ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Banking

Sector Specific AML/CFT Guidance Notes

August 2021

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Version 3
Last updated August 2021

Contents

Version history

Version 2 (April 2020)	Updates made to links in relation to the updated NRA
Version 3 (August 2021)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes 5 - changes made to reflect the removal of timescales for ongoing monitoring from the Code

1. Foreword

For the purposes of this sector specific guidance, the terms "banking" and "bank" refer to a business conducting activity that would require a licence under Class 1 of the Regulated Activities Order 2011 (as amended) to undertake deposit taking.

2. Introduction

The purpose of this document is to provide some guidance specifically for the banking sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by banks and provides further guidance in respect of approaches to customer due diligence where it may vary across or between sectors.

The case studies in this document were taken from typologies published by the Australian Transaction Reports and Analysis Centre ("AUSTRAC") and the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"). The Authority recommends that relevant persons familiarise themselves with these, and other typology reports concerning the banking sector such as the FATF Guidance for a Risk Based Approach for the Banking Sector which was published in 2014.

2.1 National Risk Assessment

The Island's first National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. The banking sector must ensure their business risk assessment (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

The nature of banking products and services, and some customer segments serviced (including high net worth individuals ("HNWI"), complex structures and PEPs), result in core inherent vulnerabilities. These vulnerabilities include, but are not limited to:

- Difficulty in establishing source of funds / source of wealth in more complex structures and understanding the purpose of such structures;
- The non-face to face nature of relationships and use of introducers / third parties;
- Sanctions risks arising from the international nature of the sector and exposure to higher risk countries (including for payments); and
- Domestic laundering (using cash) from drug related crimes.

The importance of strong controls is therefore paramount to manage and mitigate these vulnerabilities. The NRA sets out the main risks and vulnerabilities in detail.

It is considered that the overall risk for Banking is medium taking into account the threats and vulnerabilities, balanced against the controls in place in the sector. The domestic inherent retail risk (including HNWI) is medium but the international retail (including HNWI) and corporate / trust sector risks are inherently medium high. There are limited instances of the IoM banking sector being potentially used for FT, and ML is considered to be the higher risk.

3. Risk Guidance

The banking industry is a broad sector and the ML/FT risks will vary for each bank based on a wide range of factors such as the type of products they supply, their customers and delivery channels.

The Code mandates that a number of risk assessments are completed –

- a business risk assessment (paragraph 5);
- a customer risk assessment (paragraph 6); and
- a technology risk assessment (paragraph 7)

In order to complete these risk assessments and keep them up-to-date vigilance should govern all aspects of a bank's dealings with its customers, including:

- account opening;
- non-account holding customers;
- safe custody and safe deposit boxes;
- deposit-taking;
- lending; and
- transactions into and out of accounts generally, including by way of electronic transfer (wire transfer) and automated cash deposits into third party accounts.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship high risk; a customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a bank is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. Refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 (Ongoing monitoring) of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;

(b) conduct EDD in accordance with paragraph 15; and

(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and

(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and banks should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. A list of suggested red flags is included at section 3.2 of this document.

- where a customer is reluctant to provide normal information or provides only minimal information;
- where a customer's documentation cannot be readily verified;
- where a customer seems to deliberately provide information which is difficult or expensive for the bank to verify;
- the customer is reluctant to provide the bank with complete information about the nature and purpose of the relationship including anticipated account activity;
- the customer is located in a higher risk jurisdiction;
- transactions involving numerous jurisdictions;
- unusual cash deposits without apparent cause, particularly where such deposits are subsequently withdrawn or transferred within a short time;
- frequent small or modest cash deposits which taken together are substantial;

- the collection (either within the Isle of Man or in another country or territory) of significant cash sums singly or in accumulations without a plausible and legitimate explanation;
- where deposits are received from other banks and the bank is aware of a regular consolidation of funds from such accounts prior to a request for onward transmission of funds;
- the customer is reluctant to meet personnel from the bank in person and / or uses a "front person;
- the avoidance by the customer or its representatives of direct contact with the bank (such as the use of night safes to make large cash deposits);
- the use of nominee accounts, trustee accounts or client accounts which appear to be unnecessary for, or inconsistent with, the type of business carried on by the underlying principal;
- the use of numerous accounts for no clear commercial reason where fewer would suffice (so serving to disguise the scale of the total deposits);
- the use by the customer of numerous individuals (particularly persons whose names do not appear on the mandate for the account) to make deposits, the bank must ensure it knows the beneficial owner as per the Code requirements;
- frequent switches of funds between accounts in different names or in different countries or territories;
- substantial withdrawal(s) from a previously dormant or inactive account;
- substantial withdrawal(s) from an account which has just received an unexpected large credit from overseas;
- substantial withdrawal(s) from an account that incurs a significant penalty which would normally be avoided;
- use of bearer instruments outside a recognised dealing system in settlement of an account or otherwise;
- where there appears to be no reasonable explanation to retain an account in a different jurisdiction to that of the customer;
- where a customer declines to provide information which normally would make them eligible for valuable credit or other premium banking services (which benefit the customer); or where they inexplicably avoid normal banking facilities, such as higher interest rate facilities for larger credit balances;
- the customer exhibits unusual concern with the bank's compliance with reporting requirements and/or AML/CFT policies and procedures;
- the customer funds deposits, withdraws or purchases financial / monetary instruments below a threshold amount to avoid certain reporting / record keeping requirements;
- wire transfers / payments are sent to, or originate from, high risk jurisdictions without apparent business reason; and
- the customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship and would therefore usually be suspicious activity. If a relevant person identifies suspicious activity appropriate steps as explained in section 3 of this document, and the Code, must be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information and/or has tried to conceal their identity;
- where it is identified a customer provides suspicious identification documents;
- the customer refuses to provide the bank with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;
- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- the customer enquires about how quickly they can end a business relationship;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;
- the customer is known to have criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

3.3 Other risk factors specific to the banking sector

The following section of the guidance covers some of the other risk factors specifically related to the banking sector. Further guidance surrounding risk assessments is outlined in chapter 2 of the Handbook.

- Loan and mortgage facilities (including the issuing of credit and charge cards) could be used by launderers at the layering or integration stages of the traditional ML process. Secured borrowing can be an effective method of layering and integration because it

puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

- Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the identification and verification procedures of the Code must be complied with.

4. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships. Chapter 3 of the Handbook provide guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. Also, guidance on the timing of identification and verification of identity is provided. Please also see section 3.8 of the Handbook for further details on source of funds and source of wealth. For details of particular concessions which may be applicable please see Chapter 4 of the Handbook.

In all cases where the requirements of Part 4 of the Code cannot be met (Paragraphs 8(5), 9(9), 10(5), 12(11), 14(6), 15(8) and 19(11)) the procedures and controls must be provide that –

(a) the business relationship must proceed no further;
(b) the relevant person must consider terminating[1] the business relationship; and
(c) the relevant person must consider making an internal disclosure.

In instances where the above occurs any decisions must be documented with the rationale for the decision explained, and signed off, in accordance with the bank's processes.

4.1 The formation of a business relationship

Paragraph 8(2) of the Code provides that, the procedures and controls in relation to new business relationships must be undertaken -

8 New business relationships
(a) before a business relationship is entered into; or
(b) during the formation of that relationship.

[1] In relation to a new business relationship (paragraph 8) the business relationship must be terminated.

In respect of a bank it is considered that issuing an account number to a customer (e.g. following receipt of an application form and loading customer details onto the system), whether as a "pending account" or otherwise, would constitute forming a business relationship. However, it is recognised that the relationship may not yet be fully established. Accepting funds into a pending account also constitutes forming a business relationship (even where no withdrawals or transfers can be made) but again it is recognised that the business relationship may not yet be fully established.

4.2 Un-activated accounts

When an application form is received by a bank with no CDD, or unsatisfactory CDD attached (rather than a minor issue with the CDD as explained in section 4.3 of this document) the bank may require that an account number is assigned to the customer in order to process the application. As there is no CDD held on the customer the relationship cannot be fully established. Therefore, the bank must ensure that no funds are allowed in or out of the account (i.e. a "no deposits flag" or similar must be in place) and the account cannot be "active".

The system must be able to physically prevent the straight through deposit of funds to the account. The customer should be made aware that funds will not be accepted or withdrawn until CDD is complete and satisfactory. When the CDD is complete an appropriately experienced member of staff must remove the "no deposits flag" to enable funds to be received into the account (the account may at this point still be blocked for withdrawals if it has not fully been signed off).

If funds are received (electronically or by cheque) the bank must have a process in place to deal with this and the funds must not be deposited into the account. The bank must either delay the application of funds / cashing of the cheque until the account has been signed off, or return the funds / cheque.

4.3 Pending accounts

Pending accounts may be used for operational purposes where there may be a minor issue to address before the account can be fully signed-off. When an account is treated as a "pending account" customer funds may be received into these accounts but no withdrawals should be permitted until the account take-on process is satisfactorily completed and the "pending" status removed.

Examples of the common issues which a bank may face in completing the account sign-off include:

- problems with certification of identity documents;
- missing, insufficient or out-of-date address verification documents; and/or:

- a lack of full information on submitted application forms.

An account would not be able to be treated as a "pending account" if an application form was received with no additional supporting documentation (see section 4.2 of this document). To use a "pending account", the verification of the customer's identity must have been completed (paragraph 8 of the Code only allows the verification of identity to be absent in very exceptional circumstances (paragraph 8(4)). Also, the customer's source of funds and the nature and intended purpose of the relationship must have been established.

5. Ongoing Monitoring

The Code requirements in relation to ongoing monitoring of business relationships are covered by paragraph 13 of the Code. Section 3.4.6 of the Handbook further explains the ongoing monitoring provisions of the Code.

CDD information in respect of all customers should be reviewed periodically to ensure that it is accurate and up to date. It should also be considered as part of this review whether there are any changes to the customer risk rating. To be most effective, resources should be targeted towards monitoring those relationships presenting a higher risk of ML/FT.

5.1 Frequency of ongoing monitoring – standard risk relationships

The Handbook explains that dates for periodic CDD/ECDD reviews are set on a risk sensitive basis. The depth and breadth of CDD/ECDD to be reviewed and the frequency of such reviews being determined per the risk.

The Authority accepts that in respect of some banks, due to the volume and nature of clients that services are provided to, CDD information on standard risk customers may be reviewed on a trigger event basis.

In order for such a trigger event approach to be acceptable and effective, the triggers themselves need to be suitably robust and comprehensive, with reference to the types of customers and products within the standard risk portfolio. Banks should also consider if a backstop review period should be in place for the review of standard risk customers' CDD information (in the event that triggers do not occur).

For example, appropriate arrangements should be in place to screen the customer database to establish whether any customers may have had a change of status, for example have become PEPs. In addition, consideration should also be given to the adequacy of monitoring systems in place for corporate customers to make sure that companies to which services are provided (and transactions processed) have not been struck off. Further information on screening is included in sections 3.4.6.1, 3.4.6.2 and 3.8.10.1 of the Handbook and section 5.2 of this document.

In addition section 3.3.6 Handbook sets out that changes of CDD information should be verified on a risk basis.

5.2 Customer Screening

Screening of a customer usually falls into two distinct parts:

- Initial screening undertaken as part of CDD checks during the take on of a customer relationship, and
- Screening of the bank's client base as part of ongoing monitoring processes.

Initial CDD screening by banks should be conducted as part of the customer risk assessment required by paragraph 6 of the Code, in order to assist in determining the ML/FT risks associated with the customer. It will often take the form of a search performed on the name of the customer (or connected account party) using public domain and/or internal risk management systems. Banks should ordinarily screen to determine whether the customer or other party has any PEP connections, is subject to any sanctions restrictions, or adverse information/negative press.

In respect of ongoing monitoring, ideally, information on all parties associated to a customer relationship should be uploaded into a searchable database, which would then be automatically screened on a periodic basis (which could be daily) for PEP and sanctions information, and any 'hits' would be investigated to determine whether or not they are appropriate to the customer.

As part of ongoing monitoring, the Authority considers it is also appropriate for banks to screen their client database for negative press / adverse information on a periodic basis, in addition to the checks undertaken during client take-on. The Authority considers that if automatic screening of the bank's database for negative press is not possible or practical, then screening for this should be conducted manually in line with the timeframes set out in section 5.1 above. More frequent monitoring of negative press information for known PEP customers should also be considered.

5.3 Higher risk customers

It is important that the reviews in respect of higher risk customers are conducted on a timely basis, with details of the review being fully documented in order that timeliness, completeness and consistency can be demonstrated. Where such reviews are not conducted within the intended period, it is important any 'backlog' position is reported outside of the team conducting the review, in order that any associated risks can be monitored (i.e. to a risk committee or board).

A review may identify issues that require remediation but which cannot be resolved promptly. Any remediation activity must be time limited and tracked to completion. With reference to this, and depending on the level of concerns arising from outstanding matters, banks should consider whether activity on an account should be restricted pending remediation being completed.

It is recognised that sometimes the remediation of a relationship may be protracted; however, the Authority would not expect remediation issues outstanding from the previous annual review to remain outstanding at the start of the next review unless there were exceptional circumstances, and this course of action was agreed by senior management.

An annual review should be scheduled within a year of the start date of the previous review, not the date the previous review was signed off. Section 5.3.1 below details the minimum information that the Authority would expect to see recorded during an independent review of a higher risk customer.

5.3.1 Customer Reviews – areas to consider

The below is not designed to be a template for completion, however, are the suggested areas a bank should consider and document when conducting such a review.

Account Name			
Account Number(s)			
Connected Accounts			
Date of Review		Previous review	
Relationship Manager			
Reviewer			
Risk rating at start of review			
Reason for risk rating			

Background/nature of customer

Include details of:

- Brief background of customer, occupation, residency etc.
- Number of accounts (and balances)
- Connected parties (where applicable)
- Purpose of account
- Source of funds/wealth
- Any adverse media checks

Additional information for corporate/trust/foundation accounts

- Nature of business
- Key parties to this account – including details of the UBO
- Area of trade/counterparties
- Any connected accounts (e.g. same UBO)
- Structure (including ownership, control and rationale)
- Any adverse media checks

CDD review

Commentary on CDD and EDD held (including that for connected parties where appropriate), including confirmation that the CDD and EDD remains up to date and appropriate. Any concessions used – e.g. eligible introducer

Activity review

Commentary on the actual/anticipated activity through the account (s) (payments/turnover/currencies/counterparties) and comparison to expectations, given knowledge of customer and expected nature of business/source of funds/source of wealth.

Transaction review

Brief commentary on turnover through account within the last 12 months and whether the value and volume of these transactions is in line with expectations given knowledge of customer and expected nature of business/source of funds/source of wealth.

Ensure appropriate action is taken in relation to the occurrence of any unusual or suspicious activity – see section 3.1 of this document for further details.

Other information

Any additional searches undertaken as part of this review e.g. sanctions, PEPs, internal databases, adverse media, online searches etc.

Note: Where screening of certain information (e.g. for sanctions and PEPs) is conducted automatically (e.g. daily or weekly) then additional manual screening is not necessarily required at annual review.

Any other relevant information e.g. changes expected within the next 12 months.

Customer risk assessment

Details of considerations of the customer risk and any appropriate changes. Include any new risks identified and any actions to address these risks, e.g. obtaining additional EDD, consideration as to whether the relationship is still within the bank's risk appetite, SAR submission, increasing the frequency of reviews, undertaking enhanced transaction monitoring, restricting activity etc.

Actions to be taken

Detail the proposed course of actions to be taken, how this will be documented and the timescales in which this action will be completed.

Reviewer confirmations

The reviewer should be confirming that: • A full independent review has been undertaken of the above customer; • The information stated is accurate, up to date and complete; • The risk rating remains appropriate (or stated otherwise – including rationale if rating has been revised); • Any causes for concern have been addressed and any suspicions have been appropriately reported.			
Date review complete		Next review diarised	
Bank's sign off /approval process			

6 Case Studies

The case studies below are real life examples of risks that have crystallised causing losses and/or sanctions (civil and criminal) against banks. The majority of these examples are from case studies provided by FIUs of other jurisdictions, namely FINTRAC (Canada) and AUSTRAC (Australia).

6.1 Fraud related money laundering

FINTRAC received one suspicious transaction report ("STR") from a bank, which generated a case involving ten individuals and twelve businesses, located in the greater Toronto area, suspected of possible fraudulent and money laundering activities. An additional 22 STRs, provided by the same bank and two others, as well as one money transmission business, further contributed to this case.

FINTRAC's analysis revealed that most businesses in this case appeared to be involved in the employment service industry and the associated individuals/officers conducted multiple cash deposits. Employees of the businesses were also paid in cash. These transactions were found to be unusual since the employment service industry is not typically cash driven.

The businesses were linked through common directors/officers, financial transactions, and shared addresses/phone numbers. The individuals involved were also linked through similar addresses and joint signing authorities for various bank accounts.

One individual was the subject of a previous disclosure to law enforcement regarding fraud/extortion activities and was suspected to have links to Eastern European organized crime.

Higher risk indicators associated with this case:

- Individuals made cash deposits (in $100 and $50 denominations) into the personal accounts of multiple associates who then issued cheques payable to other individuals (i.e. use of pass through accounts).
- Numerous businesses paid their employees in cash and reporting entities indicated in the STR that this was not consistent with typical business operations.
- Cheques were deposited into business accounts then immediately withdrawn in cash or through the issuance of cheques payable "to cash" or payable to the individual making the initial deposit.
- Reporting entities also reported excessive cash flow in the business accounts.

The transactions conducted in this case were mostly representative of the placement and layering stages of money laundering. The relevant designated information was disclosed to four different law enforcement agencies.

6.2 Drug related money laundering

FINTRAC received information from law enforcement regarding a number of individuals and businesses, located in the greater Vancouver area, under investigation for suspected involvement in the importation of drugs to Canada from an Asian country.

FINTRAC's analysis revealed financial transactions associated to five of the individuals and three money service businesses that were mentioned in the information provided by law enforcement. FINTRAC suspected that six additional individuals and five businesses specializing in telecommunications, construction, foreign exchange and interior renovation were also involved in the scheme.

Thirty-five STRs reported to FINTRAC by multiple branches of four different banks and three different credit unions were instrumental in allowing FINTRAC to find connections between the various players in this scheme, as well as identifying ones that may not have been previously known to law enforcement.

Higher risk indicators associated with this case:

- Large cash deposits (in CAD and USD) into personal accounts were sometimes followed by the purchase of bank drafts payable to trust companies or money services/currency exchange businesses.
- Domestic wire transfers between personal accounts were followed by the purchase of bank drafts payable to trust companies.
- Bank drafts and cheques issued from other financial institutions were deposited into personal and business accounts and were sometimes followed by an electronic transfer to a Middle Eastern country.
- Electronic transfers were also received from the same Middle Eastern country.
- Multiple transactions were carried out on the same day at the same branch but with different tellers, hours apart.
- Some cash deposits were structured to keep amounts under the reporting threshold and/or conducted at different branches.
- Cash, cheques and bank drafts were deposited by third parties into the business accounts of money service businesses and domestic wires were received into the same accounts; they were immediately followed by withdrawals to purchase bank drafts payable to other money service businesses which then sent electronic transfers to various beneficiaries in foreign countries.
- The same money service businesses receiving deposits or wires also directly sent electronic transfers to beneficiaries in foreign countries.

Individuals and entities involved in this case appear to have conducted a number of suspicious activities mostly representative of the placement and layering stages of money laundering in addition to furthering their drug trafficking activities. FINTRAC disclosed all relevant designated information to law enforcement to assist them in their investigation.

6.3 Terrorist financing

FINTRAC received information from law enforcement and intelligence agencies regarding a non-profit organisation ("NPO"), located in the greater Toronto area, which was suspected of acting as a front for a terrorist organisation. The NPO and associated individuals were suspected of facilitating the acquisition and aggregation of financial resources in Canada, as well as the transmission of resources ultimately for the benefit of the terrorist organization's operations overseas.

The NPO was the subject of several FINTRAC disclosures to law enforcement and intelligence agencies between 2002 and 2007. STRs, from financial institutions were instrumental in assisting FINTRAC in its analysis.

Higher risk indicators associated with this case:

- The NPO ordered many electronic transfers to the benefit of individuals and entities (including a foreign NPO also suspected of being a front for the terrorist organization) located overseas. The transfers were ordered primarily through major financial institutions rather than through domestic money service businesses.
- Various officers of the NPO made large cash deposits to the various accounts of the suspect NPO, held at multiple financial institutions, for which the source of funds was unknown.
- An individual also attempted to deposit a number of cheques, made payable to third parties, to the account of the suspect NPO
- Multiple, recurrent electronic credits were made to the accounts of the suspect NPO for which the original source of funds and remitters' identity were unknown.
- The deposit of cash and monetary instruments (cheques, bank drafts etc.) to the account of the suspect NPO, were often followed by the purchase of bank drafts or offshore movement of funds FINTRAC disclosed all relevant designated information to law enforcement and intelligence agencies to assist them in their investigation.

ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Money Transmission Services

Bureau de change
Cheque cashing
Payment services as agent

Sector Specific AML/CFT Guidance Notes

August 2021

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

Version history

Version 2 (August 2021)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes 3.3.1 minor amends in respect of a simplified risk assessment explaining this could be undertaken on a risk based approach

1. Foreword

This sector guidance is applicable to businesses conducting money transmission services ("MTS"), in particular the following activities under Class 8 of the Regulated Activities Order 2011 (as amended) ("RAO"):

- Class 8(1) – Operation of a bureau de change
- Class 8(2)(b) – Provision and execution of payment services as agent
- Class 8(3) – Provision of cheque cashing services

For the full definitions and scope of these activities refer to the RAO.

Please note there is separate sector specific guidance for the remaining areas of Class 8 (provision of payment services as principal and e-money activities).

2. Introduction

The purpose of this document is to provide guidance specifically for the MTS sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across, or between, sectors.

This document is also based on the FATF document Money Laundering through Money Remittance and Currency Exchange Providers (June 2010). The Authority recommends that relevant persons familiarise themselves with this document and other typology reports concerning the MTS sector. Also, some case studies are included to provide context to the risks of the sector.

2.1 National Risk Assessment

The Island's National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. The MTS sector must ensure their business risk assessment (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

In relation to the main vulnerability of the sector, there is a risk that services could be used to move funds generated from crime quickly round the financial system including through different jurisdictions. To combat this, firms need a good understanding of ML/FT relevant to bureau de change and agency operations. The NRA sets out the main risks and vulnerabilities in detail.

The level of risk for both ML and FT is considered to be medium low based on the general low value and transactional activity conducted, the predominant nature of the customer base (local residents, face to face) and the level of controls and oversight arrangements in place for a sector of this small size. It is recognized that agency business poses some additional risk for both low level ML and potentially FT, as low value funds flow in and out of the IOM.

3. Risk Guidance

The MTS industry is a broad sector covering a range of businesses and products. The ML/FT risks vary for each business based on a wide range of factors such as the type of services they supply, their customers and delivery channels.

There are a number of different business types in this sector, therefore this document covers some of the general risk factors common to the sector as a whole, and then focusses on particular individual business types where necessary.

Vigilance should govern all aspects of the business' dealings with its customers, including:

- establishment of the business relationship or conducting of an occasional transaction;
- being aware of the different features each product can have;
- any linked transactions;
- ongoing monitoring of the business relationship; and
- technology / security issues if there is an online element to the business relationship or transaction.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, certain activities may increase the risk of the relationship or transaction. Just because an activity / scenario is listed below, it does not automatically make the relationship or occasional transaction high risk; the customer's rationale / nature / purpose of the business relationship or occasional transaction etc. should be considered.

If an MTS business is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concern, it should be determined whether this is suspicious or unusual activity. Please refer to chapter 5 the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 (Ongoing monitoring) of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;
(b) conduct EDD in accordance with paragraph 15; and
(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and
(b) make an internal disclosure.

The below list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. A list of red flags is included at section 3.2 and more specific risk guidance is provided later in this section.

- Where a customer is reluctant to provide normal information or provides only minimal information.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the MTS business with complete information about the nature and purpose of the relationship including anticipated relationship activity.
- The customer is located in a higher risk jurisdiction.
- Transactions involving numerous jurisdictions.
- Transactions associated with high fees and a lack of rationale.
- Unusual / large cash transactions without rationale / legitimate explanation.
- The customer is reluctant to meet personnel from the firm in person and / or uses a "front person".
- The customer engages in frequent transactions with different MTS businesses.
- The use of different MTS businesses in jurisdictions that do not have robust AML/CFT laws.
- The customer requests information about limits of transactions and any relevant thresholds.

- The customer appears to undertake transactions below a threshold amount to avoid certain reporting / record keeping requirements.
- The customer has no discernible reason for using the business' services, or the business' location.
- The customer has a history of changing providers and using a number of businesses in different jurisdictions.
- The customer's address is associated with multiple accounts that do not appear to be related.
- The customer is known to be experiencing extreme financial difficulties.
- The nature of activity does not seem in line with the customer's usual pattern of activity.
- The customer asks about how to close accounts without explaining their reasons fully.
- The customer opens an account / product without any regards to loss, commissions or other costs associated with that account / product.
- The customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities, or inconsistent with the customer's profile.
- The customer exhibits unusual concern with the business' compliance with Government reporting requirements and AML/CFT policies and procedures.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship or occasional transaction and would therefore usually be suspicious activity (as defined in the Code). Appropriate steps as explained in section 3 of this document, and the Code, must therefore be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- the customer does not provide relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- it is identified the customer has undertaken a number of linked transactions and is operating under set threshold amounts;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;
- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for; and

- the customer is known to have criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons.

3.3 Risk factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to sub-sets of this particular sector. Further guidance surrounding the risk assessments is outlined in chapter 2 of the Handbook.

Several features of the MTS sector can make MTS providers/products an attractive vehicle through which criminal and terrorist funds can enter the financial system, such as:

- the simplicity and certainty of transactions;
- criminal proceeds can be easily "cashed out" and placed in different payment systems or products;
- worldwide reach particularly with the internet being "borderless";
- cash character of transactions;
- the potential for linked transactions to take place – particularly in relation to bureau de change;
- less stringent CDD requirements (i.e. exempted occasional transactions as set out in section 5.1 of this document); and
- increased potential for anonymity (depending on the product).

A number of risk assessments must be carried out by sectors as set out in the Code, including:

- business risk assessments (paragraph 5);
- customer risk assessments (paragraph 6); and
- technology risk assessments (paragraph 7).

3.3.1 Customer risk assessment – occasional transactions

Paragraph 6(2)(b) of the Code requires that a customer risk assessment is recorded in order to demonstrate its basis. It is understood that the majority of occasional transactions undertaken by a customer (prevalent in bureau de change and payment services as agent) are likely to pose a standard (or lower) risk of ML/FT, but it is essential that a staff member confirms this risk rating, and has the ability to determine that a transaction poses a higher risk of ML/FT.

In respect of MTS businesses a risk based approach may be taken resulting in a "simplified" customer risk assessment being carried out for occasional transactions under €15,000 or currency equivalent, as long as the customer does not pose a higher risk and suspicious activity has not been identified.

A simplified customer risk assessment should record that the staff member has made a determination of the ML/FT risks posed by the customer and state the risk rating they have selected. The rationale behind the decision of which risk rating to select need not be documented if it is determined the customer poses a low or standard risk. If it is determined the customer poses a higher risk, a full customer risk assessment must be undertaken and documented as required by the Code. Also, enhanced due diligence must be undertaken in line with paragraph 15 of the Code.

Where an MTS business decides to use a simplified customer risk assessment the rationale for doing so and the considerations given to the content of the template, standard wording etc. should be detailed in their business risk assessment.

Adequate training on how to identify higher risk factors, how to carry out a simplified customer risk assessment and what actions to take for higher risk customers should be provided to all relevant staff. There should be clear procedures for staff in relation to this.

3.3.2 Technology risk assessment

Considering the technology risk assessment specifically, this must estimate the risk of ML/FT posed by any technology developments, such as the use of online delivery channels to its business which can be a prevalent feature of this sector. An assessment should be undertaken at the outset of the business and whenever a relevant system is introduced or changed. Further information about the technology risk assessment can be found in section 2.2.11 of the Handbook.

3.4 Bureau de Change

Please note that the risk factors detailed in this section are product/service specific and should be considered in conjunction with the more generic MTS business risks and customer risks detailed in previous sections of this sector specific guidance document. The provision of currency and the ability to convert currencies is the main area of risk associated with bureau de change activities.

Most customers, both personal and business, will have a legitimate need to convert currency. The risk is, however, failing to identify customers or situations where the level of foreign exchange activity is higher than one would expect; or is unusual or inconsistent in some other way. In such circumstances there is justification for looking more closely at whether the customer may be involved in ML/FT.

3.4.1 Risk guidance

- Use of cash: cash is the mainstay of much organised criminal activity. For the criminal, it has the obvious advantage of leaving no discernible audit trail and is their most reliable and flexible method of payment. Cash, however, is also a weakness for

criminals as they are more at risk of being traced to the original offence which generated the cash in the first place. The objective of the first stage of ML (placement) is to move the criminal cash into the financial system. They will therefore often seek to exchange cash in one currency for foreign currency (or vice versa). This may involve exchanging small denominations of one currency for larger denominations of another currency. This is considered to be the most difficult and risky part of the ML cycle for criminals.

- Audit trail: the product is easily transported across jurisdictions and can be transferred to another person without leaving an audit trail.
- Buy backs and refunds: amounts of foreign currency may be presented by launderers for exchange into sterling in cash, draft, travellers' cheques or other instrument. This could be either an attempt at placement or part of the layering process.
- Swaps through a third currency: amounts of currency could be presented for exchange into a third currency, possibly from small denominations into easily transported large notes. This would be part of the layering process.
- High risk sectors: some money launderers will be proprietors of cash-based businesses such as restaurants, pubs, casinos, taxi firms, etc. The aim here is to mix "dirty" money with "clean", and so muddy the trail.

3.4.2 Nature and intended purpose of transaction / business relationship

It is recognised that the nature and intended purpose of the majority of transactions will be individuals requiring foreign currency for the purpose of business or leisure travel (or buybacks) and that it is sufficient to simply understand and document the purpose of the customer's request. This can, for example, be based on a brief conversation or knowledge of the customer.

Relevant persons should however seek (and document) further information from customers where any adverse or unusual factors (such as those described in this section of guidance) may be prevalent, or where the currency requested is unusual.

It is recommended that for business relationships or larger occasional transactions (for example those over £3,000 or equivalent), especially in cash, the relevant person should formally obtain and document the nature and intended purpose of the business relationship/transaction.

3.5 Payment services as agent

Please note that the risk factors detailed in this section are product/service specific and should be considered in conjunction with the more generic MTS business risks and customer risks detailed in previous sections of this sector specific guidance document.

3.5.1 Risk Guidance

- A commonly reported ML/FT method involves the use of a third party to transfer funds. Transactions carried out by the customer using (without a reasonable basis) multiple branches or agencies and third parties (such as relatives, minors) on behalf of another person are often aimed at concealing the sender and / or the receiver (true beneficiary of the transaction).
- Structuring or "smurfing" is considered to be the most common method for ML through payment services. Structuring occurs when a person carries out several cash transactions by breaking them into smaller amounts in order to avoid mandatory reporting requirements or CDD requirements. Such transactions become more difficult to detect when multiple agents are used or where a third party is used to carry out the transaction.
- A common beneficiary or type of beneficiary (e.g. trading company in country X) could indicate an organised criminal group including (particularly when connected to a higher risk country) terrorist groups.

3.5.2 Payment agents - Nature and intended purpose of transaction / business relationship

It is recognised that the purpose and nature of the majority of transactions will be for individuals wishing to transfer money abroad to relatives, and that it is sufficient to simply understand the purpose of the customer's request (for example based on a brief conversation or knowledge of the customer). In this respect, understanding the destination of the remitted funds is important. Relevant persons should however seek (and document) further information from customers where any adverse or unusual factors (such as those described this guidance) may be prevalent, or where the principal's procedures require it.

It is recommended that for larger transactions (for example those over £3,000 or currency equivalent), especially in cash, the relevant person should formally obtain and document the nature and intended purpose of the business relationship/transaction.

3.5.3 Payment agents – Monitoring transactions

Monitoring for linked transactions is primarily the responsibility of the principal. However, the agent can assist in identifying any unusual or suspicious transactions, which may include the use of linked transactions. In this respect the focus should be on transactions, rather than a customer's identity, having consideration to the value, frequency and destination of transfers. Agents should work with principals as appropriate to help prevent customers transferring funds that may relate to scams.

3.6 Cheque cashing

Please note that the risk factors detailed in this section are product/service specific and should be considered in conjunction with the more generic MTS business risks and customer risks detailed in previous sections of this sector specific guidance document.

Third-party cheque cashers are not normally exposed to large scale ML from the most serious crimes, such as drug trafficking and robbery, because the flow of cash goes in the opposite direction to that required by most money launderers, who need to convert their cash proceeds of crime. However, cheque cashers must identify and mitigate the risks of their service being used for other offences such as tax evasion.

3.6.1 Risk guidance

- Fictitious companies may be set up for the purposes of cheque fraud. Look out for low and consecutive cheque numbers.
- A number of different people cashing cheques all of which are drawn on the same company, with an unfamiliar company name.
- People wanting to cash their final salary cheque, in the knowledge that it may not be the final amount they are entitled to. Final salary cheques are more likely to be stopped or re-issued with a lower amount than the original cheque due to deductions for monies for holiday/sickness etc.
- Fraudulently obtained cheques where a person has a number of cheques drawn on different individuals rather than a company, claiming to have done work for these people.
- A sudden increase in the value of cheques being cashed.
- A customer wanting to cash a cheque which was made payable to them weeks earlier. Usually cheque-cashing customers using a third party cheque-cashing service need the cash quickly and therefore an old cheque date could mean that the cheque has been stolen or tampered with. The customer could have informed the drawer that the cheque is lost, a replacement may have been provided and cashed elsewhere, and the customer then tries to cash the original cancelled cheque.
- Post containing a recently issued chequebook may have been intercepted by a fraudster who then creates ID to replicate the original payee's ID.
- It appears that there has been something added to the cheque after the time of issue, for example different handwriting is evident, value digits appear squeezed in.

The most common risk to the cheque casher is that of deception by the customer. Cheques can be stolen, stopped, forged, or altered in many ways. Examples include, but are not limited to those listed below.

- Use of companies: a signatory for a company cheque book may make cheques payable to an accomplice and then give approval to the cheque encashment company on a phone call checking entitlement. A further example is where the customer is a director of the company on which the cheque is drawn; the company could be in financial difficulty and the customer is trying to draw funds on the account knowing there is no money available.
- Advance fee fraud: for example where a customer receives a letter advising they have won the lottery in another country. A cheque is sent which is meant to cover taxes for the payment, sometimes along with the supposed winnings. The letter suggests the winner cashes the cheque and then sends the money for taxes via another means. The customer is unaware that this is a scam, and the cheque is usually stolen.
- Tax evasion: a customer may use a cheque cashing service to conceal income from a tax authority, thereby evading tax. A third-party cheque encashment service may reasonably assume its customers pay tax, unless there is some reason to suspect otherwise.
- Benefit fraud: a customer might use a cheque cashing service to conceal income from their own bank accounts thereby appearing to remain below means tested thresholds for certain social security benefits.

3.6.2 Cashing a cheque on behalf of someone else

Paragraph 12(2)(b) of the Code requires that:

> **12 Beneficial ownership and control**
> (2) The relevant person must, in the case of any customer –
> (b) subject to paragraphs 17 and 21, determine whether the customer is acting on behalf of another person and, if so –
> (i) identify that other person; and
> (ii) take reasonable measures to verify the identity of that person using reliable, independent source documents, data or information.

In order to comply with the Code and for commercial reasons (primarily fraud risk), customers wishing to use third-party cheque cashing services should prove their identity before a transaction can be processed**.** Cheque cashers should make the assumption that every new customer could become a regular customer (and establish a business relationship), rather than treating each separate transaction as an occasional transaction.

The customer should provide proof of entitlement to the cheque being cashed. This can be provided on paper or details can be given verbally which enable the cheque casher to seek confirmation from the drawer. Identity ("ID") fraud is prevalent; therefore when checking ID, the cheque casher must be vigilant and aware that any piece of ID could be forged. The

majority of cheques handled are expected to be salary cheques, and such customers should have a salary slip to accompany a cheque.

For small businesses, where the cheque is made payable to their business, the cheque-casher should require the normal proof of ID of the individual cashing the cheque plus evidence of their "trading as.." name, examples include a letter from their bank, a tax return, registered business name certificate or VAT return. Sole traders who have cheques made payable to their business should also complete a declaration to state that they are the sole trader and sole signatory to the account and therefore wholly entitled to the cheque. For partnerships, proof of ID must be produced for all partners.

In respect of limited companies, cheques made payable to a limited company should be presented through the bank account of that company. However, where cheque-cashers accept cheques on a regular basis that are made payable to a limited company they should ensure that they assess the risks involved and establish whether there are valid reasons for cashing a cheque made payable to a limited company.

For cheque-cashers the source of funds is the party that has issued the cheque (the drawer). Drawers of cheques whose name is unfamiliar to a cheque-casher should be investigated thoroughly. For companies, business name, address and phone number can be verified by electronic means. Further searches into the list of directors may establish that the customer is not connected to the company on which the cheque is drawn, and may alert the cheque-casher as to a drawer's negative credit status.

3.6.3 Nature and intended purpose of transaction / business relationship

It is recognised that a high proportion of transactions/business relationships will be for individuals who need to receive cash quickly relating to regular payments such as a salary cheque or Government issued cheques, or for some reason do not have a bank account into which they can deposit the cheque. However, with banks now utilising cheque imaging and cheque clearing times reducing, the reasons for persons with bank accounts requiring cheque cashing services should decline.

Cheque cashers should seek (and document) further information from customers where required and ensure they are comfortable the activity fits the customer profile, and the expected activity of that customer.

3.6.4 Transaction monitoring

Cheque cashers must have systems in place that enable them to review a customer's cumulative value of cheques cashed. These checks should be made on milestone amounts, for example £10,000 and increments of £10,000 thereafter. This review should include consideration of how often cheques are cashed, whether drawers are common or frequently change, and whether the frequency and value of the cheques match the customer's explanation for their encashment.

Cheques should also follow a pattern and should generally be of similar amounts. Anything that deviates from a customer's normal pattern of business should be queried and, if suspicion is aroused, reported in line with the requirements of the Code as detailed in chapter 5 of the Handbook.

4. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships.

Chapter 3 of the Handbook provides guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. Also, guidance on the timing of identification and verification of identity is provided.

For details of particular concessions which may be applicable see chapter 4 of the Handbook and section 5 of this document.

In all cases where the requirements of Part 4 of the Code cannot be met (paragraphs 8(5), 9(9), 10(5), 11(7), 12(11), 14(6), 15(8) and 19(11)) the procedures and controls must provide that –

(a) the business relationship or occasional transaction must proceed no further;
(b) the relevant person must consider terminating[1] the business relationship; and
(c) the relevant person must consider making an internal disclosure.

4.1 Source of funds

For all business relationships and occasional transactions (whether exempted occasional transactions or not), paragraphs 8 and 11 of the Code require that a relevant person must take reasonable measures to establish the source of funds. It is stated that the procedures and controls to be undertaken are:

[1] In relation to a new business relationship (paragraph 8) the business relationship must be terminated.

taking reasonable measures to establish the source of funds, including where the funds are received from an account not in the name of the customer —

(i) understanding and recording the reasons for this;

(ii) identifying the account holder and on the basis of materiality and risk of ML/FT taking reasonable measures to verify the identity of the account holder using reliable, independent source documents, data or information; and

(iii) if the account holder is assessed as posing a higher risk of ML/FT, satisfying the requirements in paragraph 15.

Where the transaction is funded by an instrument drawn on the customer's own account at a regulated financial institution, for example a bank debit card, the MTS provider can reasonably be considered to have taken reasonable measures to have established the source of funds, if no higher risk indicators are present. However, where there is a third party involved in the funding of the account or transaction the reasons for this must be understood, and this person must be identified and reasonable measures taken to verify this person as mandated by the Code.

Please also see section 3.8 of the Handbook for further details on source of funds and source of wealth.

MTS entities must also ensure they seek (and record) further information from customers where any adverse or unusual factors (such as those described under high risk factors above) may be prevalent, especially where the source of funds is cash.

4.2 Ongoing monitoring of linked transactions

It is important that relevant persons should put in place a process to detect and monitor repeat or linked transactions:

- that indicate that an occasional transaction relationship has evolved into a business relationship (and any exempted occasional transaction concession would then be dis-applied); and/or
- by customers who may be attempting to split large transactions into several smaller, less conspicuous amounts, which could indicate 'smurfing'.

It is deemed good practice to monitor for repeat business over the preceding three months from the date of the most recent transactions, using risk indicators and profiles that are appropriate to the business.

5. Simplified customer due diligence measures

The following sets out further detail regarding concessions that may be applicable to the sector.

5.1 Exempted occasional transactions

Paragraph 11(5) of the Code provides a concession whereby the verification of identity is not required for customers carrying out an "exempted occasional transaction".

An exempted occasional transaction is defined in the Code as follows:

> **3 Interpretation**
>
> (1) In this Code -
>
> **"exempted occasional transaction"** means an occasional transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction or, the aggregate in the case of a series of linked transactions, is less in value than —
>
> (a) €5,000 in relation to an activity being undertaken which is included in Class 8(1) (bureau de change) and Class 8(3) (cheque encashment) of the Regulated Activities Order;
>
> (b) €1,000 in relation to an activity being undertaken which is included in Class 8(4) (e-money) and paragraph 2(6)(r) (convertible virtual currency) of Schedule 4 to the Proceeds of Crime Act 2008; or
>
> (c) €15,000 in any other case[2];

If the conditions are met and this concession is utilised, the verification of customer's identity is not required. However all other Code requirements such as paragraph 6, 13, 14 and 15 continue to apply.

Typically, MTS transactions are small in value and high in volume. Often transactions will fall below the exempted occasional transaction threshold and to comply in full with the above listed paragraphs in accordance with the relevant guidance in the Handbook could prove overly burdensome and unmanageable in a busy retail outlet. Therefore, in relation to exempted occasional transactions, the Authority considers it acceptable for the relevant person to:

[2] Class 8(2) payment services would currently fall into this category of €15,000, however it is proposed at the time of the next legislative update an amendment will be made to ensure that any activities being conducted falling within Class 8(2) of the Regulated Activities Order (Payment services) may only be classed as an "exempted occasional transaction" if they are less in value than €1,000.

- complete a simplified customer risk assessment (as per section 3.3.1 of this guidance), and;
- collect a reduced amount of identification information (lower or standard risk only)[3];

If a customer is assessed as higher risk the enhanced due diligence requirements as set out in the Code will apply and must be undertake by the relevant person.

Also, for exempted occasional transactions that pose a lower or standard risk of ML/FT, relevant persons may accept a reduced amount of identification for natural persons. Further information about exempted occasional transactions can be found in section 4.1 of the Handbook.

6. Case Studies

The case studies below are real life examples of risks that have crystallised, causing losses and / or sanctions (civil and criminal) against the sector. These examples are based on relevant FATF papers in relation to these sectors.

6.1 Payment services: Use of false identities

Persons A and B repeatedly sent cash deposits via money remittance to South America to the same recipients. After a few months the money remitted amounted to several thousand EUR. There was no economic background for the transactions performed. None of the individuals resided at the stated address. The remittance forms revealed that most of the money was initially sent by A, after which B took over the transactions with the same beneficiaries. When the identification papers of the two individuals were compared, it turned out that A and B were in fact one and the same person. Police sources revealed that A's identity featured in an investigation regarding human trafficking and exploitation of prostitution.

This example indicates the importance of:

- obtaining the nature and intended purpose of a transaction or business relationship;
- verifying a customer's address;
- carefully checking identity documents;
- considering the ML/FT risks of a recipient country; and
- monitoring transactions for unusual activity.

6.2 Bureau de change: Unusual jurisdictions

The Romanian Financial Intelligence Unit received a suspicious activity report sent by a bank regarding some suspicious cross-border transfers. Thus, three Romanian citizens (X, Y, Z)

[3] Full name, date of birth and residential address should be obtained as a minimum in these circumstances.

received small amounts from company LTD (established in country A), justified as 'salaries'. After receiving money, X, Y and Z used several schemes to launder money, some of which included bureau de change to change the currency.

For example, on the same day when Mr X received a large bank transfer from Mr M, he withdrew the amount of 20,000 EUR in cash, went to a bureau de change and changed Euros to US Dollars. On the same day he visited the bank used for receiving money once more and opened a bank account where he deposited 50,000 EUR.

Mr Y withdrew the money received and opened bank accounts in smaller amounts in several other banks, bureaux de change were used to change the currency.

Mr Z changed 60,000 EUR in the Bank's exchange house (whereas X and Y used private bureaux de change) and used it to buy cars.

A request for information was sent by the Romanian Financial Intelligence Unit to the Financial Intelligence Unit of country A. The answer revealed that company LTD was involved in funds transfers in Eastern Europe, the proceeds originated from drugs and weapons trafficking. The originator of the cross-border transfers to X, Y and Z was a Romanian citizen, Mr M, the person leading the company LTD, known as the leader of a criminal group involved in drug trafficking and skimming.

It was also detected that Mr M used forged identity documents in order to transfer money to Romania. It was also detected that X, Y and Z travelled to country A occasionally, but none of them worked or obtained any legal income there and were unable to explain the large amounts of money that were transferred to their accounts.

This example indicates the importance of:

- obtaining information regarding a customer's source of funds and where appropriate, seeking verification of that information;
- challenging unusual explanations provided by a customer such as the source of funds being salary originating from a different country;
- understanding the rationale for large cash transactions; and
- monitoring transactions for unusual activity such as frequent cross-border transfers.

6.3 Payment services: Remittances to higher risk jurisdictions

A Financial Intelligence Unit received several suspicious activity reports from a postal bank regarding money remittances sent through a well-known money transmitter. The money remittances were sent by a number of entities with no apparent relation between them, from country A to several countries in South America.

Analysis of the information revealed that a number of the transfers sent abroad were made in small amounts. Transfers were made from different branches of the postal bank all located in the same geographical region in country A to various beneficiaries located in several countries in South America. These countries were considered high risk countries with regard to the manufacturing of drugs. The entities that made money remittances had no criminal or intelligence record and were usually young people with low reported income and no property. Therefore, suspicions were raised that they were straw men. A connection was found between one of the persons involved and a large criminal organisation known to be operating in drug trafficking. A co-operation exercise with one of the South American Financial Intelligence Units revealed that one of the beneficiaries was in jail for drug trafficking.

This example indicates the importance of:

- obtaining the nature and intended purpose of a transaction or business relationship;
- considering the ML/FT risks of a recipient country and
- monitoring actual activity against that which is expected for a particular customer.

6.4 Payment services: Fraud

Telemarketing sales persons defrauded victims mainly among older population, by posing as various officials. The victims were told that they had won the lottery and that they had to pay a certain sum as a handling fee before they could collect their winnings. These sums varied between 10,000 USD and 80,000 USD and were paid, among other ways, by bank cheques, or via Western Unions' postal service to fictitious beneficiaries. The cheques were apparently transferred to a professional money launderer who transferred them to money remittance/currency exchange service providers in country A and territory B. The cheques were deposited in the money remittance/currency exchange service provider's own bank accounts. The cheques were then sent to be cleared against the foreign banks from which they were drawn, at which time their source was revealed

This particular example is one of many types of scams that can abuse MTS businesses. Other common examples include:

- False employers offering jobs where the applicant is to receive money from their "employer" and is then asked to transfer the amount less their "salary" to a third party.
- Emails purporting to come from law firms of a recently deceased "family" member requesting an up-front fee in order to release an 'inheritance payment'.

In many cases, it is likely that the customer is the victim of the fraud. In such cases, the relevant person should ask the customer for a detailed explanation of the rationale for making such a transaction and should make the customer aware of the risks associated with making such a transaction.

6.5 Payment services: Cash structuring

Several Bulgarian individuals and companies sent/received a large number of remittances to/from different persons and destinations (often in a number of foreign countries) during a short period of time. They then temporarily stopped their activities for a while and after a short period of time, the transfers started again.

In this scheme large amounts were fragmented into smaller amounts, sent to a great number of persons who were the beneficiaries of the transfers ordered by them. The total sum of received and sent remittances was almost equal and the persons requesting the remittances declared they knew the persons who were the beneficiaries of the transfers ordered by them. Transfers were made in several currencies, where the change from one currency to another was performed between the transfers without any reasonable explanation. The investigation detected that many of the foreign persons involved in the scheme had a criminal background or had been convicted for drug trafficking, prostitution, etc.

This example indicates the importance of:

- monitoring transactions for unusual values, volumes or patterns;
- obtaining the nature and intended purpose of a transaction or business relationship; and
- conducting public domain searches for negative press relating to a customer or associated parties, particularly in relation to an unusual activity.

6.6 Payment services and Bureau de change: Business ownership

Several Bulgarian citizens and companies where the citizens were beneficial owners were involved in a large money laundering scheme. The companies received transfers to their bank accounts in different Bulgarian banks and transferred the money to foreign company A. The ultimate beneficiary of all money transfers was company B, one of the Bulgarian companies.

The investigation carried out by the Financial Intelligence Unit detected that a group of Bulgarians bought up sub-agents of money remittance and bureau de change businesses. After a change in ownership, the total number of transfers received multiplied and a great number of transfers were ordered by foreign citizens. Beneficiaries of those transfers were typically Bulgarian citizens and the company B. It was also found out that the ultimate beneficiary of the transactions received by the individuals was company B.

It is suspected that the funds originated from drug trafficking. The scheme was on a significant scale involving dozens of natural and legal persons from Bulgaria and foreign countries. The amount of funds transferred through the money remittance system was several mullions of Euros.

This example indicates the importance of:

- ensuring that there are appropriate entry and monitoring controls in place regarding regulated activities such as MTS including payment services as agent and
- effective AML/CFT oversight of such businesses by the relevant authorities.

6.7 Cheque cashing: Breaching AML requirements and tax evasion

Company X, a multi-branch cheque cashing company in country A, and its owner, Mr Y, pleaded guilty for failing to follow reporting and anti-money laundering requirements for more than $19 million in transactions. Mr Y also pleaded guilty to conspiring to defraud the government of country A by wilfully failing to pay income and payroll taxes.

According to prosecutors, from 2009 through 2011, certain individuals presented to Company X's manager, and other employees, cheques to be cashed at Company X. The government contended that the cheques were written on accounts of shell corporations that appeared to be health care related, but in fact, the corporations did no legitimate business. The shell corporations and their corresponding bank accounts on which the cheques were written were established in the names of foreign nationals, many of whom were no longer in Country A, according to prosecutors.

The government asserted that Company X accepted these cheques and provided cash in excess of $10,000 to the individuals but that Mr Y and others at Company X never obtained any identification documents or information from those individuals. The government alleged that the individuals cashed more than $19 million through Company X during the course of the scheme, and that Mr Y and Company X wilfully failed to maintain an effective anti-money laundering program by cashing these cheques.

Although the values seen in this case are likely to be much higher than those seen within Isle of Man MTS businesses, this example indicates the importance of:

- carrying out CDD procedures in line with the legislative requirements;
- understanding the source of funds; and
- considering the rationale for a transaction and whether the rationale is indicative of a tax offence.

This example indicates the importance of monitoring transactions, particularly large or frequent cash transactions.

ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Money Transmission Services

Payment services as principal

E-money

Sector Specific AML/CFT Guidance Notes

August 2021

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

Version history

Version 2 (August 2021)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes 3.3.1 minor amends in respect of a simplified risk assessment explaining this could be undertaken on a risk based approach

1. Foreword

This sector guidance is applicable to businesses conducting money transmission services ("MTS"), in particular the following activities under Class 8 of the Regulated Activities Order 2011 (as amended) ("RAO"):

- Class 8(2)(a) – Provision and execution of payment services directly
- Class 8(4) – Issue of electronic money (not to be confused with virtual currency which is covered in separate sector guidance).[1]

Please note there is also separate sector specific guidance for the remaining areas of Class 8 (Bureau de change, cheque cashing and payment services as agent).

2. Introduction

The purpose of this document is to provide guidance specifically for the MTS sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across, or between, sectors.

This document is also based on the following FATF documents:

- Money Laundering using New Payment Methods; and
- Guidance for a Risk Based Approach - Prepaid cards, Mobile payments and Internet-Based Payment Services.

The Authority recommends that relevant persons familiarise themselves with these documents and other typology reports concerning the MTS sector. Also, some case studies are included to provide context to the risks of the sector.

[1] For the full definitions of these activities please see the RAO.

2.1 National Risk Assessment

The Island's National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. The MTS sector must ensure their business risk assessment (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

In relation to the main vulnerability of the sector, there is a risk that MTS entities could be used to move funds generated from crime quickly round the financial system, including through different jurisdictions. Also, customers could be accepted by MTS businesses who may not be accepted by banks, therefore customers may be higher risk. The NRA sets out the main risks and vulnerabilities in detail.

Overall, after applying consideration of the control and other preventative measures in place, the payment services and e-money sector is assessed as having a medium level of vulnerability for both ML and FT.

3. Risk Guidance

There has been rapid development and increased functionality of MTS products available on the market, particularly in relation to e-money products. This has created challenges for countries and private sector institutions in ensuring these products are not misused for ML/FT purposes.[2] The MTS industry is a broad sector and the ML/FT risks will vary for each business based on a wide range of factors, such as the type of services and products they supply, their customers and delivery channels.

This document covers some of the general risk factors common to the sector as a whole and then focuses on particular individual business types where necessary.

Vigilance should govern all aspects of the business' dealings with its customers, including:

- establishment of the relationship or conducting of an occasional transaction;
- being aware of the different features each product can have;
- any linked transactions;
- ongoing monitoring of the business relationship; and
- technology / security issues if there is an online element to the business relationship or transaction.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, certain activities may increase the risk of the relationship or transaction. Just because an activity / scenario is listed below, it does not automatically make the relationship or

[2] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

occasional transaction high risk; the customer's rationale / nature / purpose of the business relationship or occasional transaction etc. should be considered.

If an MTS business is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concern, it should be determined whether this is suspicious or unusual activity. Please refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 (Ongoing monitoring) of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;

(b) conduct EDD in accordance with paragraph 15; and

(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and

(b) make an internal disclosure.

The below list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. A list of red flags is included at section 3.2 and more specific risk guidance is provided later in this section.

- Where a customer is reluctant to provide normal information or provides only minimal information.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the MTS business with complete information about the nature and purpose of the relationship including anticipated account activity.
- The customer is located in a higher risk jurisdiction.
- Transactions involving numerous jurisdictions.
- Transactions associated with high fees and a lack of rationale.
- Unusual / large cash transactions without rationale / legitimate explanation.
- The customer is reluctant to meet personnel from the firm in person and / or uses a "front person".
- The customer engages in frequent transactions with different MTS businesses.
- The use of different MTS businesses in jurisdictions that do not have robust AML/CFT laws.

- The customer requests information about limits of transactions and any relevant thresholds.
- The customer appears to undertake transactions below a threshold amount to avoid certain reporting / record keeping requirements.
- The customer has no discernible reason for using the business' services, or the business' location.
- The customer has a history of changing providers and using a number of businesses in different jurisdictions.
- The customer's address is associated with multiple accounts that do not appear to be related.
- The customer is known to be experiencing extreme financial difficulties.
- The nature of activity does not seem in line with the customer's usual pattern of activity.
- The customer asks about how to close accounts without explaining their reasons fully.
- The customer opens an account / product without any regard to loss, commissions or other costs (such as fees) associated with that account / product.
- The customer's transaction pattern suddenly changes in a manner that is inconsistent with their normal activities, or inconsistent with the customer's profile.
- The customer exhibits unusual concern with the business' compliance with Government reporting requirements and/or AML/CFT policies and procedures.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship or occasional transaction and would therefore usually be suspicious activity (as defined by the Code). Appropriate steps as explained in section 3 of this document, and the Code, must therefore be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- the customer does not provide the MTS business with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- it is identified the customer has undertaken a number of linked transactions and is operating under set threshold amounts;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;
- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;

- the customer is known to have criminal / civil / regulatory proceedings against the4m for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

3.3 Risk factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to sub-sets of this particular sector. Further guidance surrounding the risk assessments is outlined in chapter 2 of the Handbook.

Several features of the MTS sector can make MTS providers/products an attractive vehicle through which criminal and terrorist funds can enter the financial system, such as:

- the simplicity and certainty of transactions;
- criminal proceeds can easily be "cashed out" and placed in different payment systems or products;
- worldwide reach particularly with the internet being "borderless";
- the potential for involvement of numerous different entities during a transaction (many of which could be cross-border) which could dilute the CDD responsibilities as each entity may think the other entity has done it;
- cash character of transactions;
- less stringent CDD requirements (i.e. exempted occasional transactions);
- many transactions being undertaken on a non-face-to- face basis; and
- potential for anonymity (depending on the product).

A number of risk assessments must be undertaken as set out in the Code in order to assess the ML/FT risks, including:

- business risk assessments (paragraph 5);
- customer risk assessments (paragraph 6); and
- technology risk assessments (paragraph 7).

3.3.1 Customer risk assessment – occasional transactions

Paragraph 6(2)(b) of the Code requires that a customer risk assessment is recorded in order to demonstrate its basis. It is noted that the MTS sector may be involved in a number of occasional transactions, in respect of occasional transactions a risk based approach to this risk assessment may be taken resulting in a "simplified" customer risk assessment being undertaken for occasional transactions under €15,000 or currency equivalent, as long as the customer does not pose a higher risk and suspicious activity has not been identified.

A simplified customer risk assessment should record that the staff member has made a determination of the ML/FT risks posed by the customer and state the risk rating they have selected. The rationale behind the decision of which risk rating to select need not be documented if it is determined the customer poses a low or standard risk. If it is determined the customer poses a higher risk, a full customer risk assessment must be undertaken and documented in accordance with the Code. Also, enhanced due diligence must be undertaken in line with paragraph 15 of the Code.

Where an MTS business decides to use a simplified customer risk assessment the rationale for doing so and the considerations given to the content of the template, standard wording etc. should be detailed in their business risk assessment. There should be clear procedures for staff in relation to this process.

Adequate training on how to identify higher risk factors, how to carry out a simplified customer risk assessment and what actions to take for higher risk customers should be provided to all relevant staff.

3.3.2 Technology risk assessment

The technology risk assessment must estimate the risk of ML/FT posed by the use of any technology in the provision of services, such as the use of online delivery channels to its business, which can be a prevalent feature of this sector. A risk assessment should be undertaken at the outset of the business and whenever a relevant system is introduced or changed. Further information about the technology risk assessment can be found in section 2.2.11 of the Handbook.

3.4 Risk guidance – payment services as principal

A further risk factor to consider in relation to the provision of payment services as principal is structuring or “smurfing”. This is one of the most common methods for ML through payment services. Structuring occurs when a person carries out several cash transactions by breaking them into smaller amounts in order to avoid mandatory reporting requirements or CDD requirements. Such transactions become more difficult to detect when multiple agents are used or where a third party is used to carry out the transaction. MTS businesses must therefore remain vigilant in this regard.

3.5 Risk guidance – e-money

The following list, which is not exhaustive, includes some factors to consider which can make e-money products higher risk.

- The absence of credit risk for pre-paid services means that service providers may have fewer incentives to obtain full and accurate information about the customer and the nature of the business relationship. Service providers must ensure they are meeting the CDD requirements as set out in the Code.

- Transactions can often be carried out much quicker than through more traditional channels, which can cause complications in relation to ongoing monitoring.
- Many business models involve non-face-to-face relationships and transactions.
- Broad acceptance as payment method – can also permit cross border remittances.
- Products that allow cash withdrawals.
- The products are more portable – pre-paid cards could, for example, be mailed out of the country.
- Many products do not carry details of the card owners and therefore can offer anonymity.
- Products such as pre-paid cards can also be funded by cash, therefore also contributing to the anonymity aspect.
- There are facilities to use certain e-money cards in ATMs, thus providing global access to cash.

4. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships.

Chapter 3 of the Handbook provide guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. Also, guidance on the timing of identification and verification of identity is provided.

For details of particular concessions which may be relevant please see section 5 of this document and chapter 4 of the Handbook.

In all cases where the requirements of Part 4 of the Code cannot be met (paragraphs 8(5), 9(9), 10(5), 11(7), 12(11), 14(6), 15(8) and 19(11)) the procedures and controls must provide that –

(a) the business relationship must proceed no further;
(b) the relevant person must consider terminating[3] the business relationship; and
(c) the relevant person must consider making an internal disclosure.

4.1 Source of funds

For all business relationships and occasional transactions (whether exempted occasional transactions or not), paragraphs 8 and 11 of the Code require that a relevant person must take reasonable measures to establish the source of funds. It is stated that the procedures and controls to be undertaken are:

[3] In relation to a new business relationship (paragraph 8) the business relationship must be terminated.

taking reasonable measures to establish the source of funds, including where the funds are received from an account not in the name of the customer —

(i) understanding and recording the reasons for this;

(ii) identifying the account holder and on the basis of materiality and risk of ML/FT taking reasonable measures to verify the identity of the account holder using reliable, independent source documents, data or information; and

(iii) if the account holder is assessed as posing a higher risk of ML/FT, satisfying the requirements in paragraph 15.

Where the transaction is funded by an instrument drawn on the customer's own account at a regulated financial institution, for example a bank debit card, the MTS provider can reasonably be considered to have taken reasonable measures to have established the source of funds, if no higher risk indicators are present. However, where there is a third party involved in the funding of the account or transaction, the reasons for this must be understood, and this person must be identified and reasonable measures taken to verify this person as mandated by the Code.

Please also see section 3.8 of the Handbook for further details on source of funds and source of wealth.

If an explanation from a customer does not make sense based on what is known about the customer, then further investigation must be undertaken to establish the source of funds per the requirements of the Code.

4.2 Ongoing monitoring of linked transactions

It is important that relevant persons should put in place a process to detect and monitor repeat or linked transactions:

- that indicate whether an occasional transaction relationship has evolved into a business relationship (and any exempted occasional transaction concession would then be dis-applied); and/or
- by customers who may be attempting to split large transactions into several smaller, less conspicuous amounts, which could indicate 'smurfing' as explained in 3.4 of this document.

It is deemed good practice to monitor for repeat business over the preceding three months from the date of the most recent transactions, using risk indicators and profiles that are appropriate to the business.

5. Simplified customer due diligence measures

The following sets out further detail regarding concessions that may be applicable to the sector.

5.1 Exempted occasional transactions

Paragraph 11(5) of the Code provides a concession whereby the verification of identity is not required for customers carrying out an "exempted occasional transaction".

An exempted occasional transaction is defined in the Code as follows:

> **3 Interpretation**
>
> (1) In this Code -
>
> **"exempted occasional transaction"** means an occasional transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction or, the aggregate in the case of a series of linked transactions, is less in value than —
>
> (a) €5,000 in relation to an activity being undertaken which is included in Class 8(1) (bureau de change) and Class 8(3) (cheque encashment) of the Regulated Activities Order;
>
> (b) €1,000 in relation to an activity being undertaken which is included in Class 8(4) (e-money) and paragraph 2(6)(r) (convertible virtual currency) of Schedule 4 to the Proceeds of Crime Act 2008; or
>
> (c) €15,000 in any other case[4];

If the conditions are met and this concession is utilised, the verification of a customer's identity is not required. However, all other Code requirements such as paragraph 6, 13, 14 and 15 continue to apply.

In relation to exempted occasional transactions, the Authority considers it acceptable for the relevant person to:

- complete a simplified customer risk assessment (per section 3.3.1 of this guidance), and;
- collect a reduced amount of identification information (lower or standard risk only)[5];

[4] Class 8(2) payment services would currently fall into this category of €15,000, however it is proposed at the time of the next legislative update an amendment will be made to ensure that any activities being conducted falling within Class 8(2) of the Regulated Activities Order (Payment services) may only be classed as an "exempted occasional transaction" if they are less in value than €1,000.

[5] Full name, date of birth and residential address should be obtained as a minimum in these circumstances.

If a customer is assessed as higher risk the enhanced due diligence requirements as set out in the Code will apply and must be undertaken by the relevant person. Further information about exempted occasional transactions can be found in section 4.1 of the Handbook.

6. Case Studies

The case studies below are real life examples of risks that have crystallised, causing losses and / or sanctions (civil and criminal) against the sector. These examples are based on relevant FATF papers in relation to these sectors.

6.1 Payment services: Remittances to higher risk jurisdictions

A Financial Intelligence Unit received several suspicious activity reports from a postal bank regarding money remittances sent through a well-known money transmitter. The money remittances were sent by a number of entities with no apparent relation between them, from country A to several countries in South America.

Analysis of the information revealed that a number of the transfers sent abroad were made in small amounts. Transfers were made from different branches of the postal bank all located in the same geographical region in country A to various beneficiaries located in several countries in South America. These countries were considered high risk countries with regard to the manufacturing of drugs. The entities that made money remittances had no criminal or intelligence record and were usually young people with low reported income and no property. Therefore, suspicions were raised that they were straw men. A connection was found between one of the persons involved and a large criminal organisation known to be operating in drug trafficking. A co-operation exercise with one of the South American Financial Intelligence Units revealed that one of the beneficiaries was in jail for drug trafficking.

This example indicates the importance of:

- obtaining the nature and intended purpose of a transaction or business relationship;
- considering the ML/FT risks of a recipient country; and
- monitoring actual activity against that which is expected for a particular customer.

6.2 Payment services: Cash structuring

Several Bulgarian individuals and companies sent/received a large number of remittances to/from different persons and destinations (often in a number of foreign countries) during a short period of time. They then temporarily stopped their activities for a while and after a short period of time, the transfers started again.

In this scheme large amounts were fragmented into smaller amounts, sent to a great number of persons who were the beneficiaries of the transfers ordered by them. The total sum of

received and sent remittances was almost equal and the persons requesting the remittances declared they knew the persons who were the beneficiaries of the transfers ordered by them. Transfers were made in several currencies, where the change from one currency to another was performed between the transfers without any reasonable explanation. The investigation detected that many of the foreign persons involved in the scheme had a criminal background or had been convicted for drug trafficking, prostitution, etc.

This example indicates the importance of:

- monitoring transactions for unusual values, volumes or patterns;
- obtaining the nature and intended purpose of a transaction or business relationship; and;
- conducting public domain searches for negative press relating to a customer or associated parties, particularly in relation to an unusual activity.

6.3 E-money: Laundering criminal proceeds using prepaid cards

Within a few months of opening bank accounts, bank accounts of Mr P and company B were credited by international transfers totalling EUR 50,000 from a Swiss company acting as agent and trader in securities. These funds were used to load prepaid cards.

In most cases these cards were loaded with the EUR 5,000 maximum limit. Mr P claimed to have loaded these prepaid cards because he had given them to his staff for professional expenses. As soon as the money was loaded onto the cards, the card holder quickly withdrew the money by repeatedly withdrawing cash from ATM machines.

Mr P was the subject of a judicial investigation regarding counterfeiting and fraud. Given the police information on Mr P the funds from Switzerland may have been of illegal origin and linked to the fraud or counterfeiting for which Mr P was known. This example indicates the importance of monitoring transactions, particularly large or frequent cash transactions.

6.4 E-money: Using prepaid cards to finance terrorism

In this particular case, a father and son held numerous prepaid cards, which were charged daily from all over Italy. Shortly after, the sums were withdrawn so that the cards' account balances were almost always close to zero. A portion of the sums withdrawn from the prepaid cards was transferred to a bank account held by the father; funds were also credited to the same bank account by a number of persons connected to Pakistan. The funds on the account were further used to order credit transfers. Both father and son were found to be involved in the 2008 Mumbai terrorist attacks.[6]

[6] https://www.express.co.uk/news/world/141649/Mumbai-attack-Father-and-son-held

ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Collective Investment Schemes ("Funds") & Businesses providing services to Collective Investment Schemes ("Functionaries")

Sector Specific AML/CFT Guidance Notes

August 2021

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58,
Finch Hill House,
Bucks Road,
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000 Email: aml@iomfsa.im
Website: www.iomfsa.im

Version 01
(First issued August 2021)

Contents

1. Foreword

This guidance is applicable to:

- Collective Investment Schemes within the meaning of section 1 of the Collective Investment Schemes Act 2008 ("CISA08")(which includes Exempt schemes) ("funds" or "schemes"); and
- businesses providing services to Collective Investment Schemes, licensed to carry on regulated activities falling within Class 3 of the Regulated Activities Order 2011, whether or not an exemption specified in the Financial Services (Exemptions) Regulations 2011 ("Exemptions Regulations") applies to that activity (known as the "functionaries").

Paragraph 2(6)(b) of schedule 4 to the Proceeds of Crime Act 2008 states that the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") applies to:

> a collective investment scheme within the meaning of section 1 of the *Collective Investment Schemes Act 2008*

Paragraph 2(6)(a) of schedule 4 to the Proceeds of Crime Act 2008 states that the Code applies to:

> subject to sub-paragraph (13), engaging in any regulated activity within the meaning of the *Financial Services Act 2008*, whether or not an exemption specified in the Financial Services (Exemptions) Regulations 2011, as those Regulations have effect from time to time and any instrument or enactment from time to time amending or replacing those Regulations, applies to that activity;

The requirements of the Code therefore apply to all funds established in the Isle of Man, and to all Isle of Man functionaries.

The Code also applies to exempt managers, asset managers and investment advisers to specialist funds (paragraph 3.9 of the Exemption Regulations), managers of Exempt and exempt-type schemes when providing services to no more than one scheme (paragraph 3.2 of the Exemptions Regulations) and Exempt managers of Experienced Investment Funds (paragraph 3.3 of the Exemptions Regulations).

Both funds and functionaries are relevant persons for the purposes of the Code.

2. Introduction

The purpose of this document is to provide guidance specifically for funds established under CIS08, and functionaries, in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Code and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

2.1 Relationship between a fund and its functionary

In practice an Isle of Man fund will delegate the majority (if not all) of AML/CFT activities to its functionaries (fund manager/administrator); however, the fund must understand and document what services the functionary is, and more importantly is not, providing in relation to the fund's obligations under the Code. This should be considered at the outset of the relationship and included as part of the functionary agreement between the fund and the Manager or Administrator. The services/agreement document should also be reviewed on a regular basis.

Functionaries' customers are the funds themselves. Functionaries are responsible for assessing the money laundering and financing of terrorism ("ML/FT") risk associated with the take on of funds as customers and the ongoing risks of the customer relationship. This includes an understanding of not only the fund's investor base but also what the fund is investing in, the fund structure, and the other functionaries providing services to the fund.

This document covers ML/FT risks that may be faced by funds and functionaries and provides further guidance and clarification in respect of approaches to customer due diligence, and other specific matters relevant to the sector.

This document also takes into account, where applicable, the following documents:

- FATF guidance for a risk-based approach - Securities Sector (2018);
- FATF report – Money Laundering and Terrorist Financing in the Securities Sector (2009);
- MONEYVAL typology research – Use of securities in money laundering schemes (2008); and
- Joint Guidelines of ESA - Risk factor guidance (2017).

The Authority recommends that relevant persons familiarise themselves with these documents and other typology reports concerning funds and functionaries.

2.2 National Risk Assessment

The Island's National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. Funds and functionaries must ensure their business risk assessments (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

In relation to the main vulnerabilities of funds and functionaries, there can be some fairly complex structures and characteristics, particularly in non-retail funds. Also, there are often

a number of different parties involved in operating the business relationships (which are mostly non-face to face), therefore there could be gaps in compliance (by the fund) with the Code if the role of the functionaries is not fully understood, or documented, by the governing body of the fund. Robust documentation in this respect is important, as is the experience of the directors of the fund and the functionaries of the fund. The NRA sets out the main risks and vulnerabilities in detail.

Overall, after applying consideration of the control and other preventative measures in place, the sector is assessed as having a medium level of vulnerability for ML and a medium level of vulnerability for FT.

3. Responsibilities

3.1 General

	Schedule 4 to POCA	The Code	Who is the customer?	Responsibilities	Agreements
Fund	2(6)(b)	The fund must comply with all provisions of the Code. Activities and reporting under the Code, such as CDD and ongoing monitoring, may be delegated to functionaries. Further guidance is provided in section 3 below.	The investors into the fund.	As per paragraph 4(3) of the Code, the ultimate responsibility for ensuring the fund's compliance with the Code is that of the fund (the governing body).	Rule 6.60 (Requirement for written functionary agreement) of the Financial Services Rule Book 2016 requires that an agreement will be in place between a fund and its functionary which sets out the services that are to be provided. These agreements should clearly set out the roles and responsibilities of each entity with regards to the fund's compliance with the Code, e.g. the ownership of records in relation to CDD and customer risk assessments at fund level. Agreements should also clearly document how the fund will monitor and oversee the work of its delegate with regards to the fund's compliance with the Code (including clearly stating if the functionary is providing the fund's MLRO. The MLRO does not need to be named in the agreement, but the fund should be aware of who is the MLRO). It is important that a fund is able to demonstrate how it has complied and remains compliant with all areas of the Code, to do this will require reporting from those undertaking activities on its behalf. Where existing agreements do not clearly set out the roles and responsibilities of each entity this could be dealt with by way of a side letter or addendum.
Functionary	2(6)(a)	The functionary must comply with all provisions of the Code in relation to its own activities and also in relation to the fund if a delegation is in place with regards to the fund's compliance with the Code.	The fund to which they are providing services i.e. the directors / owners of the management shares of the fund.	The functionary must comply with the Code in its own right.	

3.2 The role of the MLRO

Both the fund and functionary, as relevant persons for the purposes of the Code, must appoint a Money Laundering Reporting Officer ("MLRO") to exercise the reporting functions under paragraphs 25 and 27 of the Code. They must both establish, record, maintain and operate appropriate reporting procedures and controls to enable internal and external disclosures to be made.

The fund itself can meet its obligations in relation to the reporting procedures of the MLRO by:

- implementing the procedures and controls directly; or
- if the fund has no executive staff and the administration of its investors is undertaken by an IOM functionary, the fund will be considered compliant with the Code if it has formally delegated the activity to the functionary by way of agreement or other evidence of mutual agreement of the arrangements by both parties.

3.2.1 External disclosures

For the avoidance of doubt, both the fund and the functionary are required to make an external disclosure where a functionary is providing services to a fund and the functionary detects suspicious activity in relation to the fund's customers. In practice, the functionary may be providing all services to the fund, including the MLRO; in these cases it is acceptable for one external report to be submitted on behalf of both the fund and the functionary. Where this is done the external disclosure should clearly state in the grounds section that it is being made on behalf of both the fund and the functionary.

Reporting of external disclosures is through the Themis system; Themis is also used by the FIU for disseminating information and serving notices. Therefore, all relevant persons should be registered on Themis.

3.3 Services to overseas schemes

Overseas and recognised schemes are subject to the AML/CFT regimes of the jurisdictions that they are established in. Isle of Man functionaries who are carrying out AML/CFT activities for such schemes need to be aware of the AML/CFT obligations of the fund that they are acting for. When conducting a CRA on an overseas fund a functionary should consider the AML/CFT regime of that particular jurisdiction, as part of its consideration of the location of the customer's activities required by paragraph 6(3)(b) of the Code.

If a staff member of a functionary is appointed as the MLRO of an overseas or recognised fund they should ensure that they are fully aware of the legislative and reporting requirements that the fund is subject to.

Regardless of where the fund is located the Isle of Man functionary must comply with the Code in respect of their customer (fund).

3.4 Services to another functionary

Where a functionary is providing Class 3(9) or (10) services to another functionary, that functionary is their customer.

Where a functionary ("functionary A") is providing services to the manager or administrator ("functionary B") of a fund, and functionary B is located outside the island, functionary A needs to be aware of the legislative requirements that functionary B is subject to and ensure that it is considered as part of the customer risk assessment that it undertakes for functionary B.

In such instances, functionaries may wish to consider utilising the simplified measures permitted under paragraph 16 of the Code, for the purpose of verifying the identity of the other functionary. It should be noted that, whilst group entities may be able to use the exemptions and simplified measures detailed in Part 6 of the Code if the relevant conditions are met, there are no additional concessions available in relation to group entities.

As per Rule 6.60 (Requirement for written functionary agreement) of the Financial Services Rulebook an agreement must be in place between the two functionaries setting out the services that are to be provided, under Class 3(10).

As per rule 8.12 (Contractual arrangements for management and administration) of the Financial Services Rulebook, written contractual arrangements must be in place between the Class 3(9) licenceholder and the person to which it provides management or administration services.

4. Who is the fund's customer?

The complexity of the funds sector and the variety of intermediary roles that may be involved in a business relationship highlights how difficult it is to document examples that will fit all scenarios. Therefore it is important for relevant persons in this sector to understand the business relationship and apply a risk based approach to mitigate any ML/FT risks identified. The main different types of business relationship (between a fund and its customers) are described below (sections 4.1 to 4.4 of this document).

For all fund customers, the relevant person (the fund, or the functionary to whom the fund has delegated certain matters to) must have documented steps that are utilised and evidenced to determine whether a customer is acting on behalf of another person (as per paragraph 12(2)(b) of the Code). Section 3.4.5 of the Handbook gives guidance regarding identifying whether a customer is acting on behalf of another person.

4.1 Direct investor (not through an intermediary)

For instance: A natural or legal person, or a legal arrangement, ("investor"), that directly invests into the fund and directly buys units of, or shares in, a fund in their own name and not on behalf of any other party.

The fund's customer is the investor and the fund, or its functionary, must apply CDD measures (including ECDD and any required enhanced PEP measures) to that investor, including the beneficial owner of that investor in accordance with Part 4 (Customer due diligence and ongoing monitoring) of the Code. Depending on the nature of the investor, exemptions and simplified measures may be applicable under paragraphs 16 (Acceptable applicants), 19 (Eligible introducers) or 21 (Miscellaneous) of the Code , as long as all requirements are met, the investor has not been assessed as posing a higher risk and suspicious activity has not been identified.

4.2 Direct investor (through an intermediary)

For instance: A natural or legal person, or a legal arrangement, ("investor"), that invests into the fund and buys units of, or shares in, a fund in their own name using an intermediary. The intermediary is not the legal or registered owner of the shares or units and does not control or make decisions about the investment.

The fund's customer is the investor and the fund, or its functionary, must apply CDD measures (including ECDD and any required enhanced PEP measures) to that investor, including the beneficial owner of that investor in accordance with Part 4 (Customer due diligence and ongoing monitoring) of the Code. Depending on the nature of the investor, exemptions and simplified measures may be applicable under paragraphs 16 (Acceptable applicants), 19 (Eligible introducers) or 21 (Miscellaneous) of the Code, as long as all requirements are met, the investor has not been assessed as posing a higher risk and suspicious activity has not been identified.

4.3 Intermediary – it has been determined that the intermediary is not acting on behalf of another person

For instance: A financial institution (intermediary) that as part of its business activity, directly purchases the units of, or shares in, a fund in its own name and exercises control over the investment (which may be for the benefit of one or more third parties who do not control the investment or investment decisions), and where funds or income are returned to the registered owner (an account in the name of the intermediary).

In the above case the fund's customer is the intermediary and the fund, or its functionary, must apply CDD measures (including ECDD and any required enhanced PEP measures) to the intermediary. Exemptions and simplified measures may be applicable under paragraphs 16 (Acceptable applicants), 19 (Eligible Introducers) or 21 (Miscellaneous) of the Code, as long as all requirements are met, the customer (the intermediary) has not been assessed as posing a higher risk and suspicious activity has not been identified.

4.4 Intermediary – it has been determined that the intermediary is acting on behalf of another person ("third party")

For instance: A financial institution (intermediary) that acts in its own name and is the registered owner of the shares or units, but it is acting on the account of, and pursuant to specific instructions from one or more third parties.

The fund's customer is the intermediary and the fund, or its functionary, must apply CDD measures (including EDD and enhanced measures if required) to that intermediary. Exemptions and simplified measures may be applicable under paragraphs 16 (Acceptable applicants), 19 (Eligible introducers) or 21 (Miscellaneous) of the Code, as long as all requirements are met, the customer (the intermediary) has not been assessed as posing a higher risk and suspicious activity has not been identified.

In addition, as the intermediary is acting on behalf of one or more third parties, the fund (or its functionary) must identify those third parties and take reasonable measures to verify their identity (as per paragraph 12(2)(b) of the Code). Section 3.4.5 of the Handbook gives guidance regarding identifying whether a customer is acting on behalf of another person. However, the functionary, undertaking the work for the fund, may be able to use the exemption for "Persons in a regulated sector acting on behalf of a third party" (paragraph 17 of the Code), as long as all requirements are met, including that the customer (the intermediary) has not been assessed as posing a higher risk and suspicious activity has not been identified.

5. Risk Guidance

Funds and their functionaries are part of a broad sector and the ML/FT risks will vary for each of them based on a wide range of factors such as the type of products and services they supply, their customers and delivery channels.

This document covers some of the general risk factors common to the sector and focuses on particular individual business types where necessary, but is not exhaustive. Each individual relevant person needs to consider its own risk profile.

As noted above both the funds themselves and functionaries are relevant persons for the purposes of the Code; each must prepare an assessment of its exposure to ML/FT risk - this includes a Business Risk Assessment ("BRA") (paragraph 5 of the Code), and an assessment of the risk of ML/FT that a business relationship or one-off transaction poses for each of its customers (the Customer Risk Assessment ("CRA") paragraph 6 of the Code).

A Technology risk assessment ("TRA") (paragraph 7 of the Code) must also be carried out by each relevant person. If it is considered that there is no technology risk (either for the fund or the functionary) the considerations and conclusion should still be documented. The fund's TRA may be similar, and could be based upon, the TRA of its functionary. However, the fund must have its own distinct TRA, and clear consideration of the fund's own technological risks must take place.

It is common that a fund will delegate the conducting of its BRA, TRA and its CRAs to a functionary. If this is the case this should be clearly documented in the agreement required by Rule 6.60 (Requirement for a written functionary agreement) of the Financial Services Rule Book.

The fund's BRA may be similar to, and could be based upon, the CRA that the functionary prepares in respect of the fund as its customer. However, the fund must have its own separately documented BRA which meets all the requirements of paragraph 5 of the Code.

Vigilance should govern all aspects of the relevant person's dealings with its customers, including:

- account opening;
- customer instructions;
- transactions during the relationship;
- ongoing monitoring of the business relationship (including transactions);
- technology / security issues if there is an online element to the business relationship; and
- any outsourced / delegated services.

5.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed in chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship higher risk, the customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a relevant person is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. Please refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 of the Code:

13 Ongoing monitoring

(2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;
(b) conduct EDD in accordance with paragraph 15; and
(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and
(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. Also please see the list of red flags included at 5.2 of this document.

- Where a customer is reluctant to provide normal information or provides only minimal information.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the relevant person with complete information about the nature and purpose of the relationship including anticipated account activity.
- The customer is located in a higher risk jurisdiction.
- Transactions involving numerous jurisdictions.
- The customer has no discernible reason for using the relevant person's services, or the businesses' location.
- The customer's address is associated with multiple accounts that do not appear to be related.
- The nature of activity does not seem in line with the customer's usual pattern of activity.
- The customer enquiries about how to close accounts without explaining their reasons fully.
- The customer opens an account / product without any regards to loss, commissions or other costs associated with that account / product.
- The customer acts through intermediaries such as money managers or advisers in order not to have their identity registered.
- The customer exhibits unusual concern with the relevant person's compliance with Government reporting requirements / AML/CFT policies and procedures.
- Wire transfers / payments are sent to, or originate from higher risk jurisdictions without apparent business reason.
- The customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

5.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship and would therefore usually be suspicious activity. If a relevant person identifies suspicious activity appropriate steps as explained in section 5 of this document, and the Code, must be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- the customer does not provide the relevant person with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;

- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- the customer enquires how quickly they can end a business relationship where it is not expected;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer is known to have criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

5.3 Risk Factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to the funds industry. When considering these activities there could be both retail and non-retail customers. Further guidance surrounding risk assessments can be found in Part 3 of the Handbook.

Specific risk factors to consider (in addition to those noted in 5.1 and 5.2) may include:

5.3.1 Fund

- Unusual asset types.
- Complex structures.
- Rationale (does it make sense? are there any unusual features?).
- In specie transfers of assets.
- Related party transfer of assets and related party transactions.
- Payment methods – e.g. the use of crypto currency within the fund structure.
- The wide range of jurisdictions which may be involved.
- Exempt schemes - due to being more lightly regulated, these may be more susceptible to financial crime.

5.3.2 Investors

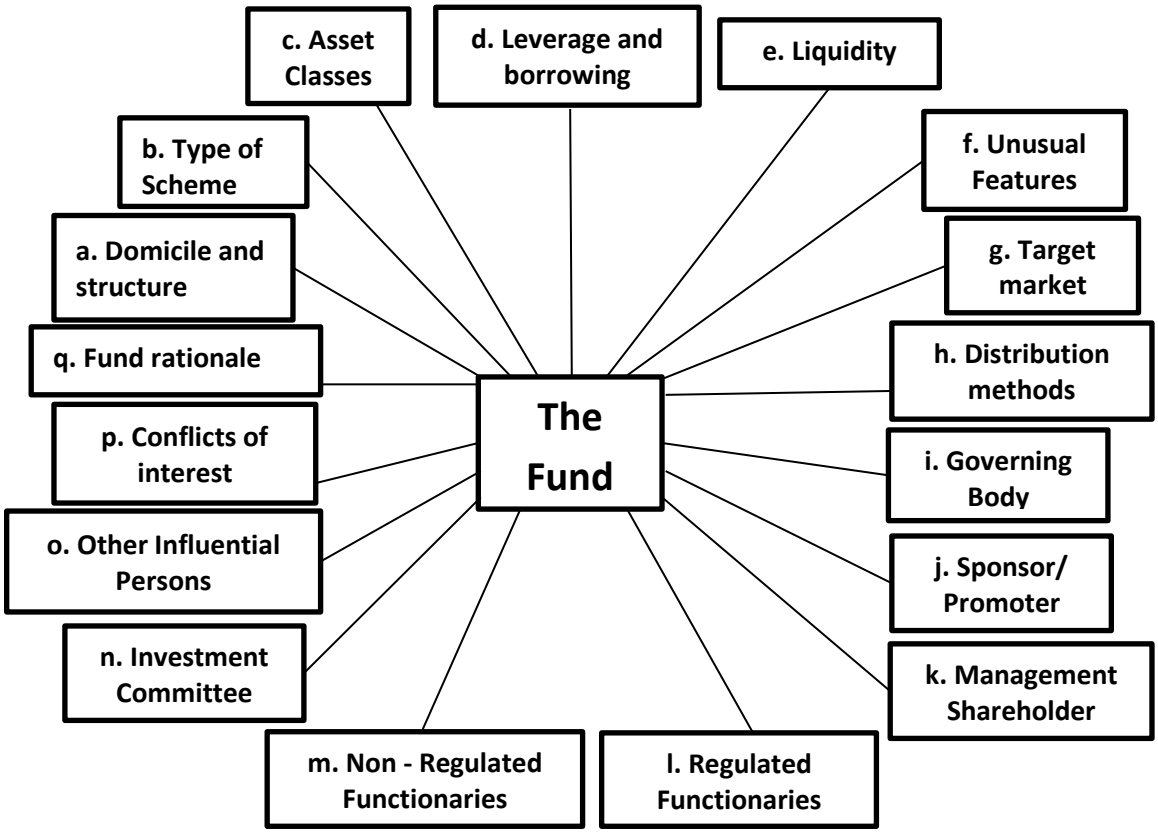
- Most transactions are conducted on a non-face-to-face basis. However, that risk could be mitigated by the fact that these transactions may involve a regulated introducer or nominee of that introducer (when relying on elements of due diligence provided by an introducer relevant persons must comply with Paragraph 9 of the Code).
- The tenure of the investment - most investment is made for medium and long-term objectives, transactions suggesting that improper use is being made of an investment fund will tend to centre on transactions held for a short time or multiple investments.
- The amount of the investment and whether this appears commensurate with the investor's circumstances.
- Holdings of investment funds may be transferred between different parties. Such transfers will be recorded by the registrar of the fund. Where transfers take place the new holder must be risk assessed and CDD must be conducted.
- The investor is undertaking many different transactions without a legitimate reason.
- The potential for payments to and from third parties.

- If the investor is another fund, high risk indicators may include:
  - aiming to invest in products that are susceptible to money laundering;
  - offering high rates of return;
  - has one off minimum investment amounts so that it operates below AML reporting thresholds;
  - highly liquid open ended frequent subscriptions and redemptions;
  - jurisdiction of the assets and advisors to the assets;
  - unregulated advisors;
  - adverse media; and
  - complex opaque structure.

5.3.3 Considerations when risk assessing a fund

In order for a functionary to have a full understanding of a fund, when completing the CRA of the fund under paragraph 6 of the Code they need to (in addition to other considerations) have an understanding of the fund's investor base, what the fund is investing in and the fund structure. The other functionaries and any related parties (for example those that contract with, or may have a relationship with, the fund, and may benefit, for example by receiving fees etc.) need to be identified and consideration given to whether any further information or due diligence is required. Diagram 1, and the table below, provide further information on matters to be considered during the CRA.

Diagram 1 - Due Diligence considerations when undertaking a customer risk assessment of the fund should include:



Risk factors to consider when conducting a Fund CRA or BRA include, but are not limited to:	
a. Domicile and Structure	- Fund's jurisdiction - Mind and management of the structure - Lack of transparency in the structure - Complexity in the structure of the fund (and the structure it is part of) - Legal structure - Separate Governing body/General Partner
b. Type of Fund	- Authorised/ Approved by a regulator - Registered with a regulator - Not subject to approval or registration (e.g. wholly or mostly unregulated) - No or very limited regulatory oversight - Open/closed
c. Asset Classes	- Listed assets - Unlisted assets – is a valid valuation methodology in place? - Unusual assets - In specie transfer of assets, related party transfers. - Use of SPV's - Real estate (potential to manipulate valuations/security/rents) Do the properties as described exist? - Valuers - experience and specialism, related party - Commodities (consider sanctions) - Esoteric, unusual or difficult to value assets - Does fund accept in specie transfers - Is fund proposing to make loans? If so is it a significant portion of the fund? Is the recipient a related party? Has the recipient been identified and verified?
d. Leverage and Borrowing (consider requirements under para 12 (7) of the Code)	- Is the lender regulated - Source of wealth of the loan provision - Jurisdiction - Related party - Financing fees and parties involved - Reasons to borrow and reasons to lend - Borrowing from related parties - Borrowing is in the fund structure but may not be directly with the fund
e. Liquidity	- Liquidity of the asset
f. Unusual Features	- Understand the reasons for the features and how they could be abused - This could relate to the product, the service providers or the assets
g. Target Market/ investors	- Jurisdiction and profile - Private arrangements - Specialist Investors - Retail investors - PEPs - Sanctions - large single source of investment/transfer from another (related) structure - Platforms
h. Distribution methods	- Financial Adviser (regulated/unregulated) - Terms of business and reliance on others - Website (global reach)

	- Jurisdictions
i. Governing Body	- Regulated / unregulated - Track record – other funds (any that may have become insolvent) and experience in the fund's investment objective - Integrity of board members (director of insolvent companies, disciplinary and regulatory action) - Jurisdiction of domicile and residence of board members - PEPs - Sanctions - Negative screening - Any other relevant information
j. Sponsor/ Promoter & k. Management Shareholder	- Regulated / unregulated - Track record – other funds and in the fund's investment objective - Jurisdiction of domicile and residence - PEPs - Sanctions - Negative screening - Any other relevant information
l. Regulated Functionaries	- Risks to arrangements - Ownership/control - Track record - Jurisdiction - PEPs - Sanctions - Reputation - Negative screening - Any other relevant information
m. Non - Regulated Functionaries	- Oversight of core functions - Risks to arrangements - Ownership/control - Track record - Jurisdiction - PEPs - Sanctions - Reputation - Negative screening - Any other relevant information
n. Investment Committee	- Regulated / unregulated - Track record - Jurisdiction of domicile and residence of members - PEPs - Sanctions - Any other relevant information
o. Other Influential Persons	- Regular suppliers and regular payments to non-functionaries - Independence, potential conflicts of interest - Risks to arrangements - Track record - Jurisdiction of domicile and residence - PEPs - Sanctions - Any other relevant information

p. Conflicts of Interest	- Consider parties having more than 1 role and related parties - Cross jurisdictional issues and risks - Assets transferred to related party structures
q. Fund Rationale	- Does the rationale make economic sense

5.4 Ongoing monitoring of the fund (customer)

The relevant person must perform ongoing and effective monitoring of any business relationship as per paragraph 13 of the Code and regularly review risk assessments (details of the review should be documented) and if appropriate these should be amended/updated as necessary. Some examples of potential higher risk indicators that may be flagged during the review process or ongoing monitoring of the fund customer are as follows (this is not an exhaustive list):

- entered into finance arrangements at a higher or lower rate than expected;
- no independent valuation of assets;
- payments away to connected parties or to unregulated third parties with no rationale;
- nature of assets changing;
- structure becomes more complex;
- purchase of assets no proof of title held by the administrator or the custodian;
- frequent changes of advisors/functionaries;
- transactions that result in big losses or total forfeiture;
- high fees paid to advisors/functionaries;
- conflicts of interest identified that are not being addressed by the fund; and
- jurisdiction of assets or investors changed to be higher risk

The relevant person should also consider the factors listed at 5.1 when performing ongoing monitoring.

6. Transfer of administration of a fund to another functionary

6.1 Customer (investor) due diligence

Where a relevant person (for this purpose the "successor firm") is taking on the administration of an existing fund from another administrator ("predecessor firm"), the successor firm should take reasonable measures to ensure that the necessary CDD of the customers of the fund (the investors) has been undertaken on behalf of the fund prior to taking on the administration.

It may be possible to rely on the CDD (including evidence of identity) obtained by the predecessor firm (who is regulated in an equivalent jurisdiction) providing that the original CDD or certified copies of the original CDD is transferred to the successor firm as part of the fund's records. The successor firm should assess the quality of the CDD (including evidence of identity held on the investors) and document deficiencies. Where there is insufficient evidence to support compliance with the Code then it may be appropriate for the successor firm, under delegation from the fund, to supplement the CDD with additional evidence to

meet the standards required by the Code. Further, if necessary, a remediation plan should be discussed with the fund and implemented as soon as is practicable after the transfer of administration. If deficiencies are serious, or the remediation plan will be protracted, the Authority should be notified.

6.2. Customer (investor) risk assessments

The successor firm will need to understand the arrangements being made by the fund in respect of the risk assessments of the investors (being customers of the fund whose administration is being transferred), and whether such risk assessments will be transferred to the successor firm (as they may form part of the fund's records) alongside the CDD (see 6.1).

If the risk assessments are able to be transferred to the successor firm, the successor firm is likely to, over time, update these risk assessments (as part its ongoing monitoring) based on its own policies and procedures, under delegation from the fund. If the successor firm finds deficiencies in the risk assessments they should discuss this with the fund and put in place a plan to remediate.

If the risk assessments are not able to be transferred to the successor firm, as part of the fund's records, a plan should be discussed with the fund and implemented as soon as is practicable after the transfer of administration.

If deficiencies are serious or any remediation plans will be protracted, the Authority should be notified.