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.