ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Money Transmission Services

Sector Specific AML/CFT Guidance Notes

December 2015

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 Unit, Enforcement Division
Financial Services Authority
PO Box 58,
Finch Hill House,
Bucks Road,
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000 Fax: 01624 646001
Website: www.iomfsa.im Email: aml@iomfsa.im

Contents

1. Foreword

For the purposes of this sector specific guidance, money transmission services ("MTS") refers to a business conducting any activity that would require a licence under Class 8 of the Regulated Activities Order 2013 ("RAO"). The Isle of Man Post Office carries out certain money transmission services but are exempted from the requirement to be licenced by the Authority. For further information on this, please refer to the Isle of Man Post Office sector specific guidance.

MTS include:

- operation of a bureau de change.
- provision and execution of payment services directly.
- provision and execution of payment services as agent.
- provision of cheque cashing services.
- issue of electronic money (not to be confused with virtual currency which is covered in a separate guidance note).

2 Introduction

The purpose of this document is to provide some guidance specifically for the MTS sector. This sector specific guidance should be read in conjunction with the main body of the AML/CFT Handbook. It should be noted that guidance is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the MTS sector and provides further guidance in respect of customer due diligence ("CDD") measures where a one size fits all approach may not work. Also, some case studies are included to provide context to these unique risks. The information included in this document may be useful to relevant persons to assist with their risk assessment obligations under the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 ("the Code").

This document is largely based on The FATF's 2010 reports *Money Laundering through Money Remittance and Currency Exchange Providers*[1] and *Money Laundering using New Payment Methods*.[2] The Authority recommends that relevant persons familiarise themselves with this, and other typology reports concerning the MTS sector.

[1] http://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf
[2] http://www.fatf-gafi.org/media/fatf/documents/reports/ml%20using%20new%20payment%20methods.pdf

The Island's National Risk Assessment ("NRA") is being undertaken at the time of writing and this document will likely be updated in due course following the publication of the NRA findings. This update is expected to take place in 2016.

3 General MTS Guidance

3.1 Business risk assessments

The ML/FT risks will vary for each business based on a wide range of factors such as the type of products they supply, their customers, delivery channels and geographic source/destination of funds. Relevant persons need to be aware of these risk factors to help prevent and detect ML/FT.

Generally, MTS providers can be used for ML/FT in two ways: either by performing relevant transactions without knowledge of the illegal origin or destination of the funds or by a direct involvement of the staff/management of the provider through complicity or takeover of such businesses by a criminal organisation.

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

- the simplicity and certainty of transactions.
- worldwide reach (particularly in the case of payment services).
- cash character of transactions.
- less stringent CDD requirements (i.e. exempted occasional transactions).

Factors which may mitigate the risks:

(a) products that are designed and mainly used for low value transactions;
(b) the ability to monitor linked transactions and identify transaction patterns;
(c) ability to freeze transactions after they have been initiated;
(d) knowledge of the recipient as well as the sender of the funds;
(e) the countries in which the product operates are regarded as having a lower risk of crime, money laundering and terrorist financing;
(f) face to face contact with the customer;
(g) understanding of the origin of funds; and
(h) a stated purpose for the transaction, confirmed by the features of the transaction.

Please note that the above mitigation methods are in addition to the generally applicable requirements of the Code and AML/CFT Handbook.

3.2 Customer risk assessments

Paragraph 7 of the Code requires a relevant person to undertake a customer risk assessment prior to establishing a business relationship or before carrying out an occasional transaction. This requirement also applies to occasional transactions however the Authority would expect

to see a graduated approach in terms of the level of detail used. Please refer to section 3.5.1 for detail on simplified risk assessments.

General risk assessment guidance is provided under Part 3 of the AML/CFT Handbook. This sector specific guidance aims to provide further guidance to the risks generally unique to the MTS industry.

Relevant persons should be vigilant at all stages of their dealings with customers. If a relevant person is unable to obtain a satisfactory explanation from the customer in the event of the situations listed below, the relevant person should treat this as an unusual activity.

In the event of an unusual activity, the relevant person should conduct appropriate scrutiny of the activity, carry out enhanced due diligence ("EDD") and in the event of a suspicion of ML/FT, an internal disclosure must be made. Please refer to part 7 of the AML/CFT Handbook for further detail.

This list is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused.

1. where a customer is reluctant to provide normal information, or provides only minimal, false or misleading information;
2. unusual/large cash transactions without a plausible or legitimate explanation;
3. frequent small transactions, which taken together are substantial;
4. where the customer is, or appears to be acting on behalf of another person, and there is an unwillingness to give the name of the person(s) they represent;
5. situations where the source of funds cannot be easily verified (which the relevant person may require for EDD or ongoing monitoring purposes);
6. a willingness to bear very high or uncommercial penalties or charges;
7. customers requesting information about reporting limits of transactions;
8. customers sending money to an unknown third party that they are unable to verify;
9. customers making payments to a higher risk jurisdiction without a plausible or legitimate explanation;
10. a customer or a group of customers making transactions to a common beneficiary/group of beneficiaries without a plausible or legitimate explanation;
11. transactions that do not make commercial sense;
12. high value remittances;
13. cash funding and cash pay-outs;
14. the countries in which the product operates;
15. the level of control or comfort regarding the entity delivering the funds in the receiving country;
16. new customers with no previous relationship looking to undertake larger transactions;
17. speed and size of transaction: money launderers normally want to move funds quickly in order to avoid detection or seizure. This is more easily done in large one-off transactions; and
18. split transactions: the more sophisticated money launderer will look to split a large transaction into several smaller ones with the intention of avoiding AML-related controls. Such splitting can occur within one location, or even across organisations. This

is known as 'smurfing' and can occur when a number of people each exchange small amounts of cash. The funds eventually end up back with the criminal.

3.3 Source of funds

For all business relationships and occasional transactions (whether exempted occasional transactions or not), the Code requires that a relevant person must take reasonable measures to establish the source of funds.

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, source of funds is automatically established. Further, for cash transactions, as part of a risk based approach, it is not considered necessary for relevant persons to normally seek further information from customers for transactions below:

- €5,000 for bureau de change and cheque encashment; or
- €1,000 for money transmission services.

Relevant persons should however 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.

3.4 Ongoing monitoring of linked transactions

Relevant persons should put in place a process to detect and monitor repeat transactions:

(a) that indicate that an occasional transaction relationship has evolved into a business relationship (and any exempted occasional transaction concession would then be disapplied); and/or

(b) 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.

3.5 Exempted occasional transactions

Paragraph 12(5) of the Code (as detailed in part 6.5 of the Handbook) provides a concession that the verification of identity is not required for customers carrying out an exempted occasional transaction.

An exempted occasional transaction is an occasional transaction under €5,000 (or currency equivalent) for bureau de change or cheque encashment or €1,000 (or currency equivalent) for payment services and e-money.

All other Code requirements under paragraphs 7 (customer risk assessment), 11 (continuing business relationships), 13 (beneficial ownership and control), 14 (politically exposed persons) and 15 (enhanced due diligence) 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 AML/CFT Handbook could prove overly burdensome and unmanageable in a busy retail outlet.

In order to reduce the compliance burden for exempted occasional transactions, the Authority considers it acceptable for the relevant person to:

- Complete a simplified customer risk assessment; and
- Collect a reduced amount of identification information (lower or standard risk only);

3.5.1 Simplified customer risk assessment

It is understood that the majority of occasional transactions undertaken by a customer are likely pose a standard (or lower) risk of ML/FT but it is essential that a staff member confirms this risk rating, has the ability to determine that a transaction poses a higher risk of ML/FT. Where a higher risk of ML/FT is posed, EDD must be carried out in line with paragraph 15 of the Code.

Paragraph 7(2)(c) of the Code requires a customer risk assessment to be documented in order to demonstrate its basis. The Authority does not expect a relevant person to document a detailed risk assessment as described in section 3.3 of the AML/CFT Handbook for all occasional transactions. A simplified customer risk assessment may be carried out for occasional transactions under €15,000 or currency equivalent.

A simplified customer risk assessment must simply record that the staff member has made a determination of the ML/FT risks posed by the customer and which risk rating they selected. This determination could be captured by selecting the option of “low/standard” or “high” in an online form, spreadsheet or paper format. The rationale behind the decision of which risk rating to select need not be documented.

Where a relevant person 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.

3.5.2 Reduced identification information:

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. Full name, date

of birth and residential address should be obtained as a minimum instead of the full list provided at 4.5.1 of the AML/CFT Handbook.

4 Bureau de Change

4.1 Risk factors

1. 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 sections 3.1. and 3.2. of this sector specific guidance document.

2. 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. Cash transactions: 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.

4. The product is easily transported across jurisdictions and can be transferred to another person without leaving an audit trail.

5. 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.

6. 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.

7. The customer operates within a high-risk sector. 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.

8. The customer undertakes transactions that make no commercial sense or do not match the profile of the customer. This also includes significant and unusual changes to a customer's established pattern of behaviour.

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 part 4.1 of this document) 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 €5,000 or equivalent), especially in cash, the relevant person should formally obtain and document the nature and intended purpose of the business relationship/transaction.

5 Payment services

5.1 Description of payment service activities

Payment services are defined in the RAO as meaning any of the following activities when carried out as a business activity:

(a) Services enabling cash to be placed on a payment account together with all of the operation requited for operating a payment account;
(b) Services enabling cash withdrawals from a payment account together with all of the operations required for operating a payment account;
(c) The execution of the following types of payment transaction –
    (i) Direct debits, including one-off direct debits;
    (ii) Payment transactions executed through a payment card or similar device;
    (iii) Credit transfers, including standing orders;
(d) The execution of the following types of payment transaction where the funds are covered by a credit line fir the payment service user –
    (i) Direct debits, including one-off direct debits;
    (ii) Payment transactions executed through a payment card or similar device;
    (iii) Credit transfers, including standing orders
(e) Issuing payment instruments or acquiring payment transactions;
(f) Money remittance;
(g) The execution of payment transactions where the consent of the payer to execute the transactions is given by means of any telecommunication, digital or IT device and the

payment is made to the telecommunication, IT system or network operator acting only as an intermediary between the payment service user and the supplier of goods or services.

5.2 Bill payment services

At the time of publishing this guidance, only the Isle of Man Post Office are providing bill payment services to customers allowing them to pay bills at the Post Office rather than paying direct to the service provider.

Only certain 'bill payment' services are 'caught' by the Code:

Not 'caught':

1. Where the money is NOT handled by the relevant person (i.e. nothing hits their bank account);
2. Where the money IS handled by the institution however receipt is given by that relevant person for that payment.

   For example, if a customer pays their electricity bill at the Post Office and the Post Office in turn loses that payment so it doesn't reach the Manx Utilities Authority ("MUA"), the customer is NOT liable to the MUA because they have a receipt for the payment of the bill.

   This is not payment services because the Post Office is acting as the MUA's agent and is able to give a receipt for payment on behalf of the MUA and settle the customers' liability.

'Caught'

1. Where the money IS handled by the relevant person but the relevant person cannot give receipt for payment on behalf of the payee.

5.3 The difference between agent and direct services

Where an MTS located outside the Isle of Man, such as MoneyGram or Western Union, transacts with a customer through an ***agent*** (which for this purposes is the relevant person in the Isle of Man and must be licensed by the Authority for payment services as agent), the business (principal) is the person contracting with the customer and is responsible for applying the CDD measures relating to that customer. The agent is therefore expected to comply with the principal's AML / CFT policies and procedures and it is therefore important that the agent establishes AML related accountabilities with the ***principal*** money transmission business.

5.4 Risk factors

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 sections 3.1 and 3.2 of this sector specific guidance document.

According to the 2010 FATF report, many ML/TF cases relating to payment service providers involve small wire transfers, however, given that the total value of funds involved in such cases are quite significant, this could imply the involvement of highly organised criminal groups.

(a) A commonly reported 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 send sender and or the receiver (true beneficiary of the transaction)

(b) 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.

(c) 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.

In order to mitigate such risks the relevant person should:

- ensure that transaction monitoring includes a check for common beneficiaries or types of beneficiaries ; and
- in relation to ***payment services as agent***, agents should have visibility of transactions conducted by other agents on behalf of the principal.

5.5 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 in section 5.4 and 3.2 above) 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.

5.6 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.

6 Cheque Cashing

6.1 Risk factors

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 part 3 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.

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:

1. 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.

2. 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.

3. 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.

4. 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.

Higher risk indicators include:

1. Fictitious companies may be set up for the purposes of cheque fraud. Look out for low and consecutive cheque numbers.
2. A number of different people cashing cheques all of which are drawn on the same company, with an unfamiliar company name.
3. An indication of benefit fraud could be where people try to cash their benefit cheque and produce a wage slip as ID, or vice versa where they are cashing a salary cheque and produce paperwork regarding state benefits as ID.
4. 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.
5. 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.
6. A sudden increase in the value of cheques.
7. 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.
8. Post containing a recently issued chequebook may have been intercepted by a fraudster who then creates ID to replicate the original payee's ID.
9. A customer wants to cash a cheque that is made payable to a limited company. The customer could be involved in tax evasion.
10. 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.

6.2 Specific identification issues to consider

Sub-paragraph 13(2)(c) of the Code requires the relevant person to determine whether the customer is acting on behalf of another person and, if so, identify that other person, and take reasonable measures to verify that other person's identity using relevant information obtained from a reliable, independent source.

It is the Authority's view that a natural person cashing a cheque on behalf of another person (legal or natural) is acting on behalf of another person.

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 may 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 must 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. 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.

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.

Relevant persons should however seek (and document) further information from customers where factors described in 6.1 of this guidance document are present.

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 part 7 of the AML/CFT Handbook.

7 E-Money

7.1 Background

Only the issuers of electronic money ("e-money") are 'caught' under the RAO. There are a number of businesses on Island that deal with, administer, promote etc. e-money but are not the issuer and therefore are not 'caught'. As there are no current businesses operating in this area, this guidance has been left intentionally brief and will be reviewed and updated at such time that there is an e-money issuer on Island.

E-money is defined in the RAO as meaning electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which is –

(a) issued on receipt of funds for the purpose of making payment transactions;
(b) accepted by a person other than the electronic money issuer; and
(c) is not excluded by exclusion 8(i)

Exclusion 8(i) states that e-money does not include –

(a) monetary value stored on instruments that can be used to acquire goods or services only –
    (i) in or on the electronic money issuer's premises; or
    (ii) under a commercial agreement with the electronic money issuer, either within a limited network of service providers or for a limited range of goods or services;
(b) monetary value that is used to make payment transactions executed by means of any telecommunications, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunications, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.

Examples of e-money products include prepaid cards and e-wallets. Examples of a product not considered to be e-money products include high street store points rewards cards and gift vouchers.

7.2 Risk factors

E-money products can be an alternative to a variety of traditional banking products and services, such as debit or credit cards or travellers cheques. Many prepaid cards enable customers to make international payments, and some are increasingly offering features similar to conventional bank accounts: such as products that allow the customer not only to make payments but to receive payments from third parties and making cash withdrawals.

In general terms, the following factors can make e-money products higher risk –

1. The absence of credit risk for prepaid 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.
2. Transactions can often be carried out much quicker than through more traditional channels. This can complicate monitoring an potentially frustrate efforts to freeze the funds.
3. Many business models rely on non-face-to-face relationships and transactions.
4. High or unlimited usage limits.
5. Broad acceptance as payment method.
6. Products that allow cash withdrawals.

8 Case Studies

8.1 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 Romania citizens (X, Y, Z) 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 bureaux 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 the 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 change 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
- monitoring transactions for unusual activity such as frequent cross-border transfers

(based on an example from FATF's 2010 report Money Laundering through Money Remittance and Currency Exchange Providers)

8.2 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/TF risks of a recipient country.
- monitoring transactions for unusual activity.

(based on an example from FATF's 2010 report *Money Laundering through Money Remittance and Currency Exchange Providers*)

8.3 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/TF risks of a recipient country.
- monitoring actual activity against that which is expected for a particular customer.

(based on an example from FATF's 2010 report *Money Laundering through Money Remittance and Currency Exchange Providers*)

8.4 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 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 money transmission services. 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.

(based on an example from FATF's 2010 report *Money Laundering through Money Remittance and Currency Exchange Providers*)

8.5 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.
- conducting public domain searches for negative press relating to a customer or associated parties, particularly in relation to an unusual activity.

(based on an example from FATF's 2010 report *Money Laundering through Money Remittance and Currency Exchange Providers*)

8.6 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 money transmission services including payment services as agent.
- effective AML/CFT oversight of such businesses by the relevant authorities.

(based on an example from FATF's 2010 report Money Laundering through Money Remittance and Currency Exchange Providers)

8.7 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
- considering the rationale for a transaction and whether the rationale is indicative of a tax offence

(based on a case detailed on the Lexis Nexis *Legal Newsroom* website dated June 2013)

8.8 E-money: Laundering criminal proceeds using prepaid cards

Within a few months of opening a bank accounts, the 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 expense. 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 O, the funds from Switzerland hay 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

(based on a case detailed on the FATF 2010 report *Money Laundering using New Payment Methods*)