Money Laundering

Guidance for Branches - Processing and Reporting FX and Cash Transactions

1. Introduction

1.1. The **Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017** set out what relevant businesses must do to prevent the use of their services by criminals for **money laundering** or **terrorist financing** purposes.

1.2. The **Criminal Finance Act 2017** sets out what businesses must do to avoid knowingly or unknowingly **facilitating tax evasion**.

1.3. The Society's Travel group, and more specifically its currency exchange facility (bureau de change), is classed as a **Money Service Business ("MSB")** and is **regulated by HMRC**, which supervises businesses' anti-money laundering processes and practices, as well as their compliance with the Regulations.

1.4. Criminals use currency exchange offices to change bulky low denomination notes into easily transported high denomination notes currency. They also often change money to facilitate further criminal activity, and to launder criminal funds by buying assets in overseas countries. They will try to identify any weakness in a currency exchange office's anti-money laundering controls in order to exploit them.

1.5. Criminals sometimes purchase holidays in cash to launder or spend proceeds of crime. Criminals sometimes also purchase foreign currency to pay for goods or services abroad, which means the party they are paying doesn't have to declare the payments received as taxable income.

1.6. To meet our obligations under money laundering legislation and the Criminal Finances Act 2017, the Society carries out anti-money laundering checks on **all** cash purchases and FX transactions of £5,000 or more in its Travel business. This includes where the transactions are "linked" – being more than one transaction by the same customer within 60 days, exceeding the £5,000 threshold.

1.7. **This guidance sets out the process for carrying out checks on any cash purchases and/or all FX transactions in travel of £5,000 or more.**

1.8. Failing to comply with the Money Laundering Regulations and the Criminal Finance Act is a criminal offence. Where a colleague's actions result in a breach of the relevant legislation, it may result in disciplinary action being taken.

1.9. This Guidance should be read in conjunction with the Society's ***Money Laundering Policy***.

2. Who is responsible?

The **Society's Money Laundering Reporting Officer (MLRO)** is responsible for the overarching monitoring of the Society's compliance with the Regulations, and for ensuring appropriate training is made available to colleagues.

The MLRO is supported by the Compliance and Governance Manager within the Travel division who helps ensure the effective implementation of the compliance framework and controls.

The Society's MLRO will also report promptly to the **National Crime Agency (NCA)** any suspicious transactions carried out in any of our Travel branches, that may be suspected to be linked to money laundering or terrorist financing activities.

2.1. **Travel branches are responsible** for:

2.1.1. **Identifying potential risks** when dealing with customers' transactions

2.1.2. **reporting accurately and promptly** to the Society's MLRO all cash purchases and FX transactions (including linked transactions) of £5,000 and over, following the process described in this Guidance

2.1.3. ensuring that **no FX transaction exceeds £10,000** (whether single or linked transaction)

2.1.4. ensuring **that business customers are not using our FX services** – it is for individuals only

2.1.5. ensuring that individuals are **not using FX services to pay for commercial goods or services abroad** (e.g. paying for a holiday home renovation)

2.1.6. **contacting the Society's MLRO** when in doubt, or if further guidance is needed, before proceeding with any transaction of £5,000 and over

2.1.7. using the Watchman alert system and not overriding any flags without authority from the MLRO.

3. Tipping-Off

3.1. **Disclosing to the customer that you are going to report their transaction to the MLRO (or the NCA, or the Police) as "suspicious" is a criminal offence**, so you should not "tip off" the customer about your intention to report the transaction, even if that is precisely what you are going to do after they have left the branch.

3.2. **You should not refuse to carry out a transaction** on the grounds of a customer, or a transaction, looking suspicious, as long as all necessary ID and proof of address evidence have been provided.

4. Linked transactions

4.1. When a customer transacts (cash purchases and/or FX transactions) more than once over a **60-day period** these are considered 'linked transactions'

4.2. If two or more **linked transactions** for a customer equates to £5,000 or more during a 60-day period, the Money Laundering Reporting Form must be completed once the reporting threshold has been met.

4.3. Colleagues may become aware that a transaction is linked because either they or another colleague served the customer during the period, or where the Watchman system alerts it as being linked.

5. Business Customers

5.1. The Society operates its foreign exchange services for the benefit of customers who are going abroad to ensure they have spending money they require. We do not therefore offer these services to business customers.

5.2. A business customer is broadly any type of corporate organisation such as company, charity, or other co-operative society etc but it can also be unincorporated organisations, such as sole traders, schools, associations, clubs etc.

5.3. With effect from August 2023, the decision has been made to **no longer** transact with **business customers** across **all** Travel branches. This decision was taken to be aligned to the intended purpose of the FX services in our branches and to further reduce the risk of money laundering or facilitation of tax evasion.

5.4. Branches are required to **not** carry out any cash purchases and/or FX transactions with any business customers, including any business customer who has historically used these services. Branches are asked to contact the MLRO for clarification if unsure whether an individual is considered a 'business customer' prior to carrying out any transaction(s).

6. How to recognise suspicious transactions or customer behaviours

6.1. Whilst carrying out an FX or cash transaction, you must **feel free to ask** as many questions as you think necessary to a customer, to ensure you are satisfied that both the customer, that the purpose of the transaction is legitimate, that the source of the funds is lawful, and to be able to complete your KYC (Know Your Customer) process correctly.

6.2. To ensure we remain vigilant to any potential tax evasion scenarios, branches must **not** allow customers to **purchase foreign currency** if the funds are to be used to **pay for services abroad** such as renovating holiday home in Spain etc. That is because, in some circumstances, the service provider (eg builder) may fail to declare those funds for tax purposes. In these circumstances, although we and the customer are not avoiding tax ourselves, it could be deemed as facilitating (i.e. enabling) the tax evasion of the service provider which is an criminal offence.

6.3. The below checklists can help you spot unusual or potentially **suspicious transactions and customer behaviours**:

For new customers

- Checking the customer's identity is proving difficult, the customer is reluctant to provide details of their identity or provides fake documents.
- The customer is trying to use intermediaries to protect their identity or hide their involvement.
- there is no apparent reason for using our business - for example, another business is better placed to handle the transaction, or closer to their residential area.
- The customer requests high denomination notes, for example €100, and €200 notes or $100 US notes.
- The customer is willing to accept poor rates of exchange.
- The destination of the transmission is suspicious.
- The customer is buying currency that doesn't fit with what the business knows about their travel destination.
- The customer wishes to exchange large volumes of low denomination notes.

For regular and existing customers

- The transaction is different from the normal type of transactions the customer would ask to do.
- The size and frequency of the transaction is different from the customer's normal pattern of transactions.
- The customer's pattern has changed since the relationship was established.
- There has been a significant or unexpected improvement in the customer's financial position.
- The value of the transaction is just below a relevant reporting threshold (e.g. £5,000) and the customer has visited previously for similar sums.

For all customers

- A third party, apparently unconnected with the customer, bears the costs, or otherwise pays for the transaction costs
- The customer asks to do an unusually big cash or foreign currency transaction
- The customer won't disclose the source of the funds; or is unable to provide satisfactory evidence of the source of the funds; or the source of the funds is unusual.
- You notice an unexplainable involvement of third parties, or large payments from private funds, particularly where the customer appears to have a low income. The value of the transaction is just below a relevant reporting threshold (e.g. £5,000).

7. Watchman

7.1. Ultrapos now includes a compliance software called 'Watchman' which is embedded with criteria to prompt branches at key points during the transaction process. These appear as error messages and should not be bypassed

7.2. The error messages are as outlined below:

- Velocity Hit – when a customer has transacted £5,000 or more with any of the Society's Travel branches during a 60-day period. The below error message will appear:

  'This customer has orders that exceed the £5000.00 threshold for completing a Money Laundering Reporting Form. You are required to complete the form and obtain the necessary ID from the customer before completing the transaction'.

- PEP Hit – when a customer transacting is classed as Politically Exposed Persons. The below error message will appear:

  'Potential PEPs Match. You must seek approval from the Society's MLRO before proceeding'.

7.3 Where a Watchman alert is received, you should **not** proceed with the transaction. You can try inputting additional details from the customer to see if that results in the match being avoided. However, where an alert is still received **you must not proceed with the transaction**. Only the MLRO can authorise an override and where the MLRO cannot be contacted, you should not proceed.

7.4 Where a Watchman alert results in a transaction being discontinued, you should apologise to the customer and explain that the system is not permitting you to complete the transaction.

8. Need more help?

8.1. This Guidance document, and the enclosed ***Useful Questions & Answers***, should be sufficient to help you decide what to monitor when you carry out any cash transactions, and how to properly report transactions.

8.2. However, if you are in doubt, always consult with your Manager in the first instance, or **Richard Simpson, Compliance & Governance Manager** (Richard.simpson@midcounties.coop). You can contact the Society's MLRO directly at: money-laundering@midcounties.coop, or by phone: 07548127154, **before carrying out any transactions of £5,000 and over**.

9. Guidance updates

9.1. This Guidance will be reviewed by the Society's MLRO on a regular basis to ensure it remains relevant with the Society's obligations under applicable law.

Useful Questions & Answers

1) Are all high-risk transactions suspicious?

To minimise risk, the limit of any FX transaction (single or linked) is £10,000. Identifying a customer or a transaction as **high risk** does not automatically mean that they're involved in money laundering or terrorist financing. Equally, identifying a customer or transaction as **low risk** does not mean that they're not involved in money laundering or terrorist financing; in most cases, alertness and common sense should guide you on a case-by-case basis.

2) What transactions do we need to monitor?

All transactions are recorded on our system and undergo some form of monitoring. For transactions on **all cash purchases and FX transactions of £5,000 and over, we require an AML form to be completed which includes copies of ID. That completed form must be reported to the Society's MLRO.**

You do this by logging a ***Money Laundering Reporting Form***, making sure it is fully completed and sent to the Society's MLRO. **Don't forget** to enclose all required supporting evidence with the Form. **Always ensure you are using the most up-to-date reporting form** - you can obtain this from Colleagues Connect here:https://colleaguesconnect.midcounties.coop/siteassets/quick-links/personnel-forms/money-laundering-reporting-form.pdf

3) What are linked transactions?

Linked transactions may be a series of transactions by a legitimate customer, or they may be transactions that appear to be independent but are in fact split into two or more transactions to avoid our detection. The time period we look at for a linked transaction is a rolling 60-day period. This typically happens when a **customer tries to avoid our controls by splitting transactions into several smaller amounts**, or perhaps using different branches, to stay below the level at which you would check their ID or enquire about the source of funds.

4) What about customers we have usual and on-going relationships with?

On-going customer relationships should continue to be monitored after they are established, as **familiarity may become a risk trigger**. This means that you should continue to remain vigilant, **monitor the source of funds**, and ensure transactions are **consistent with what you know** about the customer.

Cash purchases and FX transactions will still need to be reported to the MLRO when they are of £5,000 and over, using the Money Laundering Reporting Form. Branches must also ensure that any single FX transaction does not exceed the agreed £10,000 personal limit per customer.

5) How is money laundering connected to fraud?

Criminal activity related to fraud generates money that needs to be laundered, so **where there is fraud there is money laundering**. When we think of fraud risk, we automatically think of the risk of financial loss for the Society; so, **the key question should be: is the money really there?** for example, a customer buys an expensive holiday and wants to pay by cheque; naturally, you would want to ascertain the money is there and wait for the cheque to clear before releasing tickets etc.

Likewise, for money laundering, **your key question should be: where did the money come from?** For example, a customer buys an expensive holiday, and produces £30k in cash to pay for the holiday. When completing the reporting form, you should ask why they are using cash for the purchase rather than a credit or bank card, which is more common. The risk is that the cash has not been deposited into a bank account because of the questions that may be raised as to its source by the bank. Likewise, we should ask those questions when cash totalling £5,000 or more is being used to buy a holiday or FX money.

This is when you should apply your acquired knowledge, experience and the Society's procedure to ensure you remain compliant with anti-money laundering legislation. **It is okay to ask questions** and, if it doesn't feel right, **continue to carry out the transaction**, provided all the required ID and proof of address evidence have been checked and copies retained. You should then complete the Reporting Form, ticking the box "suspicious transaction", **explaining your reasons** for doing so.

6) What ID evidence and proof of address should I ask customers for?

The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 require that you obtain identity (ID) evidence and proof of address from customers when carrying out money exchange transactions.

HMRC's recommended guidance is enclosed in **Appendix 1** for information – you will see that guidance is provided for customers. If you have any doubt or require further assistance, you should talk to your Manager or contact the Society's MLRO directly.

Remember – **the same form of identification cannot be used for both ID proof and proof of address**. For example, if a customer provides their driving licence as proof of identity, a different form of identification must be produced by the customer as proof of address, for example a utility bill.

7) What if I am not satisfied with the ID evidence provided by the customer?

If you are not satisfied that the customer's identity has been adequately verified, you **must not carry out a transaction with or for the customer**, or establish a business relationship, or carry out an occasional transaction with the customer. Instead, you should explain to the customer that **additional or different ID evidence is required**, and that they are welcome to return once such evidence is available to carry out the transaction. For clarity, the essential elements to identify a customer are the **customer's full name**, **residential address**, **DOB**, original (not photocopies, unless certified) **ID document** (passport or valid photo card driving licence) and **credit/bank account statement or recent utility bill** dated within the last three months.

8) What about non-UK resident customers?

For non-UK residents, similar customer's identification rules apply as for UK residents, so you will need to verify the customer's **full name**, **residential address**, **DOB** and original (not photocopies, unless certified) **passport**. If in doubt, you should **contact the Society's MLRO for further guidance** before you carry out the transaction.

9) What are PEPs, and how should I deal with these transactions?

PEP means **Politically Exposed Person**. HMRC's guidance for money service businesses, such as the Society's Travel business, indicates that in certain situations you must carry out "**enhanced due diligence**"; for example, when you enter into a business relationship with a politically exposed person, i.e. individuals, or organisations, whose prominent position in public life may make them **vulnerable to corruption, bribery, fraud and money laundering**. This would include, for instance:

a) head of state
b) head of government
c) minister or deputy or assistant minister

d) Member of Parliament
e) member of supreme courts, or constitutional courts or of other high-level judicial bodies
f) member of courts of auditors
g) member of the board of a central bank
h) ambassador, chargé d'affairs
i) high-ranking officers in the armed forces
j) member of the administrative, management or supervisory bodies of a state-owned enterprise.

IMPORTANT!

You must seek the **Society's MLRO approval** before completing a transaction with a PEP.

10) Should I carry out a transaction for a customer who is not present?

It is acceptable to carry out a transaction for a **customer who is acting on behalf of a third party** ie. another individual who is not present, as long as you seek to **verify the identity of both the customer acting on behalf and the third party**. If the evidence provided by the customer is not satisfactory, refer to question 7) above.

11) What are suspicious transactions?

A **suspicious transaction** is one for which there are **reasonable grounds to suspect** that the transaction is related to a money laundering offence or a terrorist activity financing offence; this generally means that you think a transaction, or a group of transactions (see question 4) above) raises questions or gives rise to discomfort, apprehension or mistrust.

There is no requirement, under money laundering legislation, to close a customer's on-going relationship or stop dealing with a customer if you suspect a transaction may be suspicious; you should instead carry out the transaction as normal – provided you have obtained **satisfactory ID evidence** and taken copies of all relevant documents – and then **report the transaction to the Society's MLRO** in the usual way, via the Money Laundering Reporting Form, **ensuring the box "suspicious transaction" is ticked.**

12) If I think a transaction is suspicious, should I tell the customer?

No, **you shouldn't**. It is a **criminal offence** to say or do anything that may alert a customer that a suspicion has been raised, or that a money laundering investigation may be carried out, or that the transaction may be reported to law enforcement authorities.

This offence is called **tipping-off**, and it means that you should never disclose to a customer that their transaction will be reported to the Society's MLRO as "suspicious"; or tell a customer the transaction cannot be carried out because you believe they may have criminal or fraudulent intentions.

13) Are the money laundering regulations applicable to the Society?

Yes –It is applicable to the Society in relation to its foreign currency exchange business, currently supervised by HMRC. Particularly for Money Service Businesses, such as our Travel branches, the Regulations focuses on **customer due diligence**, **reporting obligations**, **record-keeping** and **internal controls**.

Branches should ensure they continue to apply the correct customer due diligence and reporting procedures as explained in this Guidance.

14) Watchman has flagged that the customer is a PEP, should I proceed?

You should first try inputting additional details from the customer to see if that results in the match being avoided. However, where an alert is still received **you must not proceed with the transaction**. Only the MLRO can authorise an override and where the MLRO cannot be contacted, you should not proceed.

If the transaction is discontinued, you should apologise to the customer and explain that the system is not permitting you to complete the transaction.

15) Who should I contact if I need further assistance, or to obtain a copy of the Society's Money Laundering Policy and other available guidance for colleagues?

All policies and procedures are available on **Colleagues Connect** (https://colleaguesconnect.midcounties.coop/). The Money Laundering policy and documents are in the process of being added. In the meantime you should contact the **relevant colleagues within the Travel business**:

- Richard Simpson, Governance & Compliance Manager
  richard.simpson@midcounties.coop
- David Watts-Davies, Learning & Development Manager
  david.watts-davies@cooptravel.coop

Alternatively, you can contact the **Society's MLRO** directly at money-laundering@midcounties.coop; or by phone: 07548 127154. You can write to: The Midcounties Co-operative, Co-operative House, (attn. of: MLRO), Secretariat Group, Warwick Technology Centre, Warwick CV34 6DA.

Money Laundering

APPENDIX 1

HMRC GUIDANCE – PROOF OF IDENTITY

1. Proof of identity checklist for individuals

Proof of name	**Proof of address**
Current signed passport	Utility bill (gas, electric, satellite television, landline phone bill) issued within the last three months
Original birth certificate (UK birth certificate issued within 12 months of the date of birth in full form including those issued by UK authorities overseas such as Embassies High Commissions and HM Forces)	Local authority council tax bill for the current council tax year
EEA member state identity card (which can also be used as evidence of address if it carries this)	Current UK driving licence (but only if not used for the name evidence)
Current UK or EEA photocard driving licence	Bank, Building Society or Credit Union statement or passbook dated within the last three months
Full old-style driving licence	Original mortgage statement from a recognised lender issued for the last full year
Photographic registration cards for self-employed individuals in the construction industry -CIS4	Solicitors letter within the last three months confirming recent house purchase or land registry confirmation of address

Proof of name	Proof of address
Benefit book or original notification letter from Benefits Agency	Council or housing association rent card or tenancy agreement for the current year
Firearms or shotgun certificate	Benefit book or original notification letter from Benefits Agency (but not if used as proof of name)
Residence permit issued by the Home Office to EEA nationals on sight of own country passport	HMRC self-assessment letters or tax demand dated within the current financial year
National identity card bearing a photograph of the applicant	Electoral Register entry
	NHS Medical card or letter of confirmation from GP's practice of registration with the surgery