

# MLR 8 at a glance - a quick guide to the prevention of money laundering and terrorist financing

## Contents

- [Introduction](#)
- [Who needs to see this?](#)
- [Why is this guide important to the business?](#)
- [Business obligations](#)
- [Risk assessment and management](#)
- [Customer due diligence](#)
- [Reporting](#)
- [Record keeping](#)
- [Internal controls and internal communication](#)
- [Agents](#)
- [Monitoring and management of compliance](#)
- [Staff awareness and training](#)
- [What happens if the business fails to comply with the regulations?](#)

## 1. Introduction

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins. It also covers money, however come by, which is used to fund terrorism.

There is no one method of laundering money. Methods can range from the purchase and resale of a luxury high value item (for example a car or jewellery) to passing money through a complex web of legitimate businesses and 'shell' companies (ie those companies that primarily exist only as named legal entities without any trading or business activities).

## 2. Who needs to see this?

You will find this quick guide useful if you are a proprietor, director, manager, employee or nominated officer of a Money Service Business (MSB), a High Value Dealer (HVD), or a Trust or Company Service Provider (TCSP).

The quick guide may help you to understand the basic legal requirements for preventing money laundering and combating terrorist financing under the Proceeds of Crime Act

2002 (PoCA), the Terrorism Act 2000 (TA00) and the Money Laundering Regulations 2007.

This quick guide is not approved by the Treasury. It is not intended to be used as an alternative to the more detailed guidance in [MLR 8 \(PDF 677K\)](#).

There are sector specific helpsheets at the back of this quick guide for:

- [HVDs \(PDF 32K\)](#)
- [Bureaux De Change \(PDF 33K\)](#)
- [Money Transmission Businesses \(PDF 30K\)](#)
- [Cheque Encashment Businesses \(PDF 34K\)](#)
- [Trust or Company Service Providers \(PDF 43K\)](#)

### **3. Why is this guide important to the business?**

It can sometimes be difficult dealing with the three pieces of legislation concerning the prevention of money laundering and combating terrorist financing. This quick guide is intended to give relevant people in businesses a basic understanding of the legal requirements when dealing with customers.

## **4. Business obligations**

### **Risk assessment and management**

Refer to section 6 of MLR 8 and relevant sectoral guidance in appendices 6-10.

Businesses must identify and assess the risks of their being used for money laundering or terrorist financing activity, mitigate these as far as possible by putting appropriate procedures and controls in place and monitor regularly, adjusting as necessary to keep them relevant and up to date – the section on Internal controls and internal communication explains these requirements in more detail.

- Your risk assessments will probably fall within the following areas:
- customers – type and behaviour
- products and services
- delivery channels eg cash over the counter, electronic, wire transfer, cheque
- geographical areas of operation or destination of funds or goods

HMRC will not dictate what risk-based measures should be in place for your business, it is for you and your senior managers to decide what is a reasonable approach which balances the costs to your business and your customers with a realistic assessment of the risks involved.

Remember to write down your risk-based policy and procedures and keep it up to date. As your supervisor HMRC may ask for details of your policies and procedures.

See appendix 3 MLR 8 for additional support in preparing a risk based policy statement that will then help you produce your business procedures.

## **Customer due diligence and ongoing monitoring**

Refer to regulations 5, 7 and 14 MLR 2007 and guidance in section 7 of MLR 8.

Knowledge and awareness of a customer's business activities or source of funds will help you to assess whether the transactions and activities undertaken or proposed are consistent with your expectations of that business or type of customer. These enquiries will also help you to identify when a transaction, or a pattern of transactions, is unusual and so must be looked into as potentially suspicious activity that must be reported to the Serious Organised Crime Agency (SOCA) (see the next section on Reporting for further information).

The Money Laundering Regulations specify the customer due diligence (CDD) steps you must take when you establish a business relationship with a customer, or carry out transactions that have a risk of money laundering attached. For some customers or situations where there is a higher risk of money laundering or terrorist financing, you are required to carry out enhanced due diligence (EDD). Where you have a continuing business relationship with a customer, you must undertake ongoing monitoring (OM) of the customer's activities. The table below summarises the regulatory requirements.

HMRC has provided information on acceptable types of evidence for identity checks at Appendix 5 in MLR 8.

<b>MLR 2007</b>	<b>Type of customer activity and timing</b>	<b>Customer due diligence/ ongoing monitoring</b>
Reg.7(CDD)	Establishing a business relationship.	Obtain and verify ID documents, data or information. Where appropriate, identify and verify details of the beneficial owner.
Reg. 8 (OM)	Transactions undertaken throughout the course of a business relationship.	Obtain information on the purpose and intended nature of the business relationship.  Carry out ongoing monitoring. This means: <ul style="list-style-type: none"><li>• scrutiny of transactions, including, where necessary, the source of funds</li></ul>

Reg. 7 (CDD)	Occasional transactions where there is no business relationship of €15,000 (£9,000) or over, where there are no significantly higher than usual risk factors present.	<ul style="list-style-type: none"> <li>• keeping documents and information on the customer up to date</li> </ul>
Reg.14 (EDD)	This section applies to customers with whom there is a business relationship <b>and</b> those doing transactions that fall into the following categories: <ul style="list-style-type: none"> <li>• non face-to-face customers</li> <li>• politically exposed persons</li> <li>• any other situation that, by its nature can present a higher risk of money laundering or terrorist financing, including where transactions are below €15,000</li> </ul>	<p>Obtain and verify ID documents, data or info.</p> <p>Where appropriate, identify and verify details of the beneficial owner.</p> <p>In addition to obtaining and verifying the ID of the customer), and, where appropriate, the beneficial owner, take risk-based further checks.</p> <p>Where the customer is not physically present for identification purposes, or there is a risk of impersonation fraud, obtain additional evidence of identification and/or apply supplementary measures to verify the documents supplied.</p> <p>Consider undertaking the first transaction through a bank account in the customer's name.</p> <p>For PEPs: carry out appropriate and reasonable extra checks, eg for occasional transactions (over £9,000), obtain details of the source of funds and purpose of transactions (S7.12).</p>

## Reporting

Refer to Part 7 of the Proceeds of Crime Act, Part 3 of the Terrorism Act, Regulation 20 MLR 2007 and guidance in section 10 of MLR 8.

Businesses in the regulated sector and their employees must disclose information to SOCA when they know or suspect, or they have reasonable grounds for knowing or suspecting, that someone is engaged in money laundering or terrorist financing. You can make such disclosures by completing and sending a Suspicious Activity Report (SAR).

Businesses (unless they are an individual with no employees) must appoint a nominated officer to receive disclosures from their employees, and have policies and procedures in place for employees to make such disclosures to the nominated officer. These disclosures

need to contain as much information as possible about the customer, transaction or activity.

The nominated officer or proprietor submits SARS to SOCA using the [SARs online system](#) or sending reports electronically, by fax, first class post or courier.

HMRC has provided some general examples of indicators of suspicious activity in section 10.8 of MLR 8. Sector specific indicators are listed in sections 18.4 (HVD), 19.8 (BdC) and 20.21 (cheque cashing).

Remember, it is a criminal offence to say anything that may either tip off a person that a disclosure has been made, or prejudice an investigation.

## **Record keeping**

Refer to regulation 19 MLR 2007 and guidance in section 12 of MLR.

Keeping records of the due diligence checks made, and information held, on customers and details of transactions is an important requirement that enables your business to demonstrate its compliance with the MLR 2007. These records will be crucial in any subsequent investigation, enabling your business to produce a sound defence against any suspicion of involvement in money laundering or terrorist financing, or charges of failure to comply with the Money Laundering Regulations.

The records can include daily log books, receipts, cheques etc. and must be maintained so that an audit trail establishes a financial profile of any suspect account or customer.

Keep your business records for five years, beginning on the date on which the business relationship ends or, in the case of occasional transactions, five years from the date of completion of the transaction. Records can include any of the following:

- original documents
- photocopies
- on microfiche
- in a scanned format
- computerised or electronic

## **Internal controls and internal communication**

Refer to guidance in section 5 of MLR 8.

You must ensure that your business has internal control systems capable of identifying unusual or suspicious transactions or customer activity and reporting the details quickly to the nominated officer or proprietor, responsible for making a report to SOCA.

Your business must have a written MLR profile, including risk assessment and monitoring procedures to cover:

- the responsibilities of your senior managers and nominated officer regarding money laundering and terrorist financing risks
- training your staff on the legal and regulatory responsibilities for money laundering and terrorist financing controls and measures
- keeping up to date copies of your business' risk management policies and procedures in relation to money laundering

## **Agents**

Refer to guidance in section 5.1.3 of MLR 8.

If your business uses agents offering your products and services, you must make sure that their premises are included on the HMRC register and that they are following your customer due diligence and internal reporting procedures. If your agents fail to comply with the Money Laundering Regulations, it is the registered business that will be liable for civil penalties, de-registration or prosecution.

Your agents will not be subject to the 'fit and proper test' under regulation 28 MLR 2007, however, we recommend that you check that they meet the same standards.

## **Monitoring and management of compliance**

Refer to guidance in section 6 of MLR 8.

It is important that there are monitoring procedures in place to lessen your business risks and ensure that your staff and agents are complying with the 2007 regulations.

Some areas to consider in particular are

- identifying changes in customer characteristics or behaviour
- new products and services which may be used for money laundering or terrorist financing, recognising how these ways can change, with reference to information and typologies supplied by law enforcement feedback
- the adequacy of staff training and awareness, especially if agents are used or there is a high turnover in staff
- compliance monitoring arrangements eg internal audit/quality assurance processes or external reviews
- the balance between technology-based and people-based systems
- capturing appropriate management information
- upward reporting and accountability, especially if agents are used or there is a high turnover in staff
- improving internal communication, especially where your business covers multi-locations

- effective liaison with regulatory and law enforcement agencies

## **Staff awareness and training**

Refer to regulation 21 MLR 2007 and guidance in section 11 of MLR.

Make all your staff aware of the law relating to money laundering and terrorist financing. Regularly train staff so that they can recognise and deal with suspicious transactions. Providing regular up to date relevant training will ensure that your business remains compliant with the 2007 regulations and conducts its activities within the law.

It is helpful for your staff to have access to the business' risk based policies and procedures, know who their nominated officer is, the requirements within the 2007 regulations, HMRC's role (including the sanctions that may be given for non-compliance), their management line for queries and access to any industry or government agency guidance. They should also have a good understanding of how your business conducts itself. HMRC can provide an educational DVD, which all your staff should watch as part of their initial and regular training.

## **5. What happens if the business fails to comply with the Regulations?**

Refer to regulations 30, 42 and 46 MLR 2007 and guidance in appendix 2 of MLR 8.

HMRC will impose appropriate civil penalties on businesses that fail to comply with the requirements of the Money Laundering Regulations in order to deter further non-compliance.

If you do not agree with the reason given for a penalty or the amount of the penalty, you can ask for an independent review of the decision, which will be undertaken by a separate part of HMRC.

If after the review, the decision stands but you still do not agree, you can appeal to the VAT and Duties Tribunal.

In the case of money service business, or trust or company service providers who consistently fail to comply with the Regulations (and also, for money transmitters, fail to comply with the EU Wire Transfer Regulation), HMRC is obliged to cancel their registration.

If you do not agree with a de-registration notice, you can ask for an independent review of the decision by another part of HMRC.

If after the review, the decision still stands but you still do not agree, you can appeal to the VAT and Duties Tribunal.

As it is an offence under the Regulations to act as a money service business, or Trust or Company Service Provider without a registration, if you continue to trade HMRC will impose civil penalties or prosecute you.

The above is HM Revenue and Customs Public Notice MLR8 at a glance guide and is subject to Crown copyright protection.