Anti - Money Laundering Proceeds of Crime

Policy Statement for Employees Involved in the Handling of All Payments

Created June 2018
Updated January 2020
Supplementary Aide Memoire added November 2020
Accessibility checked September 2021

Policy Index

Procedural Index

Appendix

1. Introduction

This Policy and Procedure Document is designed to help employees become familiar with the legal and regulatory requirements relating to the handling of money which could have come from the proceeds of crime. This Policy addresses the issues of proceeds of crime and money laundering as they affect West Dunbartonshire Council (the Council) and the procedure will assist employees operationally.

The Policy introduces procedures to help to identify and report on instances where money laundering is suspected. It complements the Council's existing Counter Fraud and Corruption Strategy Confidential Reporting Policy and Financial Regulations and contributes to the existing corporate governance framework to assist in ensuring that the Council is managed effectively and fulfils its statutory and regulatory duties.

It is the policy of West Dunbartonshire Council to prevent the Council and its employees from being exposed to money laundering; to identify areas where it may occur; and to comply with all legal and regulatory requirements - especially with regard to the reporting of actual or suspected cases. It is important to emphasise that it is every employee's responsibility to be vigilant of money laundering.

2. Definition of Money Laundering

Money laundering is the process of transforming the profits of crime and corruption into ostensibly 'legitimate' assets.

Money laundering can undermine the integrity and stability of financial markets and institutions. It is a global problem.

Serious and Organised Crime costs the UK at least £24 billion each year and therefore all West Dunbartonshire Council employees must be vigilant to spot signs of money laundering.

Money laundering is a general term for any method of disguising the origin of "dirty" or criminal money, or the process by which criminally obtained money or other assets are exchanged for 'clean' money or other assets with no obvious link to their criminal origins. This money may be the proceeds of any criminal activity including terrorism, drugs trafficking, corruption, tax evasion, and theft.

The purpose of money laundering is to hide the origin of the dirty money so that it appears to have come from a legitimate source. Unfortunately, no organisation is safe from the threat of money laundering particularly where it is receiving funds from sources where the identity of the payer is unknown.

It is therefore possible that criminals wishing to launder the proceeds of crime will target the Council and that this will probably involve the procurement of goods and services or the settlement of debts.

The money may have been stolen by the party conducting the transaction with the Council, or may have been criminally acquired by a third party for the benefit of the customer.

A suspicion that someone is benefiting financially from dishonest activities will result in a requirement for the Council to report to the National Crime Agency (NCA). All

employees dealing with the receipt of funds or having contact with the public must therefore be aware of the Council's money laundering avoidance policy.

The Council will do all it can, wherever possible to:

- Prevent the Council or its employees being exposed to money laundering;
- Comply with all legal and regulatory requirements; and
- Report all actual or suspected cases to the appropriate authorities.

Failure by any employee to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them.

3. Money Laundering Reporting Officer (MLRO)

The Council has nominated the Chief Officer-Resources to be responsible for anti-money laundering measures within the Council (the Money Laundering Responsible Officer, 'MLRO') with the Deputy being the Section Leader Corporate Fraud (DMLRO).

The MLRO is responsible for ensuring compliance with all relevant legislation and is therefore responsible for all proceeds of crime and money laundering measures within the Council. However, all employees have a responsibility to be vigilant in this regard.

The Corporate Fraud Team will act as a point of contact to receive and investigate reports about suspected and known instances of money laundering activity involving the Council's services.

Contact should be made as follows:

- Stephen West. Chief Officer-Resources, stephen.west@west-dunbarton.gov.uk
- Sharon Hughes, Section Leader, Corporate Fraud Team, Sharon.hughes@west-dunbarton.gov.uk

4. Legislation

Proceeds of Crime Act (POCA) 2002

Laws have been passed which place the burden on employees to report any suspicious transaction to their supervisor / manager who will then report to the MLRO. There are three principal offences:

***Concealing** via* **5.4.2 Section 327 of the Act:**
A person commits an offence if he conceals, disguises, converts, or transfers criminal property, or removes criminal property from England and Wales, Scotland or Northern Ireland.

Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights connected with it.

***Arranging** via* **5.4.3 Section 328 of the Act:**
A person commits an offence if he enters into, or becomes concerned in an arrangement which he knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.

Acquisition, use or possession via 5.4.4 Section 329:

A person commits an offence if he acquires, uses or has possession of criminal property.

There are two associated offences which employees need to be careful of:

Failure to disclose In the Regulated Sector (Municipal Bank) via 5.6.2 Section 330 of the Act:

A person commits an offence if:

- he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering, and
- the information on which his suspicion is based comes in the course of business in the regulated sector, and
- he fails to disclose that knowledge or suspicion, or reasonable grounds for suspicion, as soon as practicable to a nominated officer or the NCA.

Failure to disclose by a Nominated Officer in the regulated sector via 5.6.3 Section 331 of the Act:

A nominated officer in the regulated sector commits a separate offence if, as a result of an internal disclosure under s330, he knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering and he fails to disclose as soon as practicable to the NCA.

Failure to disclose In the Non-Regulated Sector (WDC) via 5.6.4 Section 332 - failure to disclose by a Nominated Officer in the non-regulated sector

An organisation which does not carry out relevant activities and so is not in the regulated sector, may decide on a risk-based approach to set up internal disclosure systems and appoint a person as nominated officer to receive internal disclosures.

A nominated officer in the non-regulated sector commits an offence if, as a result of a disclosure, he knows or suspects that another person is engaged in money laundering and fails to make a disclosure as soon as practicable to the NCA.

Tipping off in the Regulated Sector (Municipal Bank)

There are two tipping off offences in S333A of POCA. They apply only to business in the regulated sector.

- ***S333A (1) - disclosing a suspicious activity report (SAR).*** It is an offence to disclose to a third person that a SAR has been made by any person to the police, HM Revenue and Customs, the NCA or a nominated officer, if that disclosure might prejudice any investigation that might be carried out as a result of the SAR. This offence can only be committed:
    - after a disclosure to the NCA or a nominated officer
    - if you know or suspect that by disclosing this information, you are likely to prejudice any investigation related to that SAR
    - the information upon which the disclosure is based came to you in the course of business in the regulated sector.
- ***S333A (3) - disclosing an investigation***. It is an offence to disclose that an investigation into a money laundering offence is being contemplated or carried out if that disclosure is likely to prejudice that investigation. The offence can only be committed if the information on which the disclosure is based came to the person in the course of business in the regulated sector. The key point is that you can commit this offence, even where you are unaware that a SAR was submitted

Tipping off in the Non-Regulated Sector (WDC)

- Section 342(1) contains an offence of prejudicing a confiscation, civil recovery or money laundering investigation, if the person making the disclosure knows or suspects that an investigation is being, or is about to be conducted.
- Section 342(1) contains an offence of prejudicing a confiscation, civil recovery or money laundering investigation, if the person making the disclosure knows or suspects that an investigation is being, or is about to be conducted.

- Section 342(1) was amended by paragraph 8 of the Terrorism Act 2000 (TACT) and POCA Regulations 2007. The offence in s342 (2) (a) only applies to those outside the regulated sector. The offence in s342 (2) (b) applies to everyone.

- You only commit the offence in s342 (2) (a) if you knew or suspected that the disclosure would, or would be likely to prejudice any investigation.

Although the term ‘money laundering’ is generally used when describing the activities of organised crime, to most people who are likely to come across it, it involves a suspicion that someone is benefiting financially from dishonest activities.

Any persons involved in any known or suspected money laundering activity in the UK risks a criminal conviction, unless they make what is termed an ‘Authorised Disclosure’.

Authorised disclosure Section 338 authorises you to make a disclosure regarding suspicion of money laundering as a defence to the principal money laundering offences.

It specifically provides that you can make an authorised disclosure either:

- before money laundering has occurred;
- while it is occurring but as soon as you suspect; or
- after it has occurred, if you had good reason for not disclosing earlier and make the disclosure as soon as practicable.

You should make your disclosure to the nominated officer in WDC this is the MLRO, substitute (DMLRO).

The nominated officer will consider your disclosure and decide whether to make an external disclosure to the NCA. Criminal property is widely defined as property representing a person’s benefit from criminal conduct. It includes all proceeds from crime such as property (in the UK or abroad), money, and other assets that could also cover any interest held in land/land rights and/or property.

In court proceedings in order to secure a conviction it is only necessary to prove that the laundered property was criminal property. In other words even if the criminal property was generated as a result of the criminal activity of another person, the individual holding that property can be convicted of money laundering under the Proceeds of Crime Act 2002.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)

Main aspects

MLR 2017 transposed the Fourth EU Money Laundering Directive into UK Law, were laid before Parliament on 22 June 2017 and commenced on 26 June 2017. These obligations impact on certain areas of local authority business and require local authorities to maintain internal procedures to prevent the use of their services for money laundering.

A key difference of MLR 2017 is to require relevant persons to adopt a more risk-based approach towards anti-money laundering, particularly in the conduct of due diligence. Determining the appropriate level of due diligence requires analysis of risk factors based on the EU Directive and which are set out in MLR 2017.

It is a requirement of MLR 2017 that appropriate systems of internal control are in place to prevent activities relating to money laundering and terrorist financing. There must be management controls in place to identify the possibility that criminals may be attempting to launder money or fund terrorism, so as to enable appropriate action

to prevent or report it to be taken. MLR 2017 ends “automatic” due diligence. MLR 2017 also requires the creation of a “black list” of high risk jurisdictions which, if involved in a transaction, makes enhanced due diligence and additional risk assessment compulsory.

A new criminal offence was created in 2017: any individual who recklessly makes a statement in the context of money laundering which is false or misleading commits an offence punishable by a fine and/or up to two years’ imprisonment.

Additional requirements for Finance and Legal employees

Employees providing financial and/or legal services must also comply with the customer identification procedure, ‘due diligence’ and the record keeping procedures. There are various levels of due diligence with the regulations requiring due diligence to be carried out on a risk sensitive basis, taking account of customer and geographical risk factors, so that:

- Under MLR 2017 “simplified due diligence” is only permitted where it is determined that the business relationship of transaction presents a low risk of money laundering or terrorist funding, taking into account the risk assessment;
- “Enhanced due diligence” applies to those with a high risk status, for example remote transactions where the customer is not physically present to be identified would require additional appropriate documents to be requested;
- The “beneficial owner”, the individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted, should be identified;
- The business relationship should be scrutinised throughout its existence and not just at the beginning.

Reliance may be placed on due diligence undertaken by those regulated by the FCA or supervised by a listed professional regulator e.g. the Law Society. Any information obtained may be used as evidence in any subsequent investigation by the relevant enforcement authorities into money laundering.

In all cases, the evidence of the customer identification and record of the relationship/transaction should be retained for at least five years from the end of the business relationship of transaction(s). The records that must be kept are:

- A copy of, or references to, the evidence of the identity obtained under the customer due diligence requirements in the Regulations;
- The supporting evidence and records in respect of the business relationships and occasional transactions which are the subject of customer due diligence measures or ongoing monitoring;
- A copy of the identification documents accepted and verification evidence obtained;
- References to the evidence of identity; and
- Transaction and business relationship records should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect account or customer.

If satisfactory evidence of identity is not obtained at the outset of the matter then the business relationship or one off transaction(s) **cannot** proceed any further.

The customer identification procedure must be carried out when the Council is carrying out 'relevant business' and:

- Forms a business partnership with a customer,
- Undertakes a one-off transaction (including a property transaction or payment of a debt) involving payment by or to a customer of £5,000 or more,
- Undertakes a series of linked one-off transactions involving total payment by or to the customer(s) of £5,000 or more,
- It is known or suspected that a one-off transaction, or a series of them, involves money laundering.

In the above circumstances, employees must:

- Identify the person seeking to form the business relationship or conduct the transaction (an individual or company);
- Verify their identity using reliable, independent sources of information;
- Identify who benefits from the transaction;
- Monitor transactions to make sure they are consistent with what you understand about that person or country;
- Understand the source of their funds;
- Ensure there is a logical reason why they would want to do business with the Council.

This applies to existing customers, as well as new ones, but identification evidence is not required for matters entered into prior to 1 March 2004.

In relation to Council business appropriate evidence would be signed written instructions on Council headed note paper or an e-mail at the outset of a particular matter. Such correspondence should then be placed on file along with a prominent note explaining which correspondence constitutes the evidence and where it is located.

Records must be capable of providing an audit trail during any subsequent investigation, for example distinguishing the client and the relevant transaction and recording in what form any funds were received or paid. In practice, the Council will be routinely making records of work carried out in the course of normal business and these should suffice in this regard.

5. What is the Council's policy on Money Laundering?

The Council is committed to taking reasonable steps to minimise the likelihood of money laundering occurring in the course of its business and these procedures are designed to manage the risk of such an occurrence.

Our policy is to do what we can to prevent, wherever possible, the Council and its employees being exposed to money laundering, to identify the possible areas where it may occur and to comply with all legal and regulatory requirements, especially with regard to the reporting of actual or suspected cases. It cannot be stressed too strongly, however, that it is every employee's responsibility to be vigilant.

The Council will ensure that those employees who are most likely to be exposed to money laundering can make themselves fully aware of the law and, where necessary, are suitably trained.

As an organisation conducting "relevant business", the Council must:

- Appoint a Money Laundering Reporting Officer (MLRO) – see section 3 above;
- Implement risk sensitive policies and procedures relating to customer due diligence, reporting , record keeping, internal control, risk assessment and management and monitoring of compliance and the internal communication of such policies and procedures through the following:
- Undertake relevant risk assessments;
- Installing an appropriate risk management framework and a reporting regime;
- Establishing internal procedures to help prevent money laundering;
- Making arrangements to receive and manage the concerns of employees about money laundering and their suspicions of it, to make internal enquiries, and to make reports where necessary to the National Crime Agency ("NCA");
- Ensuring that all appropriate employees have an awareness of money laundering issues;
- Target training to employees most likely to encounter money laundering;
- Maintaining client identification procedures in certain circumstances; and
- Maintaining record keeping procedures.

6. What are the implications for the Council and its employees?

The consequences for employees of committing an offence are potentially very serious and the failure to disclose a suspicion of a case of money laundering is a serious offence in itself. Individuals can be found to be criminally liable for failing to report money laundering activity where it is known or suspected. This could result in serious criminal charges and/or sanctions being imposed on the Council and/or its employees. It is therefore important that policies and procedures exist to establish internal reporting arrangements and ensure compliance with the guidance and the law. Penalties include imprisonment, a fine or both.

The Council's Code of Conduct is designed to protect individuals when making a disclosure from any fear of victimisation or harassment.

Cash is the mainstay of criminal transactions, being the most reliable and flexible and having little or no audit trail. Any transaction involving an unusually large amount of cash should therefore cause questions to be asked about the source. However, electronic transactions also present a significant opportunity for money laundering.

At no time and under no circumstances should an employee voice any suspicions to the person(s) suspected of money laundering, otherwise the employee may be committing the offence of "tipping off", as described above. Similarly, no reference should be made on a client file to a report having been made to the MLRO. Should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render the employee liable to a prosecution. The MLRO will keep the appropriate records in a confidential manner.

The Council does not expect its officers to be involved in any of the three principal offences. However, if the suspicion of money laundering relates to a crime, then a failure to disclose is deemed to be a serious offence. There are only limited grounds for not reporting a suspicion.

7. What is a "Suspicious Transaction"?

The test for whether you hold a suspicion is a subjective one.

If you think a transaction is suspicious, you are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. You may have noticed something unusual or unexpected and after making enquiries, the facts do not seem normal or make commercial sense. You do not have to have evidence that money laundering is taking place to have suspicion.

If you have not yet formed a suspicion but simply have cause for concern, you may choose to ask the client/customer or others more questions. This choice depends on what you already know, and how easy it is to make enquiries.

If you think your own client/customer is innocent but suspect that another party to a transaction is engaged in money laundering, you may still have to consider referring your client/customer for specialist advice regarding the risk that they may be a party to one of the principal offences.

Therefore the law requires you to be vigilant and to immediately report any suspicious transaction. **Suspected cases should be reported to your supervisor / manager who will then report to the MLRO.** Reports of suspicious transactions could be made from employees, members of the Council, contractors, the public, the Police, or any other related party or partner. Once this is received, it is then for the MLRO to ascertain what investigation has been carried out to verify money laundering suspicions. The MLRO will decide whether there are reasonable grounds for suspicion. If it is warranted, a report will be made to the NCA by way of a Suspicious Activity Report (SAR) form found on the NCA website.

There is no clear definition as to what constitutes suspicion – common sense is required. However, the following could be taken as warning signs:

- The address given is care of a third party;
- A mobile phone number is the only means of contact provided i.e. no contact address or land-line number;
- Evasive answers and / or a failure to respond to questions;
- Refusal to provide identification;
- Unusual activity for the customer;
- Payment appears to be out with the customer's financial means;
- Payment is made by a third party who is not responsible for the debt;
- Significant overpayments which result in refunds from the Council; and
- Two or more transactions which total more than the limits set out below.

The list below provides examples relevant to Council activity, in which money laundering could occur:

- cash payments, for example, where an individual has substantial Council Tax or Rent arrears, or offers to purchase a Council property and settles by making a large cash payment;

- a customer or supplier who makes substantial overpayments or duplicate payments and subsequently requests large refunds;
- a customer who receives a business loan and repays it long before the due date and/or partly in cash;
- where there are concerns regarding the identity, location, honesty or integrity of a client or customer;
- a customer or supplier who is secretive and refuses to provide information when requested without giving any reasonable explanation;
- the involvement of a third party without any reason or explanation, e.g. the unnecessary routing or receipts of funds from third parties or through third party accounts;
- correspondence / information being received on behalf of other companies;
- poor accounting records and financial control, e.g. companies tendering for contracts that are unable to provide adequate financial details or requests for grant funding not supported by adequate accounting records;
- requests to pay money overseas or to make payments in foreign currencies with no reasonable explanation;
- other local authorities or companies querying the legitimacy of customers;
- unusual property or investment transactions, e.g. requests to purchase or rent Council assets / land with no clear business motive.

The above list is not exhaustive, but is intended to give employees an understanding of how the Council could potentially be involved in a transaction that should be brought to the MLRO'S attention.

8. Ensuring the Policy is followed

Awareness training will be provided for those employees in high risk roles, where they are more likely to experience possible signs of money laundering. This will be coordinated by the MLRO and delivered as appropriate.

All Strategic Leads must ensure that these procedures are brought to the attention of all employees.

Employees who fail to follow the rules and procedures laid out could be subject to disciplinary procedures, as well as potentially being criminally liable and face prosecution.

9. Reviewing the Policy

Internal Audit undertakes to look at all control frameworks in all planned audits including money laundering by substantive testing of transactions as deemed appropriate.

This policy will be reviewed by the Strategic Lead - Resources or designated officer on an annual basis to take account of any legislative changes and procedural improvements.

10. Further information

Further information can be obtained from the MLRO and the following sources:

- Website of the National Crime Agency
  http://www.nationalcrimeagency.gov.uk/

- Draft CCAB Anti-Money Laundering Guidance for the Accountancy Sector
  https://www.ccab.org.uk/documents/TTCCABGuidance2017regsAugdraftforpublication.pdf
- Quick guide to Money Laundering Regulations 2017 from the Law Society
  http://www.lawsociety.org.uk/support-services/advice/articles/quick-guide-to-the-money-laundering-regulations-2017/

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on payer) Regulations 2017
  http://www.legislation.gov.uk/uksi/2017/692/pdfs/uksi_20170692_en.pdf

11. Money Laundering Procedure

The procedure for employees is contained in a separate document