Customers can also get a copy of the Policy on tape, in Braille, in large print or in translation on request.