FIAU

MONEY REMITTANCE IN MALTA:

AN ANALYSIS OF THE AML/CFT CONTROL FRAMEWORK &

OBSERVATIONS DERIVED FROM 2017-2020 STRS

Issued: 30 September 2020

MONEY REMITTANCE AML/CFT CONTROL FRAMEWORK

1. INTRODUCTION

The definition of 'money remittance' under Maltese law derives from the second Payment Services Directive (EU) 2015/2366 (known as the 'PSD2') which defines 'money remittance' as a type of payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

According to the World Bank, money remittance to low-income and middle-income countries increased by 9.6% in 2018 from 2017, totaling to $529 billion.[1] The increase in Anti Money Laundering / Combatting the Financing of Terrorism ("AML/CFT") regulatory obligations resulted in more stringent banking practices leading to credit institutions reducing their high risk client portfolio to minimise risk exposure. In view of this, money remittance is proving to be a more attractive way to transfer funds in particular because it is an attractive means of reaching under-banked people.

Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfer of funds lays down the rules relating to the payers and the payees which undertake the business of money transfers, wherein one of the payment service providers is established in the European Union. Such rules are aimed as a safeguard against ML/FT risk emerging from such activity.

[1] The World bank: https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018

2 AML/CFT RISKS

In the sectorial vulnerability assessment of the Maltese National Risk Assessment of 2018, the payment services sector scored a high inherent risk and a medium-low mitigating controls resulting in medium-high residual risk.[2] The Joint Opinion of the European Supervisory Authorities (the "ESA") on the risks of money laundering and financing of terrorism ("ML/FT") affecting the European Union's financial sector ("ESA Joint Opinion"), stated that "the most significant ML/FT risk relates to payment institutions that offer money remittance services, owing to the cash-intensive nature of their services, the high speed and/or high volumes of transfers (albeit transfer size is typically small) and transfers to high-risk jurisdictions".[3]

The vulnerabilities associated with money remittance transfers, make this service susceptible to the potential laundering of proceeds from different types of criminal activities, including drug trafficking, human smuggling and customer fraud.

Below are some of the ML/FT risks associated with remittance transfers:

- The large volume of transactions being processed through this service, as a consequence of which, it can make it difficult to detect laundered funds;
- The global reach of large remittance transfer companies, which can allow customers to move funds easily and rapidly across borders;
- The use of extensive agent networks spread across multiple jurisdictions that can possibly be colluding with criminals;
- The type of customers making use of these services include immigrants who want to transfer funds to high risk countries were correspondent banking relationships are weak;
- The cash-based nature of money remittance service result in lack of visibility on the source of funds, making it difficult to determine whether the origin of the funds are from legitimate sources and not the proceeds of crime or money laundering;
- The increased ability to structure payments by breaking large amounts into smaller amounts to circumvent customer due diligence (CDD) thresholds and attempting to transfer funds possibly linked to FT without these being noted and subject to checks; and
- The high risk element resulting from the geographical location in which the payer and payee are located (e.g. high value transactions sent to countries known to have links to terrorist activities,
- would render the money remittance service provided highly vulnerable to FT risks)

[2] Results of the ML/FT National Risk Assessment, Ministry for Finance 2018
[3] Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector (October 2019)

3. MITIGATING MEASURES

In accordance to the 'Key results on the Sectoral Risk Assessment of Terrorism Financing and National CFT Strategy' published by the National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (NCC) in December 2019, the high value of money remittances in the local context as well as the high-risk nature of the source and destination of remittances increases the risk of FT emanating from these services.

In view of this, the FIAU in conjunction with the MFSA has carried out an analysis of the implementation effectiveness of the controls in place to mitigate ML/FT risks as applied by Subject Persons authorised to carry out the business of money remittance under the second schedule of the Financial Institutions Act and in terms of the Banking Act during the year ending 2019.

The analysis has established that although a number of controls are being applied there are a number weaknesses, which need to be addressed to further ascertain that ML/FT risks are adequately mitigated.

The main AML/CFT controls that were identified as being applied by Subject Persons to mitigate the ML/FT money remittance risks include:

- Obtaining MLRO or senior management approvals for transactions above defined thresholds;
- Applying controls to ascertain that(Customer Due Diligence) CDD is triggered upon reaching the regulatory thresholds;
- Applying Enhanced Due Diligence (EDD) measures for high risk scenarios;
- Limiting transaction processing to payees who are also account holders;
- Obtaining details on both remitter and beneficiary of the transaction;
- Accepting only non-cash payment methods for funding money remittance or limiting cash transactions;
- Applying rules that limit the amount of transactions that can be received or sent from/to each account;
- Refraining from receiving transactions from agents of customers; and
- Providing AML/CFT training to employees involved in the provision of the service.

Notwithstanding the above, a number of AML/CFT deficiencies were identified including the following:

- The Business Risk Assessment carried out by Subject Persons operating in this industry does not usually take into consideration all risks emanating from the money remittance, such as the volumes and values of cash payments and the jurisdictions from/to where the payments are being made;
- Assessment on the reputability of jurisdictions to identify those jurisdictions that pose a higher ML/FT risks is not being carried out by the majority of Subject Persons;
- Absence of a customer risk assessment methodology and, where in place, such methodology is not sufficiently transparent in explaining the risk scoring methodology being adopted nor does it always take into consideration all the relevant risk factors;
- Policies and procedures in place do not always distinguish between on-boarding of money remittance clients vis-a-vis other clients serviced by the Subject Person to mitigate the risk arising from these types of services;
- Deficiencies in the transaction monitoring system such as:
  - Absence of alerts to flag transactions that exceed the limit imposed on the amount of funds that can be sent and/or received;
  - Inability to identify linked transactions;
  - Inability to trigger alerts flagging transactions that are not in line with the customer's profile;
  - Multiple transactions being sent to/from the same account not being flagged;
  - Payments done by the same customers through different agent networks are not identified; and
  - A transaction monitoring system reliant solely on post-event monitoring (i.e. no scrutiny of transactions prior to processing).

This analysis has therefore identified that the major controls weakness is in relation to the transaction monitoring systems adopted by the Subject Persons. The risk arising from these types of services, coupled with the lack of robust transaction monitoring systems in place, raise concerns on the ability of Subject Persons to effectively monitor money remittance transactions and report any suspicion of ML/FT in a timely manner. In fact, the number of STRs raised by money remitters between January 2017 to December 2019 stands at 81, which is not considered to be sufficient given the number of transactions that are processed by these Subject Persons on an on-going basis.

4. KEY FIGURES BASED ON JANUARY 2017 – MAY 2020 SUSPICIOUS ACTIVITY REPORTS AND SUSPICIOUS TRANSACTION REPORTS ("STRS")

Between January 2017 and May 2020, the FIAU received 98 STRs from money remitters, 87% of which were submitted by 3 reporting entities. Whilst the remaining 13% of these were submitted by 4 other entities, some subject persons submitted no STRs with the FIAU in the 3- year period.

In terms of the quality of the STRs, these were graded with a score between 1 to 5, with 1 representing a low rating and 5 representing a good quality STR generally, with complete information and documentation provided at submission stage.

STRs received by year	2017	2018	2019	2020	Total
No. of STRs received	14	28	39	17	98
Average quality for the STRs by year	4	4	4	4	4

The STRs scoring a lower feedback rating (1-3, for example) would generally involve the suspicious transaction or activity not being reported in a complete and clear manner, the situation that gave rise to the suspicion not being described in sufficient detail, or the supporting documentation being incomplete or not included at all at the submission stage.

Even if the initial feedback provided to the subject persons on the quality of the STR would be in the range of 4-5, further queries made by the Intelligence Analysis Section should indicate to the submitters the type of additional information which is expected to be provided by them at initial reporting stage. This is intended to improve the quality of submissions to follow.

The quality of the STRs and the documentation submitted impacts the length and the outcome of the analytical process. As at May 2020, from the 40 finalized cases that were initiated from STRs submitted by money remitters, 12.5% were disseminated to local law enforcement or competent authorities. Whilst the majority of the STRs are still undergoing analysis, 6 spontaneous intelligence reports were sent to foreign Financial Intelligence Units based on the STRs received between 2017 and May 2020.

The table below presents the main reasons why the entities submitted the STRs and captures the inconsistencies observed in the customer's behavior, as well as unusual elements in terms of transactions performed.

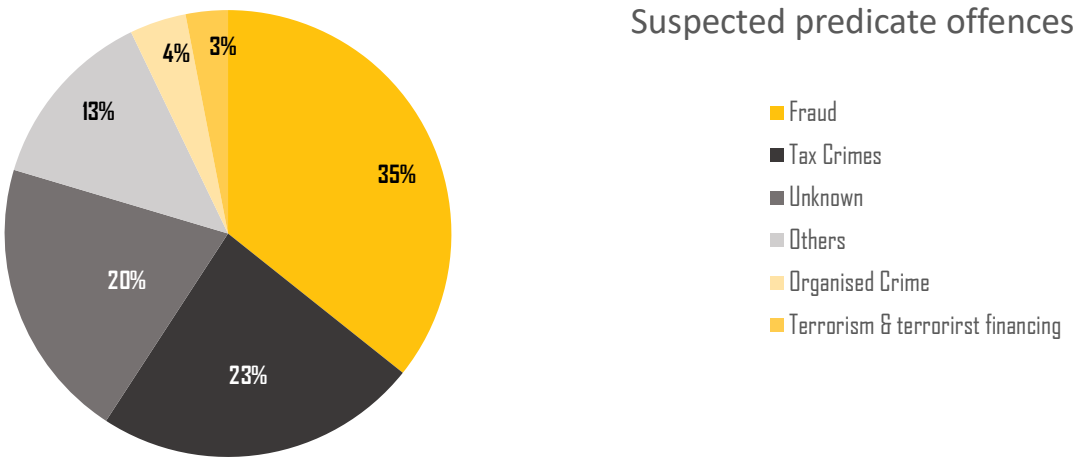
5. TOP REASONS FOR SUSPICION

No.	Reason for suspicion	%
1	Transaction activity which is unexplained or is inconsistent with known customer profile	17%
2	Transaction narrative is suspicious or does not make any commercial sense within the context of the transaction itself	12%
3	Customer requests payment of proceeds to unrelated third parties	10%
4	Transfers to, or from, high-risk jurisdictions, without apparent economic business reason/sense	8%
5	Customer became uncooperative when requested to provide required details and/or documentation on a transaction or operation	8%
6	Other	44%

Unusual or suspicious identification documents or lack of documents, adverse media, internet related scams, as well as remitting to or withdrawals made from locations which are in conflict zones or known terrorism activity areas are further considerations based on which reports were submitted by the money remitters.

The main suspected predicate offences that were considered as linked to the reports are presented in the chart below and are topped by fraud and tax crimes, participation in an organized criminal group and racketeering and funding of terrorism.

Corruption and bribery, forgery, extortion, usury and illegal gambling were other suspected predicate offences observed in the STRs received. It is to be noted that 20% of submissions do not indicate information in relation to the predicate offence. This is sentiment to the fact that while it is desirable to provide an indication to the suspected predicate offence if known, this is not a requirement when submitting reports on suspicious activity or transactions to the FIAU.



6. TYPOLOGIES AND CASE DESCRIPTIONS

To better understand the nature of existing and emerging ML/FT risks and pursue effective mitigating measures to address those threats and vulnerabilities, several cases that gave rise to suspicious activities and suspicious transactions reports being submitted with the FIAU are presented in the following paragraphs.

Case 1

A natural person attempted to send money through an agent of a money remitter to several persons in an offshore jurisdiction.
However, some of the payments were blocked by the transactions monitoring system, at which point the person attempting the transfer called the local money remitter's office.

The person provided details of the blocked transactions, but it was noted that the person contacting the money remitter's office was not the person whose details were on record as the payer. He explained that the details held on record were those of a relative, who, at the time was abroad and as such, could not visit or call the branch. No details were divulged by the subject persons and the caller was informed that no information would be given out without the named person being present.

The money remitter contacted the person whose name was listed on the transaction, and discovered that the person was not aware of said transfers.

Case 2

An STR was submitted by a money remitter as a result of the complexity of the transaction, especially in light of the apparent straight forward nature of the said transaction.

A company registered in another European Union member state, operating in the IT services field, attempted to send a payment to a company incorporated in the United States of America ("US"), operating in a completely different field. However, it did not choose to do so directly from its bank account in Malta to the bank account of the US Company, but by using the services of a local money remitter. Furthermore, the narrative of the transaction suggested it was a payment on behalf of a third-party, namely a natural person involved in another US company with whom the EU company had an agreement with.

The complex structure of the payment, involving many financial institutions, jurisdictions and parties, which did not have any apparent or economic lawful purpose gave rise to an STR being submitted with the FIAU.

Case 3

During transactions monitoring, a money remitter noted several transactions of significant amounts that were carried out by a local company, transactions which were not in line with its commercial activity and the expected pattern of transactions.

The reason provided by the client for a significant payment was for the purchase of a property. Despite the fact that the sale agreement was provided as supporting documentation for the transactions, there was no apparent link between the buyer, the seller, and the client who paid out the funds. For another transaction, given the substantial amount involved, a simple, generic loan agreement was provided. Considering the nature of the transaction and the significant amount involved, a robust agreement was expected, with clear terms and clearly identifying the parties and specifying their roles (for example, which party was the lender and which party was the borrower).

Furthermore, concerning adverse media in relation to some of the parties were identified.

7. CONCLUDING REMARKS

Although the number of financial institutions providing money remittance activity in Malta is limited to a few institutions, by nature money remittance is an activity significantly vulnerable to ML/FT risks. Therefore, unless financial institutions venturing in money remittance activities are sufficiently aware of the risks that their operations entail and invest adequately in controls that effectively mitigate the associate risks, the jurisdiction will increase its vulnerability to ML/FT risks.

The analysis indicated that although Subject Persons have in place a number of controls to address the ML/FT risks resulting from the carrying out of this business, given the nature of money remittance, it is pivotal that robust transaction monitoring systems are implemented. Therefore, Subject Persons should refine the rules, parameters and timing of monitoring currently in place to enable better scrutiny and monitoring of transactions, thereby allowing prompt identification and reporting of suspicious transactions.

65C, Tower Street,
Birkirkara BKR 4012,
Malta

Questions on this document or on the application of AML/CFT measures may be sent to **queries@fiaumalta.org**

Financial Intelligence Analysis Unit
65C, Tower Street,
Birkirkara BKR 4012,
Malta

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org