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