FATF • GAFI

Financial Action Task Force | Groupe d'action financière

COUNCIL OF EUROPE | CONSEIL DE L'EUROPE

FATF Report

Money Laundering through **Money Remittance** and **Currency Exchange Providers**

June 2010

COUNCIL OF EUROPE – COUNTERING MONEY LAUNDERING AND FINANCING OF TERRORISM (MONEYVAL)

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL (formerly PC-R-EV) was established in 1997. At their meeting of 13 October 2010, the Committee of Ministers adopted the Resolution CM/Res(2010)12 on the Statute of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). This new statute elevates MONEYVAL as from 1 January 2011 to an independent monitoring mechanism within the Council of Europe answerable directly to the Committee of Ministers. The aim of MONEYVAL is to ensure that its member states have in place effective systems to counter money laundering and terrorist financing and comply with the relevant international standards in these fields.

For more information about MONEYVAL, please visit the website:

WWW.COE.INT/T/DGHL/MONITORING/MONEYVAL

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

TABLE OF CONTENTS

ABBREVIATIONS

AML	Anti-money laundering
CFT	Counter financing of terrorism
CE	Currency exchange
CDD	Customer due diligence
CTR	Cash transaction report
EU	European Union
FIU	Financial intelligence unit
ID	Identification
KYC	Know your customer
ML	Money laundering
MR	Money remittance
NA	Not available
STR	Suspicious transaction report
TF	Terrorist financing

EXECUTIVE SUMMARY

1. This joint FATF/MONEYVAL report contains information on money laundering and terrorist financing methodologies associated with the money remittance and currency exchange sector. The findings contained in the report derive from information provided by 61 FATF, MONEYVAL and Egmont Group member States and other open source material. Though the focus of the report is to a certain degree on the MONEYVAL region and the wider European area, the experience of countries from other regions of the world was actively sought and integrated into the report.

2. Apart from providing a useful general overview of the sector of money transfer remittances and currency exchange providers, the regulatory framework, the supervision and sanctioning regimes, the report sets out identified money laundering and terrorist financing methods and techniques involving money remittance and currency exchange providers.

3. Several case studies described in this report illustrate that money remittance and currency exchange businesses have been both witting and unwitting participants in laundering activities, in all three stages of the process (placement, layering and integration), and in certain instances, for terrorist financing purposes. The identified risks of ML/TF through the sector detailed in the report are related to clients, owners or agents. The cases highlight also the links between money laundering in the money remittance sector and other criminal activities (*e.g.*, fraud, trafficking in human beings, smuggling, drug trafficking, economic crime).

4. A number of vulnerabilities to money laundering across the sector that make up the money remittance and currency exchange sector were identified. The analysis of the case studies and other materials enabled the project team to compile numerous examples of indicators of potential money laundering activities related to transactions, customer profile and behaviour as well as specific indicators for bureaux de change and money remittance providers that may help the industry to identify and describe suspicious behaviours and protect themselves against money launderers and other criminals.

5. Clearly, laundering through money remittance and currency exchange providers poses a number of regulatory and enforcement challenges. At the same time, it was observed that there is low detection of money laundering in comparison to the size of the industry as a whole. The money laundering and terrorist financing threat in the sector not only results from direct penetration of criminals into operations of money remittance or currency exchange providers. The absence or lax implementation of AML/CFT standards and adequate related policies provide opportunities which are being exploited by money launderers and other criminals.

6. Finally, the report maps also a number of issues and areas which were identified in this context as appearing to require additional efforts, both from regulatory and supervisory authorities as well as from the industry, in order to reduce the misuse of the sector and ensure that ML/TF risks are adequately addressed. These issues will likely require further investigation together and updating research, not only to continue the development of a better understanding of specific money laundering and terrorist financing risks in the money remittance and currency exchange sector but also to ensure that regulatory responses are proportionate and effective.

INTRODUCTION

7. Specialised financial businesses have for many years played an increasing role in providing certain types of services, including money remittance (MR), foreign currency exchange (CE) and the issue/management of means of payment to a variety of actors. The globalisation of financial markets and the development of information technology have made the movement of funds across the world easier and have thus further spurred the growth of these specialised financial services. The service providers in this field (the "MR/CE sector") are quite diverse and range from simple businesses to complex chain operators.

8. In order for criminals to move, hide and eventually use the funds generated by their illegal activities, they must seek ways to launder those funds without drawing the attention of law enforcement or other authorities. Given the range of products and services offered, the variety of distribution channels, the high transfer speed and the fact that they are often cash-intensive businesses, the MR/CE sector may provide significant opportunities for criminals desirous of laundering funds unless appropriate safeguards are in place. Particular risks involved with the sector are related not only to the misuse of MR/CE businesses for laundering money but also to the owning of such businesses by criminal groups and corrupt employees co-operating with criminals.

9. Typologies reports published by the Financial Action Task Force (FATF) over the years have highlighted money laundering risks posed by *bureaux de change* (FATF typologies report, 1996-1999 and 2001) and examined money laundering and terrorist financing vulnerabilities of alternative remittance systems (FATF typologies report 2004-2005). At the time that these studies were conducted, little information was available on the MR/CE sector in MONEYVAL member States or on the ML/TF risks facing the sector. Thus, MONEYVAL and the FATF decided in 2008 to undertake a joint project on methods of money laundering through MR/CE businesses.

Scope of research

10. In most jurisdictions, MR/CE businesses are not defined as banks. While in some countries, such as the United States[1] and the United Kingdom, national legislation has defined this group of financial service providers, the MR/CE sector in most countries is not explicitly defined. In the FATF 40 Recommendations as well as in the third EU Money Laundering directive[2], those financial businesses providing MR/CE services are considered to be a subset of financial institutions[3]. Using the term *non-bank financial institutions* to refer to MR/CE services can also be misleading in that the term as defined by the FATF also included broker dealers in securities and casinos. The term is even less helpful now, as the FATF currently makes the distinction between financial institutions on the one

1 In the United States, the term *money services business* has been defined since 1999 when the Secretary of the Treasury issued a ruling revising the regulatory definitions of certain non-bank financial institutions for purposes of the Bank Secrecy Act. These revised definitions were grouped into a separate category of financial institution called *money services businesses* or *MSBs*.

2 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

3 For further details, please see the glossary of the FATF 40 Recommendations and article 3 (2) (a) of the Directive 2005/60/EC.

hand and *designated non-financial businesses and professions (DNFBPs)* on the other. The former category includes all of the activities that are provided by MR/CE services.

11. Typically, MR/CE services include three types of activity:

- Currency dealers/exchangers;
- Money remitters; and
- Issuers, sellers and redeemers of stored value and monetary instruments, such as money orders and traveller's checks.

12. The category "money remitters" is diverse, ranging from large organisations, like Western Union, to what are often termed "informal value transfer systems". This latter category includes systems that often operate outside the "regulated" financial system and are deeply rooted in historical, cultural and economic backgrounds. Well known examples include "hawala", "flying money" systems indigenous to China, India's *hundi* system, and the *padala* system used in the Philippines[4].

13. Given the research already conducted on the subject by the FATF other international organisations, this study does not attempt to duplicate already existing information. For this reason, it was decided to exclude from its scope the analysis the misuse of new payment methods[5], of traveller's checks and money orders. The methods and trends of money laundering and terrorist financing through alternative remittance systems are also not analysed in-depth[6] because the potential misuse of such systems for terrorist financing was already covered in the 2008 terrorist financing typologies report produced by the FATF.[7]

14. This research report therefore focuses on non-bank financial institutions that provide at least one of the following services: (1) money remittance, (2) currency exchange/dealing and (3) issuing, cashing or redeeming of cheques/money orders/stored value cards.

15. The research conducted on this subject also provided an opportunity to take stock of potential money laundering threats arising from the changeover to the Euro in certain countries. This is an important issue for many MONEYVAL members in that a number of EU members from MONEYVAL have yet to adopt the Euro as official currency and are looking to develop best practices based on measures already adopted by euro zone countries to address those threats. This research thus attempts to lay out relevant findings, in the light of developments in this specific sector as well as in the EU regulatory area, resulting from the adoption and implementation of the EU legislation that directly impacts upon the MR/CE sector.

16. After examining how MR/CE businesses may be misused for money laundering purposes and identifying vulnerabilities that may be exploited by criminals, the report will look at appropriate measures which could be taken to address the identified vulnerabilities. It should be stressed that

---

4 HM Treasury (2006). For more details about the alternative remittance system, the profile of the users of the system and its role in ML, please refer to Chene (2008).

5 See FATF (2006). The FATF has since updated this research , and a report on the subject was published in October 2010 that considers the vulnerabilities of new payment methods to ML/TF (the report focuses on prepaid debit cards, mobile payment services, on-line payment systems). Additional literature on ML/TF schemes through new payment technologies is also available (see US Department of Justice (2006), Sienkiewicz (2007), Choo (2008)).

6 See FATF (2005), MENAFATF (2005), Carroll (2007). See also for further information the IMF (2005a, 2005b)

7 See FATF (2008a)

available information has allowed the money laundering threat facing MR/CE businesses to be documented. Regarding the threat of terrorist financing facing such businesses however, there was far less sector-specific information to work with. This report then focuses primarily on the range of ML techniques to which MR/CE businesses may be vulnerable and provides a series of illustrative typologies. A non exhaustive list of indicators of potentially suspicious activity has been included in the report, which is intended to assist the private sector, law enforcement and regulators detecting ML within the sector. Finally, the report also briefly lays out a series of issues and areas for further consideration.

Methodology and sources

17. The research and analysis of the material used to develop this report was conducted by a small joint project team of experts from MONEYVAL and FATF jurisdictions. The experts contributed to the analysis and drafting of the report through a series of working meetings and exchanges of written material that took place over a period of about two years. The project was led by Estonia, with Mr Raul Vahtra and Ms. Kerly Krillo of the Estonian financial intelligence unit heading up the work, including the main task of drafting this report. The following countries and organisations contributed to the project with either substantive material or expertise: Australia, Bulgaria, Cyprus, Germany, Italy, Mexico, the Netherlands, Poland, Romania, Sweden, Spain, the United States, the Egmont Group and the European Bank for Reconstruction and Development.

18. One of the main sources of information for the project was a detailed questionnaire which solicited a range of range of material, including case studies, national-level typologies research and other relevant expertise. Well over 50 questionnaire responses were received and analysed by the project team from FATF, MONEYVAL and Egmont Group members.[8] The project team also used the discussions and findings of the Joint FATF/MONEYVAL meeting of experts on typologies (held in Monaco, 24-26 November 2008, which gathered participants from 40 countries, 2 international organisations and 3 FATF-style regional bodies), as well as other FATF typologies reports, case studies and open source information.

19. While the focus of this report is to a certain degree on the MONEYVAL region and the wider European area, the experience of countries from other regions of the world was actively sought and integrated into the report.

Acknowledgements

20. This project was conducted by a team of experts from both FATF and MONEYVAL members, who have contributed to the project throughout the working meetings and by providing written contributions and comments which have been reflected in this report. The project team would like to thank all FATF, MONEYVAL and Egmont Group members which responded to the survey and provided other valuable input to this research.

8 See Annex 1 for a list of contributing jurisdictions.

CHAPTER I –OVERVIEW OF MONEY REMITTANCE & CURRENCY EXCHANGE SECTORS

1.1 General

21. The globalisation of the financial sector and the vast development of information technologies has contributed to a considerable increase in the volume of the activity carried out by the MR/CE sectors during the past two decades. In the US for example, the estimated value of financial services provided by the money service business industry, which includes MR/CE activity,[9] was approximately USD 200 billion annually in 1997; however, by 2005 the industry had grown to approximately USD 284 to USD 305 billion (FinCEN 2005). Unfortunately there are no similar figures available for the equivalent sector in other parts of the world; therefore it is impossible to estimate the size of the MR/CE industry globally.

1.2 The money remittance sector in MONEYVAL/FATF member States

22. The World Bank estimate of money remittance (MR) worldwide is 443.5 billion USD for 2008 and 420.1 (estimated) for 2009. Not all countries are able to determine the total volume of incoming and outgoing MR activity. It is therefore difficult to provide an indication of the proportion of global MR that MONEYVAL/FATF countries represent. Nevertheless certain jurisdictions are able to provide reliable estimates of the volume of MR activity, and these are included in Table 1 below. From this information, countries can be divided into two groups:

- *Senders, i.e,.* countries where the amount of outgoing money transfers are remarkably higher than incoming.
- *Receivers, i.e.,* countries where the amount of incoming money transfers are remarkably higher than outgoing.

23. At European level, the first group mostly includes primarily the "old" EU member states (Germany, Greece, Italy, and Spain), along with Croatia, Cyprus, Malta, and Monaco; while in the second group southeastern European countries and former Soviet republics (Armenia, Bulgaria, Georgia, "the former Yugoslav Republic of Macedonia" and Ukraine) predominate.

Table 1. Volume of money remittances sent and received in selected MONEYVAL/FATF member States (2006-2008, million EUR)

Country	Sent			Received		
	2006	2007	2008	2006	2007	2008
Armenia	615.6	787.7	722.0	971.0	1 353.7	1 433.5
Bulgaria	NA	11.1	8.6	NA	94.7	73.5
Cyprus	190.5	212.1	227.3	17.0	37.1	29.8

9 See paragraph 10 above for an explanation of the difference between MSBs and MR/CE service providers as the terms are used in this report.

Country	Sent			Received		
	2006	2007	2008	2006	2007	2008
Germany	1 830.1	1 927.3	1715.5	548.0	1 026.7	1 200.1
Spain	4 891.0	6 267.0	NA	202.0	222.0	NA
Georgia	92.9	77.5	77.5	387.1	606.0	701.1
Greece	570.4	775.4	NA	178.4	203.9	NA
Croatia	44.5	42.0	43.9	21.9	22.3	22.0
Italy	4 528.9	6 044.1	5 980.0	248.2	252.2	191.6
Monaco	10 732.0	11 471.0	11 833.0	1 469.0	1 382.0	1 389.0
"the former Yugoslav Republic of Macedonia"	5.6	7.1	10.3	68.6	78.8	95.3
Malta	68.3	80.7	78.7	31.0	64.9	35.2
Ukraine	97.2	133.6	267.2	1 070.4	1 444.7	1 773.5

NA: not available.

24. Among those MONEYVAL/FATF countries that provided information for this study, MR systems are very heterogeneous. Even within the same geographical regions, countries often have very different MR systems. Therefore, it is difficult to highlight any 'typical cases'.

25. The number of independent MR service providers[10] varies greatly from one MONEYVAL/FATF country to another (see table 2 below, data reflecting 2008 figures). At one end of the scale are the United States with more than 25 000 MRs (this number does not include agents)[11], the UK (approximately 2 800 MRs) and Mexico (approximately 1 100 MRs). At the other end of the scale are Austria, Japan, Monaco, Moldova, San Marino, Serbia and Turkey. In these countries, there are no companies that provide MR services alone. In these jurisdictions, MR services are provided by either banks and/or post offices, which also offer other services in addition to MR. Most countries, however, are in between the two extremes.

Table 2. Number of money remittance service providers in FATF and MONEYVAL member States

Country	N° of MR providers	Country	N° of MR providers	Country	N° of MR providers
USA	25 096	Chile	15	Poland	2
UK	2 818	Greece	14	Croatia	1
Hong-Kong, China[1]	2 008	Armenia	11	Liechtenstein	0
Mexico	1 085	Slovakia	11	Austria	0
Denmark	334	Bulgaria	7	Japan	0
Argentine	122	Cyprus	7	Monaco	0
Sweden	96	Malta	7	Moldova	0
Finland	70	Latvia	6	San Marino	0
Spain	46	France	4	Serbia	0

10 Note: throughout this study 'independent MR service providers' refers to the companies to whom the money transferring is a core business, it does not include banks, post offices, and other agents of the MRs to whom MR is side-business.

11 As at 13 February 2009.

Country	N° of MR providers
Germany	38
Estonia	34
Italy	30
Netherlands	28

Country	N° of MR providers
Lithuania	4
Romania	4
Macau, China	2
"the former Yugoslav Republic of Macedonia"	2

Country	N° of MR providers
Turkey	0
Albania	NA
Georgia	NA
Ukraine	NA

Table Notes:

Remarks: only independent MR services providers (excluding banks, post offices, agents).

1. Please note that in Hong-Kong, China no distinction is made between money remittance and currency exchange providers. Remittance agents and money changers (RAMCs) are entitled to provide both services. Although not all RAMCs provide both services, most of them do so.

26. In some countries, MR providers have well-developed agent systems, with post offices, currency exchange offices, banks, travel agencies, hotels and other companies providing remittance services as agents of the MR companies. Examples in which MR services are offered by other than specific MR businesses include:

Albania:	currency exchanges (as agents of Western Union and MoneyGram);
Bulgaria:	banks, currency exchanges and financial houses;
Chile, Liechtenstein, Monaco:	post offices (in the first two as agents of Western Union and in the latter as agents of Western Union and MoneyGram);
Croatia:	post offices and one bank[12] (as agents of Western Union);
Estonia:	post offices, banks, currency exchanges and travel agencies;
Finland:	currency exchanges, travel agencies and miscellaneous shops;
France:	post offices (through an agreement with a branch of Western Union licensed as a financial company);
Germany:	post offices, currency exchanges and banks;
Greece:	post offices and currency exchanges (as agents of Western Union);
Italy:	currency exchanges, travel agents, hotels, phone centres, internet centres, news agents and stationers;
Malta:	post offices, travel agencies and hotels;
Moldova:	banks (as agents of Western Union, MoneyGram);
Mexico:	post offices, currency exchanges, banks and travel agencies;
Netherlands:	travel agencies;
Poland:	banks, one credit unions' financial services provider, travel agencies and a few other providers of selected banking

12 Société Générale Splitska Banka.

	services;
Romania:	both post offices and banks (as agents of Western Union, MoneyGram);
Slovakia:	post offices, currency exchanges and banks;
Spain:	post offices;
Sweden:	post offices, currency exchanges, banks, money transaction offices, travel agencies and hotels;
"The former Yugoslav Republic of Macedonia":	currency exchanges, banks, travel agencies and hotels;
UK:	post offices, travel agents and other outlets like restaurants and general stores; and
US:	currency exchanges, banks, travel agencies and hotels.

27. Post offices usually provide money transfers as an independent side-business of their main activity or act as agents for other MR companies. Typically they are registered / licensed as money remitters in several countries. For example, in San Marino 5 out of 10 post offices operating domestically are authorised to perform money transfer services.

28. Banks offer MR services in Argentina, Chile, Cyprus, France[13], Greece, Malta, the Netherlands, Poland and Serbia, and Spain.

29. Both post offices and banks are authorised to perform MR services as side-businesses in Albania; Armenia; Denmark; Georgia; Hong-Kong, China; Italy; Latvia; Macau, China; Poland; Turkey and Ukraine.

30. Furthermore, currency exchanges (in Argentina, Chile, Malta, the Netherlands, Romania), travel agencies (in Cyprus, Romania) and hotels (Romania) also offer MR services, although money transfer is not their core business activity. This distinguishes them from companies that are defined as 'independent MR providers' in this report.

31. The distinction between national/international MR providers also differs greatly. In some countries, like Croatia, Liechtenstein and Lithuania, Western Union is the only MR service provider. In others, like "the former Yugoslav Republic of Macedonia" and Poland, where Western Union and MoneyGram operate as MR providers, there are no similar domestic MR operators. In other countries on the other hand, such as Japan and San Marino, no international companies operate. Latvia combines both systems. Latvian Post is the only national provider of money remittance services. The foreign providers are not registered and are supervised by banks that provide money transfer service.

32. When an MR service establishes a permanent business relationship, the identification of the client is mandatory for money remitters in most jurisdictions. For occasional transactions, the thresholds triggering certain measures vary from the obligatory identification of all customers in Argentina, Austria, Cyprus, Germany, Italy, Netherlands, and Spain, to EUR 15 000 in Finland, San Marino, and Serbia. In respect to the identification requirements for clients initiating money

[13] The particular feature of the France is the presence of foreign banks (mostly African and Asian) that are specialised on offering money remittance services to their customers. Quite naturally, the customers of these banks are foreigners living in France.

remittance, countries can be placed into the following three broad categories (for more details, please refer to table 6 in annex 3):

1. Identification of the client is mandatory for each MR transaction;
2. Identification applies starting from a EUR 1 000 threshold (as required in the EC Regulation No 1781/2006) and
3. Identification applies starting from some other threshold.

33. If there is a suspicion of ML or TF, as a general rule, the threshold does not apply and identifying the client and informing the FIU is mandatory.

Table 3. The client identification threshold in MONEYVAL/FATF member States

No threshold, mandatory identification	Argentina; European Union State members[1]; Liechtenstein; Macau, China[2]; Monaco
EUR 1-999	Armenia, Georgia, Japan, Turkey, Ukraine
EUR 1 000	Croatia, Mexico[3], Moldova[4], San Marino
EUR 2 000-2 999	"The former Yugoslav Republic of Macedonia" and US
EUR 3 000-11 999	Chile
EUR 12 000	Albania
EUR 15 000	Serbia

Table Notes:

1. In EU Member States, financial institutions must identify and verify the complete information on the payer/originator before executing any wire transfer regardless of any threshold. Only where the wire transfer is (1) executed from an account of a customer who has been identified and whose identity has been verified in the course of the account opening and whose identification records have been stored according to requirements of the 3rd EU AML Directive or (2) of an existing customer whose identity has to be verified at appropriate times according to the 3rd EU AML Directive financial institutions stating that there is no requirement to repeatedly verify the originator's identity (Art. 5(3) of Regulation (EC) No. 1781/2006). In case a wire transfer is not made from an account, the financial institution must verify the identity of the originator only when the amount is above EUR 1 000 unless the transaction is carried out in several operations that appear to be linked and together exceed EUR 1 000.

2 In Macau, China, under the regulations for cash remittance activities, cash remittance companies are required to record the identification and address of remitters and beneficiaries regardless of the amount of the remittances in Macau. For wire remittances done through banks and post office, the threshold is MOP 8 000 (appr. USD 1 000).

3 In Mexico, there are three different thresholds in order to require information for individual cash operations or with travellers cheques, as follows:

- between USD 1000 – 3000, information is requested
- between USD 3000 – 5000, information is requested along with a copy of the official identification
- for USD 5000 or more, information is requested and a whole file is integrated to the system.

4 In Moldova, the threshold for occasional transactions is 50,000 lei (appr. EUR 3 500) and for electronic and wire transfers 15 000 lei (appr. EUR 1 000). At the same time, according to the foreign exchange legislation, payment/ transfers shall be made by licensed banks upon the submission by the individual of the identity document regardless of the amount of the payment/ transfer.

1.3 The currency exchange sector in MONEYVAL/FATF member States

34. Similar to money remittance, the currency exchange[14] (hereinafter CE) services vary somewhat in MONEYVAL/FATF member. However, due to the standardised nature of the business, the differences are not as noteworthy as for MR.

[14] The terms '*bureaux de change*' and 'currency exchange providers' refer to the same type of activity. For the sake of consistency within this report, the term 'currency exchange provider' is used.

35. According to the data received, the number of currency exchange service providers shows considerable variation from one MONEYVAL/FATF member to another (see table 4 below). In a number of countries (*e.g.*, Croatia; Georgia; Hong Kong, China; Mexico; Poland; Serbia; Spain; United Kingdom, Ukraine and United States) the number exceeds 1 000. At the other end of the scale, there are Finland and Monaco with less than 5 currency exchange providers.

Table 4. Number of bureaux de changes[1] in selected MONEYVAL/FATF member States

Country	No. of bureaux de change	Country	No. of bureaux de change	Country	No. of bureaux de change
Albania	NA	Bulgaria	625	Sweden	56
Argentina	NA	France	515	Denmark	44
Poland	4 193	Italy	489	Germany	24
US [2]	3 294	Romania	470	Macau, China	17
Mexico [3]	2 757	Slovak	455	Greece	12
Spain	2 256	"the former Yugoslav Republic of Macedonia"	271	Netherlands	12
Hong Kong, China[4]	2 008			Malta [5]	7
Serbia	1 781	Moldova	319	Finland	4
UK	1 404	Armenia	246	Monaco	2
Croatia	1 242	Japan	196	Austria [7]	0
Ukraine [6]	1 104	Estonia	163	Cyprus[7]	0
Georgia	1 050	Chile	128	Liechtenstein[7]	0
Turkey	755	Latvia	75	San Marino[7]	0
		Lithuania	62		

Table Notes:

1. Only independent service providers, i.e. excluding banks and other businesses for which CE is not a core business.
2. As of 13 February 2009, the date of the US response to the questionnaire for this project.
3. currency exchange services providers.
4. Please note that in Hong-Kong, China no distinction is made between money remittance and currency exchange providers. Remittance agents and money changers (RAMCs) are entitled to provide both services. Although not all RAMCs provide both services, most of them do so.
5. In Malta CE (as well as MR) providers form part of a wider category of entities defined as "financial institutions". Therefore, the number of MR and CE providers in the tables refers to the same institutions
6. In Ukraine, the following institutions are authorised to open currency exchanges for conducting currency exchange transactions: banks operating under a banking license and having prior written permission, and financial institutions/national operators of postal services that obtain general license from the National Bank of Ukraine for conducting non-trade transactions with currency values.
7. Only banks provide currency exchange services.

36. Naturally in most (if not in all) countries, banks are authorised to perform CE services. In a few countries – Austria, Cyprus, Liechtenstein and San Marino – CE is provided exclusively by banks, and no independent currency exchanges exist. Although it is not obvious from the first sight, in Lithuania the system is quite similar. All CE businesses (approximately 60) in Lithuania are operated by banks. Furthermore, divisions and branches of banks as well as credit unions (22 at present) are also authorised to perform currency exchange.

37. In Mexico, the currency exchange service providers can be divided into two groups:

- 'Foreign exchange houses' (*casas de cambio*) are legal entities that require a license to engage in currency exchange services with the public; and

- 'Foreign exchange centres' (*centros cambiarios*) are either natural or legal persons that do not require a license in order to engage in currency transactions, but whose operations are limited to the equivalent of USD 10 000.00 per customer per day. They must be registered with the Tax Administration Service.

38. In Slovakia there are three types of foreign currency exchange providers:

- *Currency exchanges* – require a 'simple FX license' that authorises natural or legal persons to purchase or sell local currency against foreign currency (money transfers are not included);
- *FX business providers* I – legal persons with a minimum capital requirement of EUR 333 333. Their license allows them to both purchase and sell local currency against foreign currency on their own or their client´s behalf but only in cashless form. They are permitted to make only domestic money transfers; and
- *FX business providers II* – legal persons with minimum capital requirement of EUR 33 333. Their license authorises them to carry out or intermediate cross-border money transfers both in local or foreign currency in cash. They are permitted to make foreign money transfers through banks only.

39. Regarding customer identification, the same thresholds apply as for MR in most countries. The exceptions are:

Table 5. Threshold Exceptions to Applicable Customer Identification Requirements

COUNTRY	THRESHOLD (as of 2008)
Croatia	HRK 105 000, *i.e.* appr. EUR 15 000
Estonia	EEK 100 000, ie. appr. EUR 6 400
France	EUR 8 000
Japan	YEN 2 000 000, *i.e.* EUR 15 566
Germany	EUR 2 500 threshold applies if the transaction is carried out through an account other than the customer's account;
Georgia	GEL 3 000, *i.e.* appr. EUR 1 400
Greece (and Italy, Malta, Poland, Sweden, United Kingdom)	EUR 15 000
Latvia	LVL 5 000, *i.e.* appr. EUR 7 117
Lithuania	EUR 6 000
Moldova	MLD LEI 50,000 (approx. EUR 3 500)
Macau, China	MOP 20 000 , *i.e.* appr. EUR 1 740
Mexico	Thresholds vary for transactions involving cash or travellers' cheques
Slovakia	EUR 1 000
United States	USD 1 000, *i.e.* appr. EUR 820

Table Notes:

1. In Mexico there are three different thresholds in order to require information for individual cash operations or with travellers cheques, as follows:
   - between USD 500 - 3000, information is requested;
   - between USD 3000 – 5000, information is requested along with a copy of the official identification (identical threshold applicable also to MR);
   - for USD 5000 or more, information is requested and a whole file is integrated to the system (identical threshold applicable also to MR).

1.4 Licensing, supervision and sanctioning system of money remittance and currency exhange providers[15] in MONEYVAL / FATF member States

Licensing/registration

40. In most MONEYVAL and FATF member states the MR provider must be registered or licensed (see table 7 in annex 1)). In countries that require licenses in order to provide MR service, either the central bank, as in Albania, Bulgaria, Cyprus, Slovakia, Spain, or the financial supervisory authority, as in France, Germany or Malta, is the competent authority to grant licenses.

41. In the European Union, new rules on payment services in the EU internal market provide for an evolution regarding the licensing of providers of money remittance services. Directive 2007/64/EC on payment services in the internal market (which was due to be integrated into the EU legal framework in November 2009) establishes the obligation to licence payment service providers (except for certain financial institutions that already have a licence, such as banks). The Directive creates two levels of licences. Firstly, the EU-wide licence for the newly created category of 'payment institution'. This category includes payment service providers which are not allowed to accept deposits from the public (which banks do) and which do not issue electronic money (which is done by banks or so-called 'e-money' institutions). Obtaining an authorisation as a 'payment institution' is subject to a set of strict conditions, including prudential requirements. The authorisation granted by a EU Member State to a 'payment institution' is valid for the entire EU territory, which can, for instance, provide its services in other EU countries including through local agents. There is a specific procedure to approve agents, where AML checks can be done by the relevant competent authorities. Therefore, it is possible that a payment institution licensed in one EU country operates in another EU country without the need to obtain a second licence from that second EU country. Secondly, the EU directive on payment services allows EU Member States to establish a lower level (but this level is not compulsory): natural or legal persons unable to meet all the strict conditions for becoming 'payment institutions' may nevertheless carry out payment services in the Member State where they have their head office or legal residence after having been registered in that EU Member State. Some of the Directive requirements for 'payment institutions' are nevertheless applicable to this lower level. The goal of this lower level regime is to "bring all persons providing remittance services within the ambit of certain minimum legal and regulatory requirements" (cf. paragraph 15 of the preamble of the Directive). As a result, the provision of money remittance services in the EU is forbidden for other categories of undertakings or individuals.

42. In the countries that require registration of MR service providers, one of three entities generally oversees the registration process:

- The financial intelligence unit (FIU) (for example, in Chile; Hong Kong, China, and the United States[16]);
- The financial supervisory authority (for example, in Georgia); or
- Another government authority (for example, the Ministry of Economic Affairs and Communications in Estonia; State Provincial Office of Southern Finland in Finland; the Monetary Authority in Macau, China; the Tax Administration Service in Mexico; HM Revenue and Customs in the UK).

---

15 In this section we focus solely in independent money remittance /currency exchange providers, *i.e.* those that do not operate as a part of banks, post offices and/or agents of the MR providers.

16 In addition to federal registration, MSBs must be licensed or registered in 48 of the 50 US States.

43. Latvia is an exception, as money remitters need neither register nor obtain a license to operate; however, legislation addressing this matter was in the process of being drafted at the time of the survey.

44. As regards the provision of CE services, a license is required in most countries.[17] As a general rule, the authority responsible for issuing licenses is the central bank.

45. In a few countries, the CE businesses do not need to be licensed, but have to be registered in order to be permitted to provide currency exchange service. Usually the institution responsible for keeping the registry is a governmental authority (for example, National Revenue Agency in Bulgaria, the Commerce and Companies Agency in Denmark, the Ministry of Economic Affairs and Communications in Estonia, HM Revenue and Customs in the UK, etc.).

46. In Chile in 2009 there was no mandatory registering/licensing system for money remitters and currency exchange at the state level, and the FIU had in the interim taken on the task of keeping the record instead. The current system was considered to be ineffective and amendments to the legal framework were being discussed in order to introduce the statutory registering system.

47. In Japan there is no registering/licensing system for currency exchange at all. In Finland, there is a legal requirement to establish a registering/licensing system for currency exchanges, but its concrete implementation had not yet taken place at the time the survey was carried out.

48. In most countries (with the exception of Chile; Georgia; Hong Kong, China; and Japan where no specific 'fit and proper' controls apply to MR/CE businesses) the 'fit and proper' control is applied in some form at least during the licensing/registration process. As a minimum standard, this background check usually includes evaluating the qualification, creditworthiness (*i.e.* absence of tax duties) and criminal record (for serious offences) of the owners and managers of the company. In Denmark the 'fit and proper' controls cover beneficial owners, too.

49. However, there are countries that apply more in-depth control mechanisms. For example, in Armenia the central bank also checks the qualification through examination of the employees of the currency exchange business. The qualification document is valid for three years.

50. After granting the license/registration to the company, in most countries no permanent on-going monitoring is applied and further action is taken only if there is evidence of unlawful activities or a change in the company's management board. In some countries this system is somewhat standardised; for example, in Germany prosecution authorities and courts have to notify *Bundesanstalt für Finanzdienstleistungsaufsicht* (BaFin – the Federal Financial Services Supervisor) of criminal proceedings against managers. The same system is applied in Estonia, where the registration of the company is cancelled if the member of the administration of the company is convicted of criminal offences.

51. However, there are a few countries that monitor the eligibility criteria more or less on an periodic basis. For example, the information about meeting the eligibility criteria of the managers and owners is updated at least once a year in Albania, Croatia, Italy, Lithuania, Mexico, and Sweden.

AML/CFT supervision

52. In most countries, the central bank, the FIU and/or financial supervisory authority carries out AML/CFT supervision over the money remitters and currency exchanges.[18]

---

17 See Annex 3, Table 7.

53. In the countries that apply the registering system of money remitters/currency exchanges, usually the authority responsible for keeping the register also supervises the entities.

54. Typical sanctions applied to an unregistered /unlicensed money remittance providers are fines and/or imprisonment.[19] Maximum levels of fines imposed vary from EUR 5 000 in Bulgaria to unlimited amounts in the UK.

55. Most responding countries indicated that existing sanctioning regime was considered to be effective in deterring the illegal MR providers. In the United States, for example, there are federal and state sanctions for operating a money remitter or currency exchange that fails to become licensed or registered. For example, knowingly operating a money remittance business without a proper state license/registration and federal registration is subject to a fine of up to USD 5 000 a day and imprisonment for up to five years. Furthermore, an unlicensed or unregistered MR/CE service providers may be subject to civil and criminal penalties for violations of the Bank Secrecy Act. In contrast, in Denmark, the current system is considered to be relatively ineffective because it takes a long time for law enforcements to investigate and prosecute persons in the case of unregistered activities. However, Danish AML supervisors in close co-operation with the State Prosecutor have decided to intensify the sanctions in cases of non-compliance.

56. In Mexico, the Tax Administration Service, a decentralised entity of the Ministry of Finance and Public Credit) is in charge of the supervision of money remitters (*transmisores de dinero*) and currency exchange centres (*centros cambiarios*) regarding the AML/CFT preventive measures in Mexico. With regards to supervision, in the case of *casas de cambio*, these are by decree of law supervised by the National Banking and Securities Commission (CNBV).

57. Although there is no agency that supervises CE service providers in Japan, such businesses must report the volume and number of transactions to the Ministry of Finance when they exceed a certain volume.

---

18 See Annex 3, Table 4.

19 See Annex 3, Table 5.

CHAPTER II - MONEY LAUNDERING METHODOLOGIES INVOLVING MONEY REMITTANCE AND CURRENCY EXCHANGE PROVIDERS

58. This chapter describes some of ways in which money remittance and currency exchange providers have been exploited for ML/TF purposes through a series of selected case studies provided by responding jurisdictions. The focus of this material is primarily on "traditional" *i.e.* formal money remittance and currency exchange providers; however, a few observations have also been included about informal systems.

59. Generally, these MR/CE providers can be used for money laundering and terrorist financing in two ways: either by performing relevant transactions without knowledge of the illegal origin or destination of the funds concerned or by a direct involvement of the staff/management of the provider through complicity or takeover of such businesses by the criminal organisation.

60. Several features of the MR/CE sectors make them an attractive vehicle through which criminal and terrorist funds can enter the financial system, such as the simplicity and certainty of MR/CE transactions, worldwide reach (in case of money remitters), the cash character of transactions, low-thresholds, the often less stringent customer identification rules that apply to such transactions compared with opening bank account and reduced possibilities for verification of the customer's identification than in credit or other financial institutions , etc. The nature of the customer's relationship with the MR/CE service provider and the brevity of contacts is also a significant vulnerability.

61. Money remittance providers are used at all stages of the money laundering process. Currency exchanges specifically are an important link in the money laundering chain, particularly during the placement stage. Once the money has been exchanged, it is difficult to trace its origin. Also, it has been noted that considering that they are small businesses, currency exchanges can be easily prone to takeover by criminals and used to launder money.

62. From responses received to the survey questionnaire for this project, the most important factors that may indicate possible misuse of MR/CE service providers:

- Use of underground remittance systems;
- Use of mules / straw accounts;
- Mismatch between the economic activity, country of origin, or person and the money remittances received;
- Periodic transfers made by several people to the same beneficiary or related persons;
- Transfers over a short period of time of low amounts that together represent a large sum of money;
- Transfers from one or more senders in different countries to a local beneficiary.
- Sudden inflow of funds in cash followed by sudden outflow through financial instruments such as drafts and cheques;
- Structuring of transactions and/or changing of MR/CE provider for subsequent orders to keep a low profile; and
- False information during the identification procedure/lack of co-operation.

63. Many cases involve small value wire transfers, however, given that the total value of funds involved in these cases is quite significant, this could imply the involvement of highly organised criminal groups. However it is also interesting to note that a number of cases deal with high-value wire transfers. The information gathered highlights the links between money laundering in the money remittance sector and other criminal activities (*e.g.*, fraud, trafficking/smuggling in human beings, drug trafficking, economic crime, etc). The identified ML vulnerabilities associated with the MR/CE sectors can be related to customers, owners or agents as highlighted below.

2.1 Customers

64. Structuring or "smurfing" was frequently reported and appears to remains the most usual ML method identified in regard to MR/CE providers and the most frequently reported suspicious activity in many countries. Structuring occurs when a person carries out several cash transactions by breaking them into smaller amounts in order to avoid the mandatory threshold reporting and/or customer identification requirements. Such transactions can be carried out either in a single day or over a period of days, through the same or several agents.

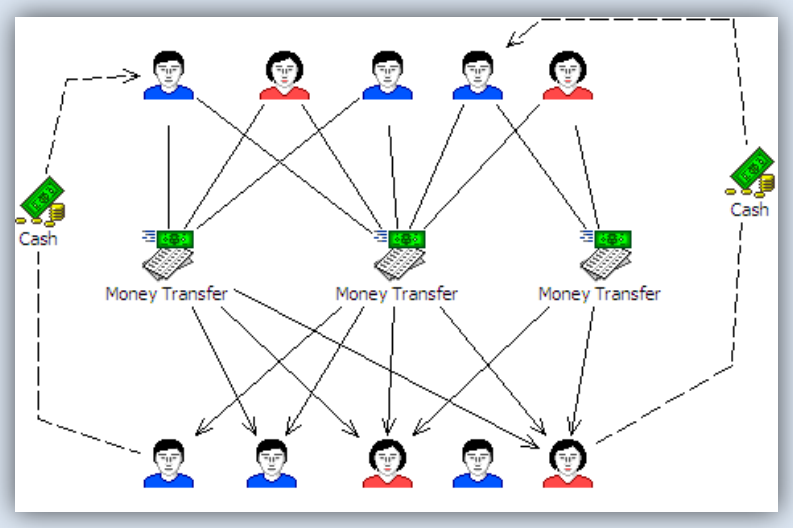
Box 1. Structuring

Customer: individual/ business

Mechanism: money remittance

Red-flag indicators: use of several currencies, structured transactions, a great number of persons involved, large number of transactions related to each other during a short time period.

Case description: 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. Then they 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 in different countries and finally returned to the originators. The total sum of received and sent remittances was almost equal, and the persons 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.



Source: Bulgaria.

65. In countries where there are many MR/CE service providers, it is difficult to cross-match data, and the risk of being involved in "smurfing" schemes is therefore typically higher than in countries where there are few service providers. The abundance of MR/CE service providers makes structuring a relatively "safe" choice for the criminals in most countries and minimises the possibility that law enforcement agencies might detect such activity unless there is well-functioning co-operation at the national level that then helps to identify smurfing schemes that may be using multiple service providers.

66. It is often very difficult to find a link between persons using money remittance services for the transfer of funds because the transaction paper trail is often lacking. The nature of MR/CE business is that service providers often carry out one-off transactions with occasional customers, and many of the customer relationships that do exist are not of a durable nature. In the case of one-off transactions, some MR/CE service providers are not able to monitor the financial behaviour of their customers in the same way as a traditional bank is able to do with its customers.

67. As a consequence, due diligence measures applied by some MR/CE service providers in less developed markets are usually at most confined to identification and verification of the identity of the person, without the possibility of ongoing monitoring of the customer's activities. In addition to the name of the customer, the indication of the beneficiary (sender or receiver), the destination or origin of the funds, limited additional information is typically available for MR/CE providers.

68. Another method commonly identified in money laundering schemes is the use of straw men (so-called 'money mules'). A money mule is a natural person who makes his (bank) account available to a criminal or criminal organisation receiving some form of remuneration in return. A money mule is often solicited via a spam e-mail to accept a transfer of money –received from the victim(s) of a criminal or of a criminal organisation – which he/she then is instructed to transfer to the account of another person, whose personal details the money mule also receives via e-mail. The money mule is allowed to retain a part of the money for the services rendered to the criminal or criminal organisation.

Box 2. Use of 'money mules'

Customer: individual

Mechanism: money remittance

Red-flag indicators: use of straw men, organised criminals involved

Case description: An FIU from country A received a request for information from country B that involved among others company X, known to be alleged to have laundered funds by making multiple wire transfers to launder fraudulent card billing proceeds. According to this request a criminal network involved in credit card fraud schemes was using mules to transfer the profits of the illegal business to different parts of the world. The mules were instructed to send money only via money remittance services to hide the origin of the profits.

The undercover agent of country A succeeded to come in contact with one of the leading persons of this network (person C). The undercover agent convinced person C that it is better to use wire transfers through banking institutions instead of money remittance offices. This was done because the authorities of country A were trying to identify persons behind bank accounts instead of mules sending money via money remittance services.

Person C instructed the undercover agent to send money to company's X account in country A. From analysis carried out, it appeared that the money was transferred from country A to country B and most probably to accounts owned by the leaders of organised crime in that country.

Source: Cyprus.

69. The ultimate purpose for structuring transactions is to conceal the true beneficiary of the transaction and the origin of the money. Therefore, another potential risk for the MR/CE provider

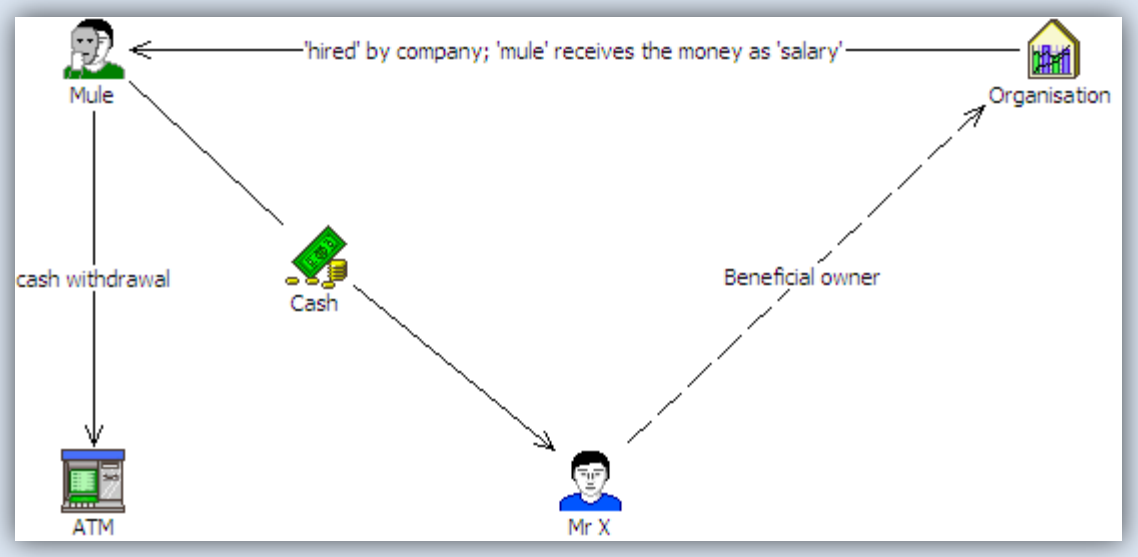
comes from accepting the money of straw men and persons identified on the basis of forged documents. Some examples of money laundering schemes obtained as part of this study involved straw men who were hired as 'employees' of a foreign company.

Box 3. Use of persons hired as employees to launder money originating from internet fraud

Mechanism: money remittance

Red-flag indicators: using 'money mules'

Case description: A person is 'contacted' (for example through the internet) for a job in a company established abroad. The person receives money on a personal bank account as a 'salary', withdraws most of money in cash immediately after the transaction (the 'commission', typically approx. 8% is often maintained in the bank account), and sends the money through money remittance abroad. Typically the true beneficiary of the transaction is a criminal and the scheme is used to launder money originating from internet fraud (phishing).



Source: Cyprus.

70. Yet another commonly reported method involves the use of a third person to transfer funds. Transactions carried out by the customer using (without a reasonable basis) multiple branches or agencies and third parties (for example relatives, minors) on behalf of another person are often aimed at concealing the sender and/or receiver (true beneficiary of the transaction).

71. Another way the MR/CE services may be misused in order to facilitate criminal or terrorist access to the financial system is through schemes with multiple money remittance transactions between persons not directly related. A reporting entity is not always able to effectively determine the connection between the transfers of funds and the related reason of the customer that sends or receives the funds. It is particularly difficult to understand the origin of the money and the scope of the transactions. For example, money transfer transactions initiated over a short time period by several persons to beneficiaries known to be linked to organised crime, executed in certain areas (in case of drug trafficking, in ports, for example), sent to 'dangerous' destinations (known as drug trafficking routes for example) should raise the concern of the remitter. It is often difficult for law enforcement agencies to detect whether the transaction is of a legal nature (for example, persons working abroad and sending income to his/her family via MR services) or as part of an illegal network (forced transactions, for example in relation to prostitution/human trafficking).

72. One of the patterns associated with such schemes also appears to be an indicator of possible ML is receiving transfers from unusually high number of people (often from different countries and in different currencies). The linked nature of the transaction often becomes apparent because several individuals go to the same institutions in the short time period to send money in the same countries and often to the same beneficiaries[20]. These elements usually indicate that the senders and/or receivers may be part of the organised networks[21].

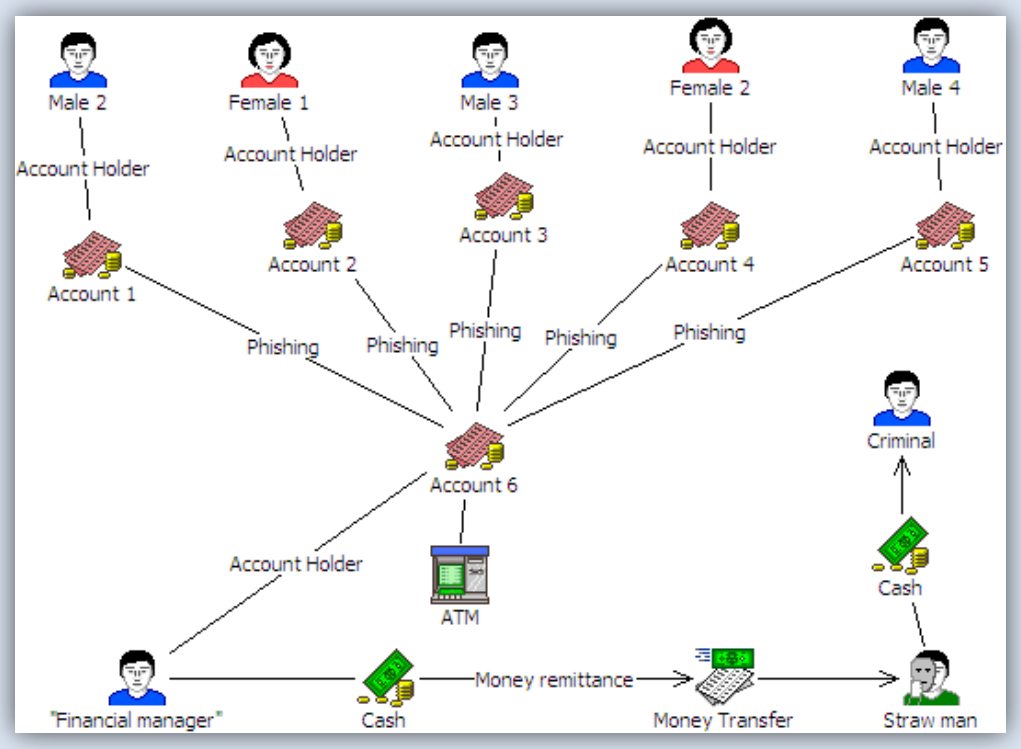
Box 4. Linked nature of the transactions

Customer: individual

Mechanism: money remittance

Red-flag indicators: receiving funds from high number of senders over a short period of time, large-sum transactions compared to person's living standard

Case description: A person is a beneficiary of a great number of remittances (often in relatively small amounts) during a short time period. Sometimes 'mules' are used as intermediaries to make the scheme more complex and harder to follow by the law enforcement agencies. In this case intermediaries re-order the remittances immediately again through the money remitter. Often the value of money remitted does not correspond to senders' economic profile.



Source: Bulgaria.

73. MR services offer widespread and legitimate services to immigrants. They serve the unbanked, provide a convenient, efficient and cost-effective means to send money to an immigrant's home country and often can reach remote areas and locations beset by political instability that are

20 See CTIF-CFI (2003), *pp* 106-107.

21 FATF (2005), *pp* 74.

otherwise outside the networks of the international banking system. However, investigations in some countries have shown that the services provided by some MR businesses have also been linked to human trafficking and the repayment of 'human trafficking agents'. As an example, in certain trafficking cases, money remittance providers have been used to pay mules, intermediaries, airplane tickets, etc.

74. Other ML methods detected in cases involving MR/CE services include transactions with companies incorporated in countries with low or no taxation (no or insufficient AML/CFT measures, known routes for ML/TF, etc.), the use of new payment methods to launder funds, often without a physical presence, and the potential for offshore service providers to access a foreign market online or via a wireless ATM network, evading AML/CFT requirements of jurisdictions.

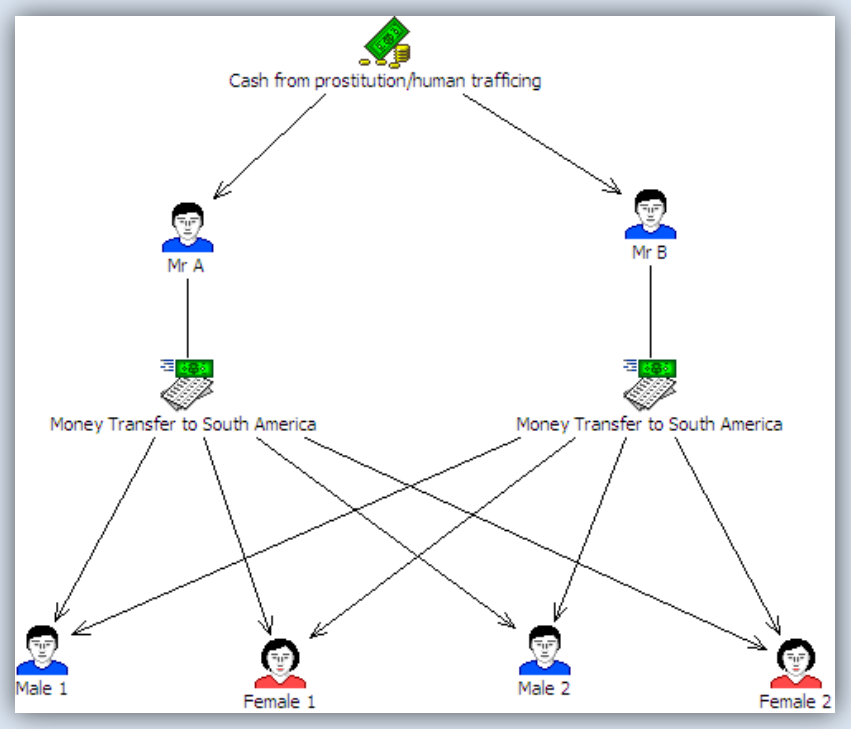
75. The use of forged identity documents is another method commonly identified and which appears to be to be increasingly used. This is particularly difficult to detect by MR/CE providers, especially due to the increasing quality of those forged papers or given that customers are often occasional and the business relationship is not of a continuing nature. False identities are often used to hamper further investigation on the transfers/ operations.

Box 5. Use of false identities

Mechanism: money remittance

Red-flag indicators: structuring, same beneficiaries, a large number of transactions during a short time period

Case description: Persons A and B repeatedly made cash deposits sent via money remittance to South America to the same recipients. In a few months time 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 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.



Box 6. Remittances to high risk countries

Customer: individual

Mechanism: money remittance

Red-flag indicators: structured transactions, several beneficiaries, remittances to high-risk countries, use of straw men, people involved have a criminal background, the volume of remittance is not in accordance of the economic profile of the sender

Case description: The financial intelligence unit received several unusual activity reports from the postal bank regarding money remittance through a well known money transmitter that were done by a number of entities with no apparent relation between them, from country A to several countries in South America.

Analysis of information revealed that a number of 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, which are 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 with one of the South American FIU revealed that one of the beneficiaries was in jail for drug trafficking.

Source: Israel.

2.2 Owners and agents

76. Obtaining an ownership over MR/CE company either directly or via sub-agent relationships provides criminals a perfect tool to manipulate the money transfer system and to launder money. Detecting such cases is particularly difficult for law enforcement agencies, and to a certain extent, it also depends on the capacity of the entity to apply know-your-customer and reporting requirements effectively. Several examples were provided in the survey responses gathered for this research which illustrate cases where the MR/CE company was owned and used by criminal organisations to launder money or where the company was complicit in providing services to an organised group.

Box 7. Use the ownership in MR/CE company to launder money

Mechanism: money remittance company/ currency exchange

Example 1 – Mr B is the owner and CEO of a money service business registered in country A. Mr B engaged in check discounting for a commission. He used the bank accounts of various companies and provided straw men to act as beneficial owners and authorised signatories of the bank accounts. Mr B discounted cheques for his customers using these bank accounts. Mr B made use of the services of other MR/CE service providers which recorded his transactions under another name. He discounted cheques in return for cash for his customers, and in turn, discounts the cheques received from his customers at an MR/CE, with instructions not to record his name so that a report would not be filed. Stolen cheques were brought to Mr B for discounting, and so as not to be connected with them, he gave them for discounting to another MR/CE, which recoded the transaction under the name of a straw man. Mr B instructed the customer to say that he delivered the cheques for discounting to the straw man, and instructed the straw man to say that he received the cheques from a customer, in order to hide his own involvement with discounting the stolen cheques. Mr B was indicted of money laundering offences.

Source: Israel.

Example 2 – Currency exchange business providing services to organised crime group

A currency exchange company in Sweden was identified as providing services for organised criminals. A lot of “runners” came to the exchange office several times a day and made large cash

withdrawals. Some "runners" had during a period of months made withdrawals for millions. The money was used for paying to black labour. STRs were received from banks indicating money flows from different companies' bank accounts to the bank account of the currency exchange-company. The owner of the currency exchange company was later prosecuted and convicted.

Source: Sweden.

Example 3 – Criminal group obtaining ownership over sub-agents of money remitters and exchange offices

Several Bulgarian citizens and companies where the citizens were beneficial owners were involved in large ML 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 FIU detected that a group of Bulgarians bought up sub-agents of MR and CE. After a change in ownership, the total number of transfers received multiplied and a great number of transfers in small sums 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 of a significant scale, involving dozens of natural and legal persons from Bulgaria and foreign countries. The amount of funds transferred through MR system was several millions of Euros.

Source: Bulgaria.

Example 4 - In October 2008, 5 persons pleaded guilty to one count of operating an illegal money remitting business in the US. According to documents filed with the court and statements made in court, persons operated different enterprises. From December 2005 to March 2008, the defendants managed illegal and unlicensed money transmitting businesses in Connecticut. In exchange for remitting a total of more than USD 22 million from Connecticut to Brazil and for guaranteeing the anonymity of both their customer and their customer's intended beneficiary, the defendants took a percentage of the remitted funds for their own financial gain. Several other persons have been pleaded guilty in committing the crimes similar to this, the destination of the transfers have been to Middle East countries.

Source: United States.

Example 5 - Use of agents of money remittance business

A suspicious transaction report from a money remittance business was received in the FIU. The report revealed that one of the agents of the money remittance company was making operations with the following characteristics:

- Every remittance operation was sent to country B (Country B was a drug producing country).
- The amount sent in every remittance operation was higher than usual for money remittance operations to country B.
- In the period of time of one year, the senders of money never made more than three operations.
- Every sender sent money to different receivers.
- There were no apparent relationship between the sender and the receiver of the money.
- The receivers never received money from more than three or four senders.

After making a more comprehensive analysis, other agents of different money remittance companies with similar operational profile were discovered.

Police investigations revealed that those agents were working together in a joint action with the objective to launder money for a drug trafficking organisation. Money laundering and drug trafficking organisations were dismantled. The information was shared with country B, where several police operations were carried out.

Source: Spain.

Example 6 – Ownership of bureaux de change

A suspicious transaction report was received in the FIU. The report revealed that one person owned more than 15 businesses, and three of them were bureaux de change. The characteristics of the operations of the bureaux the change were the following:

- The bureaux de change mainly change European currencies, especially one.
- The amounts changed are higher than usual.
- There is no link between the amount of money changed and holiday periods.

Police investigations revealed that not so many people enter into the bureaux de change and, from time to time, a person made contact with the owner of the bureaux the change and gave him a bag with money in foreign currency. One or two days later the owner of the bureaux de change gave back the money in the local currency to that man. It was also established that the money laundered came from drug trafficking.

Source: Spain.

77. The following indicators could be relevant in this context:

- Reluctance by the MR provider to provide information about customers' identification to relevant stakeholders;
- Use of false identification and fictitious names for customers;
- Frequent transactions or purchases of negotiable instruments slightly under the legal threshold amount in order to avoid filing a STR/CTR;
- Turnover of the MR provider exceeds to a large extent the cash-flows of other comparable businesses;
- Suspicious connections of the MR provider owner; and
- Suspicious transactions performed on the bank accounts of the MR provider or its owner.

78. To deal with these vulnerabilities, most of the jurisdictions contributing information to this study require a 'fit and proper' test to be applied to the owners and managers of the MR/CE service providers at least as a component of a licensing/registration procedure. There are exceptions, as in Chile; Georgia; Hong Kong, China; Japan; and Mexico, where no specific requirements are applied for owners and managers of bureau de change. The most prevalent 'fit and proper' checks include determining that (1) the person has not been convicted for a criminal offence, (2) the person has not been denied the right to hold certain positions/undertake certain activities; and (3) the person has no outstanding tax obligations and not been in bankruptcy for a defined number of years.

2.3 Most common predicate offences identified

79. A number of law enforcement investigations have revealed that MR service providers are frequently used as a vehicle for laundering illicit proceeds. Laundered proceeds in such cases come primarily from drug trafficking, fraud (mainly IT-fraud like *phishing*); economic crimes (document forgery, malfeasance, tax evasion, etc); trafficking in human beings, smuggling of human beings; theft (credit card fraud, currency theft, etc) and smuggling (*e.g.*, tobacco, alcohol, arms). Previous FATF typologies have identified that ML schemes involving these types of crimes often appear to avoid using the banking system, and that systems for money remittance[22] are therefore sometimes specifically preferred as offering less risk of detection.

[22] FATF (2005), *pp* 73.

Drug trafficking

Box 8. Use of MR to launder money originating from drug trafficking

Mechanism: money remittance

Red-flag indicators: large scale of funds transferred compared to the socio-economic profile of the client, frequent transactions to different beneficiaries, transfers to high risk countries

Example 1 - A person made a large number of money transfer transactions to various persons over a short time period. The total amount of funds remitted amounted to a considerable sum of money. It was detected the ultimate beneficiary in the transactions was always the same.

Additionally it was noted that the individual had sent a considerable amount of funds to seven beneficiaries having the same surname as him. The financial intelligence unit noticed that the amount sent to three of them was significant compared to the general living standard of the recipient country. Another remarkable fact was that almost 25% of funds were transmitted to persons in the Netherlands. This could be indicative of an illegal operation to finance human smuggling or drug trafficking.

Source: Malta.

Example 2 – The financial intelligence unit received an STR from a commercial bank about suspicious money transfers through a well-known money transmitter. The report indicated that a group of persons systematically transferred sums averaging between 1000-5000 USD to a Latin American country, and that when conducting the transaction, these persons were always accompanied by an unidentified person. It also indicated that the names of the receivers of funds frequently are recurrent and almost always the same. The analysis established that in a period of 4 months (in 2005), 27 money transfers operations were performed by a group of 13 persons and that the transferred sum amounted to 111 400 USD. It was established links of group: 4 persons had criminal history background, 2 persons were cousins, others lived in the same street.

A special request for further information was sent to the criminal police. Answers received indicated that the persons had links with drug trafficking networks. A joint investigative group was established and with the use of operative and special investigative techniques, it was established that the group was linked to one of the most serious organised crime group. A drug trafficking channel from that country to Europe was identified, where the senders of cocaine are Lithuanian citizens. Cocaine was delivered by ship to ports in Varna (Bulgaria), Saint Petersburg (Russia) and Talinn (Estonia), with the major part of cocaine being delivered to Russia. After the drug deals, all the money was sent to Lithuania, and then transferred through the money transmitter back to Latin America. Overall, transfers were made by about 90 persons (mostly students, asocial persons). The total amount of transfers identified amounted to USD 540 000.

Source: Lithuania.

Example 3 – The financial intelligence unit received 38 STRs made by a money remittance business involving transactions made by 38 persons to Mr A, including relatives and friends of this person. Money received had similar characteristics and circumstances, such as:

- close date of transaction (between January and June of the same year)
- same amount (USD. 6000 and/or USD 5000)
- same country of the sender
- same name of the senders or with variations in their names.

The analysis of the database enabled to identify that persons related to Mr A. had purchased luxurious vehicles in cash; that there was an indirect link with Mr and Ms B, citizens of country Y, who were suspected to be part of a drug trafficking organisation (subject to another financial intelligence report) and that there was a link with the case of Mr C, who has been detected by national and international customs authorities relocating approximately USD 980,000.00

Source: Peru.

Box 9. Use of MR for cross border transfer to "unusual jurisdictions"

Mechanism: exchange bureau

Red-flag indicators: money transmitting by criminals, MR to unusual jurisdictions

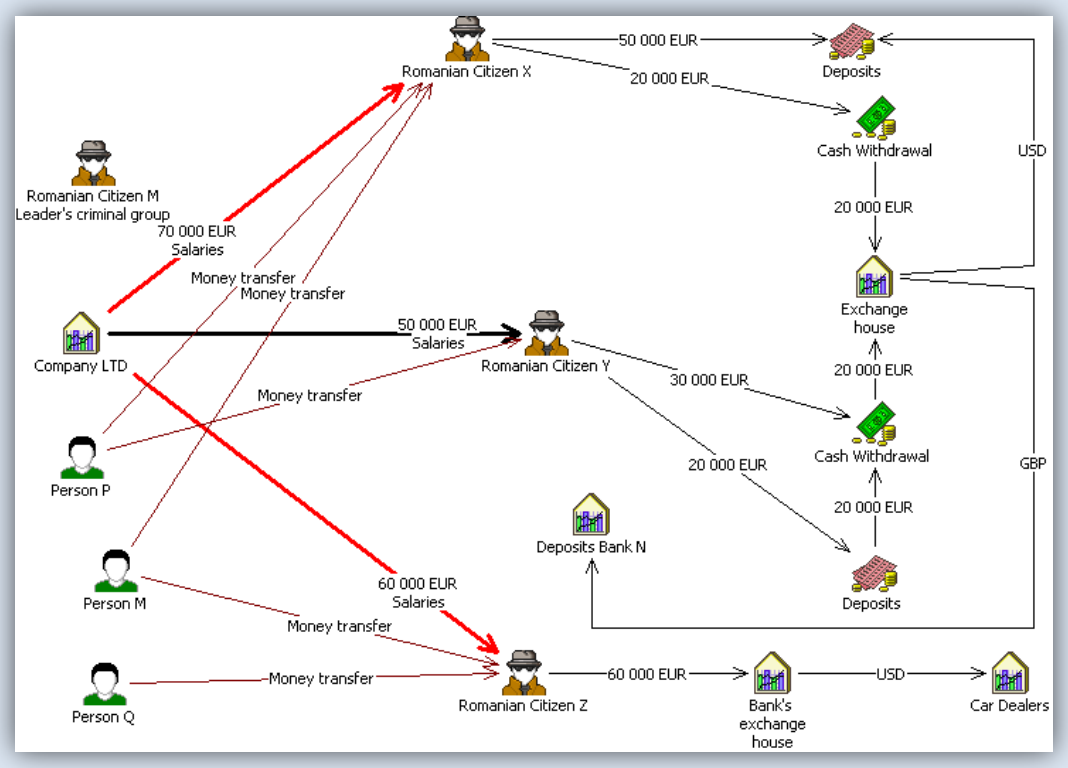
Example – the Romanian FIU received an STR sent by a bank regarding some suspicious cross-border transfers. Thus, three Romanian citizens (X, Y, Z) received small amounts from company LTD (established in country A), justified as "salaries". After receiving money, X, Y and Z used several schemes o launder money, some of which included exchange houses 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 EUR 20 000 in cash, went to the exchange office and changed Euros to USD dollars. At the same day he visited the bank used for receiving money once more and opened bank account where he deposited EUR 50 000. Mr Y withdrew the money received and opened bank accounts in smaller amounts in several other banks, exchange houses were used to change the currency. Mr Z changed EUR 60 000 in Bank's exchange house (whereas X and Y used private exchange houses) and used it to buy cars.

Suspicious elements:

- Cross-border transfers consisting in small amounts under the reporting threshold
- Frequency of cross-border transfers

In a short period of time amount received by the Romania citizens was around EUR 180 000.

The request of information was sent to country A and 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 originated by X, Y an Z was 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 document in order to transfer money to Romania. It was also detected that X, Y, Z travelled to country A occasionally, but none of them worked or obtained legal income there. X, Y and Z could not prove that they worked or obtained any legal income from country A, they could not explain the large amount of money that were transferred to their accounts.



Source: Romania.

Fraud

80. The "advance-fee fraud is a classic scheme but still successful in many cases. Typically an e-mail is sent to victim where cash is promised (for example, "you won the lottery" or "please help us conduct a transaction"). The e-mail also indicates that certain costs must be paid before the winnings can be awarded and/or the transaction can place. In addition to bank transfers, money remittance agencies and agents of known money remitters (Western Union, MoneyGram, etc) are often cited as the means to effect the necessary payment. After the victim has transmitted the money, the criminals disappear, and of course the victim does not receive any reward. A variation of this type of fraud occurs when the fraud involves the offering of some sort of product or service.. In the case of dating scams, for example, fictitious profiles are created by the criminals on internet dating web sites. Through these fictitious profiles, the criminals gain trust of the victim and ask him/her to send money, for various expenses, such as plane tickets, family aid, etc. Often the potential victim is requested to send the funds through money remitters.

Box 10. Fraud

Mechanism: money remittance

Red-flag indicators: cost of receiving the winnings is asked to pay beforehand

Example - Telemarketing fraud using MR/CE service providers to launder the proceeds

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 laundered who transferred them to MR/CE service providers in country A and territory B. The cheques were discounted and deposited in the MR/CE service provider's own bank accounts. The cheques were then sent to be cleared in the foreign banks from which they were drawn, at which time their source was revealed.

Source: Israel.

Trafficking in human beings and migrant smuggling

Box 11. Trafficking in human beings and migrant smuggling

Customer: individual

Mechanism: money remittance
Red-flag indicators: large number of transactions to the same beneficiaries, the person does not hold any bank accounts

Example 1 - An individual A residing in an Eastern Europe country received hundreds of funds transfers usually in small amounts through an MR/CE service provider initiated by more than 35 women of the same nationality as individual A. Typically the number of remittances initiated by one person was small (four on average). The addresses disclosed by the women referred to different hotels situated in Paris. Most of the women did not have a criminal record and did not hold a bank account. One of the women however had opened bank account in France and indicated as her address the address of a company whose manager was convicted for aggravated procurement some years ago.

The case was transmitted by Tracfin to the judicial authorities on a presumption of involvement in the procurement of prostitutes.

Source: France.

Example 2 - **Use of MR to launder the money from prostitution mediating**

The Cypriot financial intelligence unit in co-operation with the Cyprus Police conducted an investigation in relation to the activities of a lady from Asia working in Cyprus for the last eight years as a housekeeper. According the facts of the case and to information obtained from the Police, suspicions were raised that she was a prostitute. Co-operation with all the local and international financial institutions in Cyprus revealed that she did not hold any bank account in Cyprus. Further co-operation with all the Money Remittance offices in Cyprus revealed that she used MR instead. From analysis and investigation carried out from the information obtained from the Money Remittance Offices she sent a significant amount of money outside Cyprus. She also collected and sent small amounts of money from other nationals, women that according to information from the police were also involved in prostitution activities. According to the analysis the suspect sent money to her country and also to both E.U. and non-E.U. countries to different persons each time. The funds that she sent did not correspond with her salary.

Source: Cyprus.

Example 3 - A suspicious transaction report from a money remittance business was received in the FIU. The report revealed that different women were sending money to the same country. Most of the operations were sent to the relatives of the senders, but sometimes one or two operations were sent to two different persons (A and B) in the destination country in amounts higher than usual. After a first analysis other groups of women with the same operational profile were discovered and it was noticed that A and B also were receiving money from them.

A police investigation was undertaken which established that the senders were women that were working in prostitution activities and that the money sent to A and B was to pay the debt to the illegal immigration organisation in the country of origin.

Source: Spain.

Terrorism

Box 12. Terrorism

Mechanism: money remittance

Red-flag indicators: money transmitting by criminals, MR to unusual jurisdictions

Example 1 - Mr X was a defendant of operation CREVICE, a case concerning the purchase, transportation, concealment of fertilizers for use in the construction of an improvised explosive device. Mr X was found guilty in 2007 of conspiracy to murder and conspiracy to cause by an explosive substance an explosion of a nature likely to endanger life or cause serious injury and damage to property. He was sentenced to a custodial sentence of forty (40) years. Between 07/11/03 and 12/11/03 Mr X withdrew GBP 2540 (sterling) in cash from his Barclays Bank PLC account. On 12/11/03 Mr X sent £2471 to person Y in Kharian, Pakistan via UK Western Union money transfer, converting to 233,326.5 rupees. Mr Y is a US citizen and was arrested by the FBI in April 2004. He pleaded guilty to committing terrorist offences and was sentenced to a custodial sentence of seventy (70) years.

Source: United States.

Example 2 - In November 2008 a Pakistani national Mr X residing in the US was sentenced to 110 months in prison, followed by three years of supervised release, for conspiring to launder money and for concealing terrorist financing. He was also ordered to forfeit assets worth USD 2 208 000. Mr X operated company A, Inc., a money remitting business in Washington, D.C. Mr A, company X, Inc. and five other defendants allegedly conspired to launder over USD 2.208 million received from a cooperating witness working with ICE and FBI agents. The money was purported to be the proceeds of drug trafficking, terrorist financing and trafficking in contraband cigarettes.

Source: United States.

Example 3 – Between 2000 and 2007, Mr. A received 102 money transfers of a total amount of USD 203,768.91. During the same period, Mr. A sent 120 transfers abroad for USD 107,000.00. to various countries, primarily to the United States, Ecuador, Colombia, Guatemala, Mexico, India, Egypt and

Bolivia. Mr. A has been detained in 2007 by the authorities for being related to an alleged international criminal organisation responsible for smuggling persons illegally to the United States. Several persons coming from countries such as Malaysia, China, Korea, India, Iran, Irak and Egypt were sheltered in Peru by Mr. A and his local associates. Then, they followed the route to the United States through Ecuador, Guatemala and Mexico. According to the Peruvian police, there is a possible link between Mr. A and a member of the terrorist group, who is detained in Venezuela. Among indicators having triggered the suspicion was the fact that there was no link between the person making the transfers and the variety of countries to which transfers were being made.

Source: Peru.

2.4 Informal money remittance services

81. Informal money remittance systems can be used to send money around the world. They are often linked to a certain geographical region and go under specific names such as *hawala*, *hundi*, or *hawilaad*, depending on the geographical or cultural links of the persons who establish or use them. These are underground 'banking' channels in which the transactions are settled by offsetting an equivalent some at the receiving location. The transfer request is made in one location (where funds the funds to be transferred are received). The counter value is then distributed to a beneficiary at another geographic location through one of the network's correspondents. These systems have numerous advantages: they are quick, discreet and reasonably priced, which makes these services attractive for both legal and illegal use. In recent years it has become clear that informal money remittance systems play an important role in international terrorism financing and that they are a suitable medium for terrorists to transfer money[23] .

82. Detecting these underground systems is by definition very difficult. In countries with alternative money remittance systems, it is often difficult to prove illegal activities in these systems as they are often trust-based, secretive and unregistered, with indirect fund movements. It is therefore difficult to assess the degree of compliance even when informal value transfer service providers are legal. In most countries having experience with such systems, informal remittance services are illegal. In others (Denmark, Sweden, United Kingdom, and United States, and in some cases in Germany), their activities are regulated by the AML/CFT regime.

83. Underground remittance activity, particularly that which is carried out by immigrants, serves a legitimate need, but also offers a potential for misuse for ML/TF purposes. For instance, due to the lack of effective monitoring, anonymous customer transactions can take place and customer's beneficial owner can be hidden.

84. To guarantee that informal systems are not operating in an unregulated manner, the safeguards below are often used:

- Adoption of legislation, in compliance with FATF SR VI, requiring the licensing and/or registration of MR/CE services.
- Regulating the operations of the MR/CE services, including licensing and /or registration, identification and awareness-raising, the adoption of AML/CFT laws and regulations, monitoring of compliance with those laws and regulations; and creation and implementation of a sanctions regime.
- Implementation of an effective currency transaction report and suspicious transaction report system, which includes effective analysis by a supervisory agency that cooperates with law enforcement. Non-registered MR/CE services are often identified through

23 FATF (2003), *pp* 11

reports by other currency suppliers under the reporting regime; by tip-offs made to the supervisory agency; and by analysis of information coming to the supervisory agency's attention either from its own staff/activities or from that of other law enforcement/regulatory agencies.

- Effective supervision by regulatory authorities (on-site inspections; oversight over high volume/ number remittances with no apparent economic substantiation, risk-based examinations, timely law enforcement actions, etc.) and close co-operation between supervisory and law enforcement authorities.

85. Several countries, such as Austria; Hong Kong, China; France; Germany; Netherlands; Spain; and the United States indicate that they have prosecuted individuals for criminal activities related to informal money remittance service. As illustrated in the examples below, the reporting parties can play a very important role in this detection.

Box 13. Use of Informal MR System

Mechanism: informal money remittance system

Example 1 - An East African residing in Belgium, Mr X, stated that he performed Hawilaad banking activities. His account was exclusively credited by cash deposits and numerous transfers in small amounts. During several months the funds were transferred to company A in Eastern Africa. Shortly afterwards the funds were transferred to company B in Western Europe. Companies A and B performed money remittance transactions around the globe. Mr X claimed that he performed Hawilaad activities for fellow countrymen wishing to send money to Eastern Africa. However, he did not hold any position within Belgian companies and he was not registered as manager of an authorised exchange office. The individual did not have an authorisation from the CBFA (banking supervisor) either. Police sources revealed that he was known to be a member of a terrorist organisation. In this case the alternative remittance system may have been used for terrorism financing. The police are investigating.

Example 2 - In September 2008 Mr X, a Pakistani national residing in Canada, pleaded guilty in the U.S. to conspiring to launder money. According to his guilty plea, Mr X operated a money transfer business in Montreal, Canada to transfer monies abroad through an informal money transfer system called a "hawala," using a network of persons and/or businesses to transfer money across domestic and international borders without reliance upon conventional banking systems and regulations. A cooperating witness, acting at the direction of law enforcement, held himself out to Mr X and his associates to be involved in large scale international drug trafficking and international smuggling of counterfeit cigarettes. From January 2004 to November 2005, Mr X assisted co-defendant Mr Y in 10 hawala transfers from the U.S. totalling USD 828 000 in U.S. currency provided by the cooperating witness. The cooperating witness represented that the monies sought to be transferred were the proceeds of drug trafficking, and Mr X laundered these funds believing they were to be used to support those activities.

Source: United States.

CHAPTER III - KEY FINDINGS

4.1 Assessing ML/TF risks and threats within the MR/CE sector

86. Based on the analysis of information provided through the survey, the project team identified certain potential vulnerabilities in the money remittance and currency exchange sector.

Assessments by competent national authorities

87. From the responses received, it appears that so far only a few countries have conducted assessments of ML/TF risks or threats in the MR/CE sector[24]. Countries where the risk assessments have been made and where the risks have thus explicitly addressed can be divided into two groups:

- Countries where the financial intelligence unit assessed the ML/TF risks posed by money remittances and currency exchange (Bulgaria, Estonia and Poland, for example). These risk assessments are mainly based on analysis of suspicious transaction reports and the results of law enforcement actions.

- Countries where the national risk assessment was performed on an interagency basis (Netherlands, Spain, and the US, for example).[25] In these assessments, the expertise of the FIU and the investigative authorities was used; however, significant involvement from other relevant stakeholders (representatives of the private sector, scholars, etc) also occurred.

88. In conducting risk analysis for the MR/CE sectors, it appears that such analysis cannot be done solely by looking at individual STRs. Whilst relevant disclosures usually capture specific remittance transactions, this approach lacks a more strategic perspective that could help identify relevant flows and trends. A proactive approach appears to be needed that will allow the evaluation of relevant flows, coupled with the consideration of socio-economic factors such as the distribution of immigrant communities, the destinations of remittances, the extent and features of the informal sector, the strategic location of the country, etc. This appears to be an advantage that the interagency approach can provide.

89. In addition to the STRs, intelligence developed by those authorities with supervisory responsibility over the MR/CE sector has proven to be valuable source of information when analysing the potential threats and new and emerging trends.

90. The national experience derived from identified ML/TF schemes in which money remittance and currency exchange providers were involved (the intelligence emerging from STRs analysis) can

---

24 For a detailed overview of the ML&TF threat assessments in FATF member states, please refer to FATF (2008b).

25 In the US, the National Money Laundering Threat Assessment conducted in 2005 as an inter-agency initiative included MSBs as well as online payment systems, informal value transfer systems, insurance companies, trade-based ML and bulk cash smuggling. The U.S. published a follow-up national strategy in 2007.

contribute to reviewing the legal framework at national level (and supranational/ EU level as well) to guarantee the effectiveness of the system in the light of the new services.

91. For example, in Germany and the UK[26], a periodic overview of the AML/CFT threats posed by MR/CE businesses is published. The overview contains up-to-date information on threats and trends identified on the basis of STRs.

92. A specific example is related to the assessment of risks posed by the introduction of the euro. Of the FATF and MONEYVAL member States from the euro zone, the information provided indicated that only five countries had conducted an assessment of the related ML threats[27]. The scope of each risk assessment varied substantially, while in some countries a special committee was set up that co-ordinated the risk assessment and management, in other countries the process was rather informal.

Box 14. Examples of experiences in assessing risks posed by the introduction of the euro

In the Netherlands, the ML threat assessment was addressed by an official working party which was established by the Dutch Ministry of Justice. Typologies and risk indicators were developed from the results of this working party.

France set up a task force at the national level in 2000, coordinated by the FIU (Tracfin) and comprising representatives of the judicial police, the customs, the Bank of France and the banking supervisor. The task force was in charge of conducting risk analysis, raising awareness and coordinating prevention and detection of suspicious transactions in relation with the adopting euro. At the international level, Tracfin invited its EU counterparts concerned by the adoption of the euro to a meeting in 2000 to ensure the best and timeliest co-operation in exchanging information, on the basis of MoUs already signed or via the Egmont secure website. A contact person was designated in each of the twelve FIUs to deal specifically with any transaction and information related to the Euro.

In Italy the ML/TF risk assessment of adopting euro was analysed in-depth and involved both reporting entities and competent authorities. Indications were provided to reporting entities for the detection of possible suspicions, particularly related to the need to convert cash or other means of payment of illegal origin into the single currency within the set deadline. A peak of disclosures was registered in the change-over phase, leading to the detection of possible illegal financial transactions. Together with instances of money laundering, several cases of fiscal violations were identified.

In Malta, the FIU specifically addressed the ML threat to MR and bureaux de change in the period preceding the adoption of the euro. It carried out an assessment of the legislation in force at the time and consulted its EU counterparts, both in the euro area and prospective members of the euro area. The assessment revealed that the AML/CFT measures in place were sufficiently effective and there was no need to introduce additional measures. The FIAU recommended that only credit and financial institutions (as defined under Maltese law) be authorised to exchange Maltese liri into euro. Moreover the FIAU established a set of ad hoc guidelines for CDD for all financial and credit institutions. These guidelines directed mainly to credit institutions and money remittances/bureaux de change require, *inter alia*, to identify all persons requesting to exchange currency and any other person on whose behalf the person was acting, encourage the general public to deposit any amounts of cash into existing or new bank accounts prior to changeover, strictly comply with existing record keeping and reporting obligations and prepare staff by providing intensive training on AML/CFT procedures. Also, further to adopting the euro on 1 January 2008, a National Euro Changeover Committee was set up to

26 The UK threat assessment of organised crime 2009-2010 (SOCA (2009), *pp* 11) indicates that money service businesses (MSBs), which include bureaux de change, money transmission agents and cheque cashers, are frequently used by organised criminals to launder the proceeds of crime. Criminals may make small value transactions in high volume through legitimate MSB outlets that are not aware that their services are being abused, while complicit MSBs knowingly facilitate large volumes of currency exchanges on behalf of criminal customers.

27 The FATF examined the money laundering implications of Euro introduction in its 1998-1999 and 2001-2002 typologies reports.

oversee the process, in which the FIU was actively involved in this Committee

Although the UK is not a member of the euro zone the country has considered the specific ML threats associated with the introduction of the euro; UK experience has been that, as anticipated, demand for the 500 euro note in the MR/CE sector has been high (for smuggling/bulk reduction); UK reporting sectors were alert to the possibility of large quantities of stored legacy currencies surfacing for exchange, but there were few STRs about this in the event (and most were tax evasion focused).

93. Responding countries indicated that the ML/TF threat in the sector was primarily a result of both the direct penetration of organised crime group into operations of MR/CE providers and of the lax implementation of AML/CFT standards.

94. The absence of a formal risk assessment of the sector however does not mean that the vulnerabilities of the MR/CE have been completely ignored however. Several countries, where the risks to the sector have not yet been addressed through a national risk assessment emphasised that competent authorities constantly monitored the sector to identify the possible risks and vulnerabilities, meet to discuss the problems, and share their experiences.

4.2 Additional measures to be considered at national and international level

95. ***Knowledge of the sector, services offered and transaction channels***: Responses received point out that competent authorities in many countries do not have a comprehensive picture of the MR/CE sector and the services provided. The sector is very heterogeneous and remittance service providers innovate and evolve in developing new transaction channels. In certain jurisdictions, regulators do not engage in a continuous dialogue with MR/CE providers, thus they do not have a clear picture of the sector and measures taken by the businesses themselves regarding the control of their agents, of audit plans, how often agent locations are visited, the turnover of operators, etc.

96. ***Guidance and training*** **–** Money remittance and currency exchange providers tend to lack the capacity, experience and resources to implement AML/CFT requirements. Therefore regulators and/or supervisors have a key role to play in providing appropriate guidance to MRs and CEs. In this regard, adequate guidance for detecting false documentation appears to be a recurring issue of concern.

97. ***Implementation of CDD measures*** – Especially in countries where the AML/CFT legislation concerning MR and CE service providers is still relatively weak and developing (mostly due to the fact that countries are in the process of introducing the AML/CFT rules that are in accordance with international standards, such as in many countries of the former Soviet Union), the main problem found was weakness in implementing the necessary safeguards and control mechanisms relating to customer due diligence requirements (including adequate red-flag indicators for obligated persons). Because of the absence of durable relationships with customers and the nature of transactions, money remitters and currency exchange offices find it particularly challenging to perform ongoing monitoring with a view to detect anomalies and risk profiles.

98. ***Licensing / registration systems*** – Countries have not always clearly designated the regulatory or other authority to license and/or register MR/CE service providers and to monitor such business activity. When designation has occurred sometimes the licensing and control authorities are split between two agencies which can lead to weakness on oversight of the MR/CE.

99. The data gathered through this research did not permit a conclusion to be drawn on linkages between the abuse of MR/CE services and the type of regulatory framework, for example, whether the jurisdictions with a registration regime as opposed to a licensing regime tend to face more cases of the misuse of MR/CE services or whether jurisdictions with a higher threshold on CDD for wire transfers observe higher cases of abuse.

100. ***Supervision*** – The level of vulnerability of the MR/CE sector to misuse for ML and TF was found to be rather high, with some countries indicating high levels of non compliance. There appeared to be in some cases a lack of understanding on the particular nature of the MR/CE sector that make it vulnerable to misuse for ML/TF purposes.

101. ***Fit and proper*** – As described in Section II there is a risk in some instances that MR/CE operators or agents may be owned by criminals and that an adequate 'fit and proper' test should rule out as effectively as possible. One possibility used in some countries is the regular registration renewal obligation. This has helped to detect attempts at controlling the businesses and/or agents.

102. ***Agents*** – The monitoring of agents and sub-agents of MR/CE service providers appears to be lacking in some instances. Weakness in this area provides for a potential 'loophole' whereby agents might operate at 'arms length' on behalf of other CE service providers and/or are not subject to the 'fit and proper' test. The role of smaller and local players should not be underestimated.

103. ***Reporting systems –*** The implementation of reporting requirements, including the threshold-based reporting system, appears to have contributed to detecting ML in the MR/CE sector. It is noted that in several responding countries, MR/CE service providers rank among the top five in numbers of transactions reported as unusual or suspicious. In others, reporting in this area remains rather low, which may be explained by a variety of reasons (size of the sector, recent introduction of the reporting requirement, low understanding of the STR requirements).

104. ***Law enforcement action –*** The number of referrals, prosecutions and convictions based on STRs received from the sector appears to differ greatly from one jurisdiction to another. However overall, a discrepancy can be noted between the number of referrals and the number of prosecutions. The information gathered indicated that the law enforcement in many jurisdictions is unable to gather sufficient information upon which to act, mostly due to incomplete or insufficient records, and in some cases falsified ones. Following the money trail and seizing assets are a often a real challenge, and it may be impractical to focus on the individual MR/CE transactions between customers, rather than on the elements and data that the operator needs to collect and provide to the law enforcement.

CHAPTER IV – ISSUES FOR FURTHER CONSIDERATION

5.1 Assessing ML/TF risks and threats within the MR/CE sector

105. A non exhaustive list of issues and areas were identified by the project team as requiring additional efforts, in order to ensure that ML/TF risks are adequately addressed in the money remittance and currency exchange sector.

Assessments by competent national authorities

106. As indicated in the previous section, few countries have conducted assessments of ML/TF risks or threats in the MR/CE sector, and in certain cases, the analysis that has occurred has not taken been at a such a level that would help to identify related money flows and trends. It therefore seems logical that countries should be encouraged to carry out studies of their respective MR/CE sectors – using a strategic approach that integrates information and experience from a variety of sources – so as to better understand MR/CE activity and its potential vulnerabilities to misuse for ML and TF.

107. Furthermore, countries should also use their sector-specific threat/risk assessments to help identify gaps in the existing AML/CFT regulatory framework. When conducted on an inter-agency basis, national level assessments may derive the maximum benefit of the knowledge from different authorities, and the results can then be used as another input in the development of an overall national AML/CFT strategy. A sectoral risk assessment should not be just a one-off initiatives but rather on a continuing basis. Countries may want to consider the following factors, as noted in *FATF Risk-Based Approach: Guidance for Money Service Businesses* (FATF (2009)), when conducting a risk assessment:

- Political and legal environments.
- Country's economic structure.
- Cultural factors and the nature of civil society.
- Sources, locations, and concentrations of criminal activity.
- Size of the financial services industry.
- Ownership structure of MR/CE service provider.
- The scale of and type of business done by unregistered or unlicensed MSBs.
- Corporate government arrangements at MSBs and in the wider economy.
- The nature of the payment systems and the prevalence of cash-based transactions.
- Geographical spread of financial industry's operations and customers.
- Types of products and services offered by the financial services industry.

- Types of customers serviced by the industry.
- Types of predicate offenses.
- Amounts of illicit money generated domestically.
- Main channels or instruments for laundering or financing terrorism.
- Sectors of the legal economy affected.
- Underground areas in the economy.

Assessments by the MR/CE sector itself and measures at service provider level

108. It is also essential that MR/CE service providers assist in identifying, assessing and managing ML/TF risks associated with their products, services, customer groups, and geographical location. ML and TF risks should be assessed on a regular basis at a company level to ensure that the AML/CFT measures applied are up-to-date and appropriate. AML/CFT procedures to manage and mitigate these risks also need to be constantly under review and implemented.

109. It makes sense that MR/CE service providers should implement a risk-based approach that takes into account the particular ML/TF risks that their sector faces also in terms of the different players (for example, concerning MR/CE agents) and that they implement appropriate controls for higher-risk situations. On this issue, the FATF guidance on the risk-based approach lays out some of key factors and issues that should be considered by both the public authorities and the MR/CE service providers when implementing. For example, the guidance states that these businesses should pay particular attention to categories of customers that may indicate a higher risk, including:

- Customers conducting business or transactions in unusual circumstances;
- Customers who are politically exposed persons;
- Non face-to-face customers;
- Customers who structure their transactions;
- Customers who wire money to online gambling sites or high-risk jurisdictions;
- Customers who use agents or associates to hide beneficial ownership;
- Customers who know little about or are reluctant to disclose details about the payee;
- Customers or parties with no apparent ties to the destination country;
- Suspicion that the customer is acting on behalf of a third party but not disclosing that information;
- Transactions involving charities and other non profit organisations which are not subject to monitoring or supervision, like cross-border charities;
- Customers who have been subject of a law enforcement enquiry known by the MBS;
- Customers who use false identification;

- Customers who offer different identifications or identifiers on different occasions;
- Customers who receive transactions in a pattern consistent with criminal proceeds; and
- Customers who receive transfers in seasonal patterns consistent with criminal proceeds.

110. Regarding transactions conducted by MR/CE businesses, it is essential that there be control mechanisms that will permit the identification of any money flows or customers warranting closer scrutiny. This should also apply in cases of single-person businesses. In larger MR/CE businesses, the person responsible for compliance with AML/CFT measures should ensure that internal monitoring processes provide for effective controls and readily available information concerning, inter alia:

- Who approaches as a customer, how often, when, from where, remitting or receiving how much, and the probable and plausible rationale for that;
- Many customers sending to one beneficiary;
- One customer sending to several beneficiaries (and other similar schemes);
- The use of data and IT to scan for patterns of transactions.

111. There are a number of other areas which should be considered carefully by the MR/CE service providers. For example, the background of the employees should be carefully checked. Also, at the company level, it is important that employees regularly receive appropriate training on AML/CFT measures. Such training should ensure not only that they understand their responsibilities but also have sufficient knowledge to detect any suspicious activity. For this purpose, written compliance procedures are of paramount importance. Also, other issues include the need to prevent situations when data/ input by operators could be insufficient, incorrect or subsequently modified fraudulently without any possibility to track subsequent changes, which would impact on the usefulness or accuracy of the information kept by the MR/CE service providers.

5.2 Additional measures to be considered at national and international level

112. ***Knowledge of the sector, services offered and transaction channels***: There is clearly a need for competent authorities to understand fully how the sector operates and the services it provides, as well as developments in the sector, which could be exploited for ML/TF purposes. In order to further solidify understanding of the MR/CE sector along with its vulnerabilities, regulators should therefore engage in a continuing dialogue with MR/CE providers. Such a dialogue would also make them more aware of the measures that some service providers themselves already take to oversee the activity of their agents as far as compliance with AML/CFT measures.

113. ***Awareness raising*** – Outreach to the MR/CE sector, generally, to explain and reinforce AML/CFT obligations, as well as to enhance industry supervision, is important. Making the general public more aware of the need for AML/CFT measures to be applied to MR/CE services can be equally important however. Such awareness raising may assist in building trust in the regulated system and thus help to foster the use of the system rather than underground or unauthorised means for the movement of funds.

114. ***Guidance and training*** – Since many MR/CE service providers tend to lack the capacity, experience and resources to implement AML/CFT requirements, regulators and/or supervisors have a key role to play in this process by providing adequate guidance to the sector. Given the specific nature MR/CE activity where adequate knowledge of the customer is heavily reliant on effective

identification and record keeping procedures, training on the detection false documentation could be especially useful.

115. ***Licensing / registration systems*** – Countries should clearly designate the regulatory authorities delegated the authority to license and/or register MRs/CEs and to monitor MR/CEs. Due to the particular nature of the services they are providing, it is highly beneficial for the same institution to license or register and supervise them. The institution authorised to issue licenses or registering the MR and CE service providers should have access to public as well as restricted information. Often the information held in databases that have a restricted access (for example, police databases) is of great value. As indicated in the previous section, the advantages of one type of regulatory framework (licensing or registration) over another could not be determined by this study. This issue may be worth exploring further.

116. ***Supervision*** – Given the high vulnerability of MR/CE activity to ML and TF, reinforcing supervision should be considered as essential to prevent and deter the misuse of such businesses. Training should enable the staff of relevant supervisory authorities to assess the quality of internal procedures of MR/CE service providers. It should also enable them to determine whether or not risk management policies and processes are appropriate in relation to the business's profile and whether senior management has adequate risk management policies along with the necessary procedures and controls.

117. ***Fit and proper*** – It is vital to have an appropriate 'fit and proper' system in place to effectively identify the true beneficial owner of a company and to guarantee that MR and CE providers do not operate in an unlawful manner. The 'fit and proper' control should be of a continuous nature to effectively rule out any cases where the company is controlled by criminals. Using a regular registration renewal obligation is one way that this might be implemented.

118. ***Agents*** – There should be ongoing scrutiny and monitoring of agents and sub-agents of MR/CE service providers. Whether this can be achieved by a regulatory requirement on principals to undertake more detailed background checks on their agents, or the inclusion of agents within the requirements should depend on the particular circumstances of the country.

119. ***Reporting systems –*** The detection of ML/TF activity in the MR/CE sector can be improved only if reporting requirements, including the threshold-based reporting systems, are implemented effectively. Given the risk of receiving too many (or too few) STRs from the sector and in order to avoid over-reporting in threshold-based reporting system, automatic or semi-automatic control mechanisms could be integrated into the databases of the authority that collect such information.

120. ***Information sharing*** – The legal framework should clearly define information-sharing responsibilities between the regulatory authorities, law enforcement agencies, and the private sector. Information exchange between the public and private sector is essential for an effective national ML strategy to function.

121. ***At international level –*** Closer cross-border co-operation has sometimes found lacking in this area. MR/CE business activity by its nature often involves persons and activities (as well as currency) from different jurisdictions. MR/CE services are therefore frequently provided by multinational companies. Due to the cross-border aspect of money remittance there is sometimes confusion as to which authority in which country should intervene if suspicious activity is detected. Effective and prompt international co-operation between the law enforcement agencies has proven to be of paramount importance in guaranteeing that such attempts do not remain unpunished. FIU-to-FIU co-operation has proven to be particularly important in this respect, even beyond exchanges on specific STRs.

122. The MR/CE sector provides a service that meets significant and genuine economic needs, and its vulnerability to misuse for money laundering is closely linked to the effectiveness of AML/CFT preventive measures. As with other parts of the financial sector, it may take several years for the AML/CFT regime applicable to money remittance and currency exchange providers to evolve. Moreover, criminal networks often appear able to change their laundering methods more quickly than law enforcement authorities and supervisors can adapt their detection and enforcement capacities. Therefore it is inevitable that it frequently takes time for appropriate legislation to be drafted and agreed upon and still longer for legislation to be tested by the courts and proven to be effective.

123. It clear however that certain measures, if not properly adapted to the specific situation of country, could inadvertently drive the sector further underground, particularly in developing countries where the informal sector is commonly observed. From the regulatory and supervisory perspective, enhancing the level of requirements and controls, while certainly improving the capacity to prevent the misuse of legitimate entities, might in some cases increase the cost of compliance, thus creating greater incentives for marginal businesses to shift to the underground sector, which would then escape from monitoring.

ANNEX 1 – JURISDICTIONS PROVIDING INPUT TO THIS STUDY

Africa		
Egypt *		
Nigeria*		
Americas		
Argentina	Guatemala*	Paraguay*
Belize*	El Salvador*	Peru*
Chile	Honduras*	St Vincent & the Grenadines*
Colombia *	Mexico	United States
Costa Rica *	Panama*	
Asia		
Hong Kong, China	Korea *	Philippines*
India *	Macau, China	Chinese Taipei *
Indonesia *	Malaysia *	Thailand*
Japan		
Europe		
Albania	Greece	Serbia
Armenia	Latvia	Slovakia
Austria	Liechtenstein	Spain
Bulgaria	Lithuania	Sweden
Croatia	Italy	"The former Yugoslav Republic of Macedonia"
Cyprus	Malta	Turkey
Denmark	Moldova	Ukraine
Estonia	Monaco	United Kingdom
Finland	Netherlands	European Commission
France	Poland	
Georgia	Romania	
Germany	San Marino	
Middle East		
Qatar *		
Syria*		
United Arab Emirates *		

* Provided answers to the short version of questionnaire through the Egmont Group.

ANNEX 2 – LIST OF INDICATORS OF POTENTIAL MONEY LAUNDERING ACTIVITY

This section attempts to feature indicators which appear in the selected case studies in this report as well as additional indicators which have been developed in responding jurisdictions to assist anti-money laundering and counter-terrorism financing officers to identify and describe suspicious behaviours for inclusion in suspect transaction or suspicious matter reports. This is a non-exhaustive list. It should also be noted that the single indicators by themselves may not necessarily be linked to money laundering, as some indicators may be typically be found for many money service businesses not facilitating illicit finance.

1. Indicators for all money remitter and currency exchange (MR/CE) service providers

Transactions

- The transaction seems to involve unnecessary complexity.
- Use of front men and/or shell companies.
- Transactions in a series are structured just below the regulatory threshold for due diligence identity checks.
- The customer appears to be trying to avoid reporting requirements by using two or more MR/CE locations or cashiers on the same day to break one transaction into smaller transactions.
- Two or more customers appear to be trying to avoid reporting requirements and seem to be working together to break one transaction into two or more transactions.
- Transactions are carried out by the customer on behalf of third parties without there being an appropriate business relationship with such parties.
- Frequent transaction orders are made by the same client
- Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.
- An unusually large (cash) transaction.
- The amount of the transaction is unusually large for the typical customer or for the MR/CE.
- The transaction has no apparent purpose or no obvious economic/financial basis.
- Unnecessary routing of funds through third parties.
- The customer uses intermediaries which are not subject to adequate AML Laws.
- A customers sends/receives funds to/from him/herself, for no apparent purpose.

- There is no genuine reason for the customer to use the services of an MR/CE business.
- Transfers of large sums of money to or from overseas locations with instructions for payment in cash.
- Customers send or receive (regular) payments from countries which are regarded as "tax havens" or non co-operating.
- One legal/natural person transfers sums to many legal/natural persons.
- One legal/natural person receives sums from many legal/natural persons (from various countries).
- Many legal/natural persons (who have no obvious blood/business relation) are beneficial owners of transfers ordered by one legal/natural person.
- An under-aged person receives funds from many legal/natural persons and/or from different locations.
- A customer sends/receives funds to/from counterparts located in jurisdictions which are known to be exposed to risks of, *i.e.* drug trafficking, terrorism financing, smuggling.
- Non face-to-face customers are not physically present for identification purposes.
- Transactions are accompanied by information which appears clearly false or contradictory.
- The customer is unwilling to provide routine information when requested or the information provided is insufficient, false, or hard for the MR/CE to verify.
- No or limited information about the origin of funds.
- The explanation for the business activity and/or the funds involved is not credible.
- Electronic transfers involving large sums of money does not include data allowing for the clear identification of such transactions.
- Rounded deposits of funds are followed by like-amount wire transfers.
- The customer is accompanied by others who keep a low profile or stay just outside.
- The customer reads from a note he apparently did not write himself.
- The customer receives instructions from others.
- The customer appears to be in doubt when asked for further details.
- Difficulty in obtaining details of the beneficial owners.
- No relationship between sender and beneficiary.
- Operations are irregular.

- The supporting documentation does not add validity to the other information provided by the customer.
- The customer is in a hurry to rush a transaction through, with promises to provide the supporting information later.
- The customer represents a business but seems to have no business experience.
- Authority for others to withdraw funds does not seem to be well-founded.
- Correspondence is to be sent to another person than the customer.
- The customer needs information on what has been deposited in the account before a large cash withdrawal or transfer to abroad.
- Form is filled in advance.
- The pattern of transactions has changed since the business relationship was established.
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings.
- Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.
- Instruction on the form of payment changes suddenly just before the transaction goes through.
- The customer, without a plausible reason, repeatedly goes to agents located far from his/her place of residence or work.
- Funds are sent at a time not associated with salary payments.
- Remittance sent outside migrant remittance corridors.

For cash transactions

- Unusually large cash payments in circumstances where payment would normally be made by cheque, bank draft, etc.
- Cash is in used notes and/or small denominations (possible indication that the money originates from the criminal offence).
- Customer refuses to disclose the source of cash.
- Customer has made an unusual request for collection or delivery.
- Banknotes brought by customer are in small denominations and dirty; stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty are, packaged carelessly and precipitately; when the funds are counted, there is a substantial

difference between the actual amount and the amount indicated by the customer (over or under); detection of counterfeit banknotes in the amount to be transferred or exchanged.

- Depositing funds in cash with further transfer of funds to other person on the same or next day.

Customer profile and behaviour

Customer profile

- Customer's area of residence is inconsistent with other profile details such as employment.
- The size or frequency of the transaction(s) is not consistent with the normal activities of the customer.
- The goods/currencies purchased, and/or the payment arrangements are not consistent with normal practice for the type of business concerned.
- The customer's address is a post office box or a c/o ('in care of') address.
- The customer's address is that of a company service provider (domiciliation service).
- The customer's address information is difficult to verify.
- The postal address for correspondence differs from the customer's official address.
- The stated address does not exist.
- A large number of persons are registered at the stated address, or there are a very large number of changing occupants, or other information is available indicating that it is not the real address of residence or domicile.
- The address of customer's residence does not correspond to the customer's financial arrangements.
- The customer changes address frequently.
- The customer is a business whose name and purpose do not correspond with its transactions.
- The customer cannot immediately provide additional identification documents.
- Identification documents appear to be unused.
- Identification documents are soiled making it difficult to read the necessary information.
- The customer is known to have a criminal past.
- The customer is close to a person who is known to have a criminal past.
- Sudden change in the customer's life style.

- The customer drives very expensive cars that do not correspond to his income situation;
- The customer hires or leases costly assets (*e.g.*, real estate or cars) that do not correspond to his income situation.

Customer behaviour

- The customer is unwilling provide details of his/her identity information and references.
- The customer needs information on what has been deposited in the account before a large cash withdrawal or transfer to abroad.
- Use of false identity documents to send money.
- Customer changes a transaction after learning that he/she must show ID.
- The customer shows no interest in costs or interests.
- The customer does not choose the simplest way to carry out a transaction.
- The customer has no connection with the area where the customer relationship is established.
- Transaction is a price-raising link in a series of transactions with no obvious reasons for the choice.
- The customer gives a rather detailed explanation that appears to be rehearsed concerning the reasons for the customer relationship or the transaction.
- The customer does not respond to letters to the stated address.
- The customer has many newly established companies.
- The customer contracts a loan secured on lodging of equivalent security.
- The customer has companies abroad that are not justified by the customer's business.
- The customer explains that expensive assets are a loan from or financed by a third party.
- The customer uses a payment card from a country which is not his country of residence.

2. Indicators for CE service providers

- Exchange of large quantities of low denomination notes for higher denominations.
- Exchange of large amounts or frequent exchanges that are not related to the customer's business.
- Structuring of large amounts.

- Repeated requests from an exchange office for foreign exchange purchasing-selling transactions in the amounts slightly less than the transaction limit for identification in a short period of time.
- The customer requests currency in large denomination notes.
- The customer buys currency that does not fit with what is known about the customer's destination.
- The customer buys currency from an unusual location in comparison to his/her own location.
- The customer apparently does not know the exact amount being exchanged.
- The customer looks around all the time and does not watch the counting of money.
- The customer is happy with a poor rate.
- Currency purchases with large cash amounts.
- Large exchanges between foreign currencies.
- Frequent exchange of cash into other currencies.
- Exchange of primarily one type of currency.
- The amounts exchanged are significantly higher than usual.
- There is no link between the amount of money exchanged and holiday periods.
- High frequency of currency exchange transactions over a period of time.
- Many currency exchange office used by a same person.
- Requests to exchange large amounts of foreign currency which is not convertible (or not frequently used) another kind of foreign currency.

3. Indicators for MR providers

- Transferring funds without any apparent economic reason.
- Unusual large cash payments in circumstances where payment would normally be made by cheque, banker's draft, etc.
- Transfers of funds without underlying transactions.
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings.
- Transfers paid by large cash amounts in different sums in a short period of time.

- Personal remittances sent to jurisdictions that do not have an apparent family or business link.
- Remittance made outside migrant remittance corridors (*e.g.*, Asian foreign domestic remits funds to South America).
- Personal funds sent at a time not associated with salary payments.
- The customer seems only after the counting to know which amount is being transferred.
- The customer shows no interest in the transfer costs.
- The customer has no relation to the country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there.
- The customer has a note with information about payee but is hesitating if asked whether to mention the purpose of payment.
- Large or repeated transfers between the account of a legal person and a private account, especially if the legal person is not a resident.
- Large amounts are transferred to companies abroad with a service provider address.
- Large or frequent transfers of money.
- Frequent transfer of value that is not related to the customer's business.
- Use of groups of people to send money.
- Use of different money remittance businesses.
- Amounts sent are higher than usual.
- There is not relationship between sender and the beneficial owner.
- The operations are irregular.
- Receiving money from different parts of the world (developed countries) from different people.
- Money is received during short periods of time.
- Money is received from different money remittance companies.
- Money is withdrawn in cash.
- Multiple senders toward a single individual.

Agents

- Reluctance to provide customers' identification to parent MR/CE business.

- Using false identification and fictitious names for customers.
- Frequent transactions or purchase of negotiable instruments under the reporting obligation.
- Each agent work with a different money remitter.
- Make false remittance operations.
- Use false identity documents to send money.
- Make too many operations.
- Not so many people enter into the agent office.
- Sending money to certain countries/cities.
- Amounts sent are higher than usual.
- Large volume of business in large person-to-person transactions.
- Unusual ratio of sent to received transactions (the direction of the flow of the suspicious ratio imbalance being determined by the context).
- High ratio of larger than normal transactions (the complicit operator attracts the larger-transacting criminal customers).
- Seasonal pattern of business that is different from other similar local businesses.
- High percentage of customers that are high dollar or value customers.
- High percentage of high-risk customers.
- High percentage of criminal activity corridor business, where the location is susceptible to involvement in known criminal activity, such as drugs, prostitution, certain fraud, etc..
- High percentage of total dollar business by high-risk customers.
- High volume of large or suspicious transactions in comparison to other MR/CE service providers in the same area.
- Turnover of the MR service provider, after changes in the management structure (with no development of services) exceeds remarkably the flows that were recorded before those changes.
- Conducting transactions before or after business hours.
- Common acceptance of false identification that permits structuring by customers that leave funds in the system for more than the average time before pick-up.
- Multiple transmissions to or receipts from a single customer in a high criminal activity corridor.

- Large volume of transactions for the same customer with multiple instances of using different name spellings, false addresses or identification that "evolves," *i.e.*, some parts of the identification change, while other parts remains the same, such as a person whose last name changes while his first name, date of birth, identification number and address remain the same.

- Transmission of funds by the same customer on the same day to several money transmitter locations to purportedly same or different recipients.

ANNEX 3 – TABLES : QUESTIONNAIRE RESULTS[28]

Table 1 – Overview of MR/CE service providers in jurisdictions contributing to this study

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Albania	X	X	X	X	X	X			
Argentina			X	X		X			
Armenia	0	X	X	X	X	0	0		Although the first field isn't marked, there are money remittance providers in Armenia (post offices, banks and others).
Austria	0	0	0	0	0	0	0	0	These activities may be carried out only by banks.
Bulgaria	X	0	0	X	X	X	0	X	Financial houses
Chile	X	0	X	X	X	X	0		
Chinese Taipei	0	0	0	X	0	0	0	0	
Croatia	X	X	0	X	0	0	0	0	

28 Tables below reflect data and information received from responding countries in 2008.

29 And other anonymous means of payment.

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Cyprus	0	0	0	0	0	0	0	X	Companies (legal persons) specifically licensed by the Central Bank of Cyprus to provide exclusively "money transfer services" (MTS means the operation of a business whose activities consists of the acceptance of money, exclusively for their speedy transfer from and to the Republic of Cyprus by any means)
Denmark	0	0	0	0	0	0	0		
Estonia	X	X	X	X	X	X	X		providers of payment services , money broker service providers
Finland	X	X	X	X	X	X	X	0	
France	X	X	X	X	X	X	X		MR conduct as a business is under the provision of the banking regulation.
Georgia	X	0	0	X	0	0	0	0	
Germany	X	X	0	X	X	X	0	X	
Greece	X	0	0	X	0	X	0	X	Electronic money institutions
Italy	X	0	0	X	0	0	X		*There are no such entities in our jurisdiction. Nevertheless these activities may be carried out by banks and supervised financial institutions.

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Japan	0	0	0	0	0	0	0	0	*As the definition of MR/CEs is not provided in this questionnaire, Japan assumes that MR/CEs are non-banking financial institutions providing money remittance services. In our jurisdiction, money remittance services are provided only by banks based on the Banking Act.
Latvia				X		X		X	Others – banks. Moreover, the Latvian Post is the only national MR provider.
Liechtenstein									There is no separate definition of MR/CEs in Liechtenstein. All services listed below can only be offered by Banks, Bureaux de change, or the Postal Services
Lithuania	0	0	0	0	0	0	0	X	Other – banks. Lithuanian Post provides MR services.
Macau, China	0	0	0	X	0	X	0	-	
Malta	0	X		X	X	X	X		Agents of authorised financial institutions – see point 4 below - such as the Post Office, travel agencies, stationeries, and others as may be authorised in terms of Article 8A of the Financial Institutions Act.
Mexico	X	X	X	X	X	X	0	0	
Moldova	X								
Monaco	0	0	0	0	0	0	0	X	"*Banque Postale"*
Netherlands	0	X	X	X	0	0	0	-	
Nigeria	X	X		X	X	X	X		

	Money orders providers	Travellers' checks issuers	Check cashing providers	Bureaux de change	Currency dealers	Currency exchange service providers	Stored value means providers[29]	Other	Remarks
Peru	X	X	X	X	X	X	X		
Poland	X	-	-	X	X	X	0	-	
Romania	X	X	-	X	-	X	-	-	
San Marino	X	0	0	X	0	0	0	0	The activity of MR is performed by banks and post offices, while CE is only performed by banks
Serbia	X	X	X	X	X	X	X	-	
Slovakia	X	0	0	X	X	X	0	0	
Spain	0	0	0	X	0	X	X		
Sweden	X	X	X	X	X	X	X	0	
"The former Yugoslav Republic of Macedonia"	0	X	X	X	X	X	0		
Turkey									Money service businesses are not defined specifically in Turkish legislation. These activities are carried out by banks in Turkey
Ukraine	X	0	X	X	0	X	0		
United Kingdom	0	X	X	X	0	X	0	X	Money Transmitters
United States	x	X	X	X	X	X	X	X	Money transmitters[1] and the United States Postal Service

Table 2 - Overview of the MR/CE service providers in jurisdictions contributing to this study

	Post Offices	Bureaux de change	Banks	Money transaction offices	Travel agencies	Hotels	Other	National MR providers	International MR providers
Albania	x	x	x						
Argentina		x	x						
Armenia	x		x				x		
Austria	x	x	x	x	x				
Bulgaria	x	x	x				Financial houses		
Chile	x	x	x						
Chinese Taipei			x						
Croatia	x		x						
Cyprus			x	x	x				
Denmark			x				miscellaneous shops		
Estonia	x	x	x	x	x				
Finland		x		x	x				
France	x		x						
Georgia	x		x						
Germany	x	x	x	x					
Greece	x	x	x	x					
Hong Kong, China	x	x	x				x		
Italy	x	x	x	**	x	x	Phone centres, internet centres, news agents, stationers		
Japan									
Latvia	x		x	x					
Liechtenstein	x								
Lithuania	x		x						

	Post Offices	Bureaux de change	Banks	Money transaction offices	Travel agencies	Hotels	Other	National MR providers	International MR providers
Macau, China	x		x				x		
Malta	x*	x	x		x*	x*			
Mexico	x	x	x	x	x				
Moldova	x		x						
Monaco							Banque Postale		
Netherlands		x	x	x	x	x	-		
Nigeria	x	x	x		x				
Peru	x		x	x					
Poland	x		x				x		
Romania	x	x	x	x		x	x		
San Marino	x		x						
Serbia			x						
Slovakia	x	x	x	x					
Spain	x		x	x					
Sweden	x	x	x	x	x	x			
"The Former Yugoslav Republic of Macedonia"		x	x	x	x	x			
Turkey	x		x						
Ukraine	x		x	x					
United Kingdom	x		x	x	x		outlets (*e.g.,* restaurants, general stores)		
United States	x	x	x	x	x	x			

* As agents of MR service providers.

Table 3 - Regulatory framework of MR service providers in jurisdictions contributing to this study

Country[30]	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Albania	NA	Central bank	NA
Argentine	NA	NA	NA
Armenia	Yes (licensing)	NA	No
Austria	None since there operate no independent money remittance service providers		
Bulgaria	Yes (licensing)31	Bulgarian National Bank	NA
Chile[32]	Yes (registering)	FIU	NA
Croatia	No		NA
Cyprus	Yes (licensing)	Central Bank	NA
Denmark	Yes (registering)	NA	NA
Estonia	Yes (registering)	Ministry of Economic Affairs and Communications	No
Finland	Yes (registering)	State provincial Office of Southern Finland	NA
France	Yes (licensing)	French Banking Commission	NA
Georgia	Yes (registering)	Georgian Financial Supervisory Authority	NA
Germany	Yes (licensing)	BaFIN (Federal Financial Supervisory Authority)	NA
Greece	Yes	NA	NA
Hong Kong, China	Yes (registering)	FIU	NA
Italy	Yes (registering)	NA	NA
Japan	None since there operate no independent money remittance service providers		
Latvia	No**		NA
Liechtenstein	NA		NA

30 For European Union/ EEA members, please see the explanations provided under Section 1.3 regarding licensing requirements as set out in the EU Directives.

31 During the licensing process, Bulgarian National Bank (BNB) also enters the agents and branches of the money remitter to the register. Agents and branches may not commence operations prior to the registration thereof. BNB shall not register and, respectively, delete from the register any agents and branches of money remittance companies if the BNB determines that the persons who manage and represent the said agents and branches do not possess the required qualifications, professional experience or reliability. A company licensed to operate a money remittance business shall notify the BNB upon the discontinuance of the execution of money remittances by any agent or branch of the said company not later than seven days before the date of discontinuance of the operation.

32 No registration/licensing required at country level.

Country[30]	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Lithuania	None since there operate no independent money remittance service providers		
Macau, China	Yes (registering)	Monetary Authority of Macau	NA
Malta	Yes (licensing)	Malta Financial Services Authority[33]	NA
Mexico	Yes (registering)	*Servicio de Administracion Tributaria* (Tax Administration Service)	No deregistration system
Moldova	None since there are no independent money remittance service providers operating		
Monaco	None since there are no independent money remittance service providers		
Netherlands	Yes (licensing)	NA	NA
Poland	Yes (registering)	NA	NA
Romania	Yes (registering)	National Commerce Register	NA
San Marino	None since there are no independent money remittance service providers		
Serbia	None since there are no independent money remittance service providers		
Slovakia	Yes (licensing)	National Bank of Slovakia	NA
Spain	Yes (licensing)	Central Bank*	NA
Sweden	Yes (registering)	NA	NA
"The former Yugoslav Republic of Macedonia"	NA	NA	NA
Turkey	None since there are no independent money remittance service providers		
Ukraine	Yes (licensing)	State Commission on Regulation of Financial Services Markets	NA
United Kingdom	Yes (registering)	HM Revenue and Customs	NA
United States	Yes (registering)***	FinCEN	Yes (every 2 years)

Remarks:
* In order to get the license from central bank, the positive report from FIU is also mandatory.
In Italy agents of MR service providers must be registered as well, provided that similar integrity and expertise requirements are met.
**The appropriate legislation is at the process of drafting.
*** A business operating as an MSB solely because that business serves as an agent of another MSB is not required to register, but an MSB that engages in activities requiring registration on its own behalf must register even if it is also engaging in activities as an agent for others. See paragraph 10 of main report for explanation of difference between MSB and MR/CE.

33 In Malta the activity of money remittance (as well as currency exchange) or transmission service forms part of a wider category of entities defined as "financial institutions"* that fall under the regulatory and supervisory responsibilities of the Malta Financial Services Authority (MFSA) for prudential purposes.

Table 4 - AML/CTF supervision [34]

Country	Central bank	FIU	Financial Supervisory Authority	Other
Albania	+	+		
Argentina			+	
Armenia	+			
Austria	No independent money remittance service providers			
Bulgaria	+	+		
Chile		+		
Croatia	+			+ (Financial Inspectorate of the Ministry of Finance)
Cyprus	+			
Denmark			+	+ (Danish Commerce and Companies Agency)
Estonia		+		
Finland				+ (The State provincial office of Southern Finland)
France			+	
Georgia			+	
Germany			+	
Greece	+			
Hong Kong, China	No supervision			
Italy	+			+ (*Guardia di Finanza*/Financial Police: on-site inspections, supervision over agents)
Japan	No independent money remittance service providers			
Latvia				+ (Ministry of Transport)
Liechtenstein		+	+	
Lithuania				+ (Financial Crime Investigation Service, Communications Regulatory, both supervise post offices)
Macau, China				+ (Monetary Authority of Macau)
Malta		+	+	
Mexico				+ *Servicio de Administracion Tributaria* (Tax Administration Service)
Moldova	No independent money remittance service providers			
Monaco	No independent money remittance service providers			
Netherlands	+			

[34] Other than banks and postal services.

Country	Central bank	FIU	Financial Supervisory Authority	Other
Poland		+		+ (Ministry of Infrastructure)
Romania		+		
San Marino	No independent money remittance service providers			
Serbia	No independent money remittance service providers			
Spain	+	+		
Sweden			+	
"The former Yugoslav Republic of Macedonia"	+			+ (Ministry of Finance)
Turkey	No independent money remittance service providers			
Ukraine	+			+ (State Commission on Regulation of Financial Services Markets)
United Kingdom				+ (HM Revenue and Customs)
United States				+ (FinCEN, Internal Revenue Service, state local authorities)

Table 5 - Sanctions applied to unlicensed /unregistered MR service providers

Country	Sanction
Albania	Fine or up to 3 years of imprisonment
Argentina	NA
Armenia	Fine or up to 3 years of imprisonment or the deprivation of the right to hold certain positions or practice certain activities for up to 5 years
Austria	Fine up to EUR 50 000.
Bulgaria	Fine up to EUR 5 000
Chile	Fine
Croatia	NA
Cyprus	Fine up to EUR 85 430 or imprisonment up to 2 years
Denmark	Fine
Estonia	Fine up to EEK 500 000 (appr. EUR 31 956)
Finland	Fine
France	Fine up to EUR 75 000 and/or imprisonment up to 3 years
Georgia	NA
Germany	Fine
Hong Kong, China	HK$ 50 000 (appr. EUR 717)
Italy	Up to 4 years of imprisonment
Japan	None since only banks may provide money transfer service
Latvia	Fine
Liechtenstein	Fine or imprisonment up to 1 year
Lithuania	Public works fine or imprisonment up to 4 years
Macau, China	Fine up to MOP 5 000 000 (appr.EUR 451 891)
Malta	Fine up to EUR 465 875 and/or imprisonment up to 1 year
Mexico	Fine
Moldova	There operate no independent money remittance service providers
Monaco	NA
Netherlands	Fine
Poland	None since only banks and Polish Post may provide money transfer service
Romania	NA
San Marino	Second-degree imprisonment (6 month to 3 years) and a fine as well as by third-degree disqualification from holding the offices of director holder of representative powers internal auditor external auditor actuary liquidator or commissioner in companies or other bodies with legal personality
Serbia	NA
Slovakia	Fine up to EUR 333 333 or imprisonment

Country	Sanction
Spain	Fine
Sweden	NA
"The former Yugoslav Republic of Macedonia"	NA
Turkey	Fine (up to 5 000 days salary) or imprisonment up to 5 years
Ukraine	NA
United Kingdom	Fine (unlimited) or imprisonment
United States	Sanctions vary by state. At the federal level: fine up to $ 5 000 (appr. EUR 3 476) per day and/or imprisonment for up to 5 years. There are several civil and criminal penalties for violations of the Bank Secrecy Act as well.

Table 6 - Threshold for identifying the customer

Country[35]	Threshold (CE)	Threshold (MR)
Albania	EUR 12 000	EUR 12 000
Argentina	obligatory	obligatory
Armenia	appr. USD 1300	appr. USD 1300
Austria	EUR 15 000	No threshold mandatory
Bulgaria	BGN 10 000 (appr. EUR 5 000)	BGN 10 000 (appr. EUR 5 000)
Chile	USD 5 000	USD 5 000
Croatia	HRK 105 000 (appr. EUR 15 000)	EUR 1 000
Cyprus		No threshold mandatory
Denmark	EUR 1 000	EUR 1 000
Estonia	EEK 100 000 (appr. EUR 6 400)	No threshold mandatory
Finland	EUR 15 000	EUR 15 000
France	EUR 8 000	No threshold mandatory
Georgia	GEL 3 000 (appr. EUR 1 400)	GEL 1 500 (appr. EUR 700)
Germany	EUR 2 50036	No threshold mandatory
Greece	EUR 15 000	EUR 1 000
Hong Kong, China	HK USD 8 000	HK USD 8 000
Italy	EUR 15 000	No threshold mandatory
Japan	YEN 2 000 000 (appr. EUR 15 566)	YEN 100 000 (appr. EUR 700)
Latvia	LVL 5 000 (appr. EUR 7 117)	EUR 1 000
Liechtenstein	CHF 5 000 (appr. EUR 3 271)	CHF 5 000 (appr. EUR 3 271)
Lithuania	EUR 6 000	EUR 600 (for local or cross-border post remittances) EUR 1 000 (for banks according to EU Regul No 1781/2006)
Macau, China	General rule: MOP 20 000 (appr. EUR 1 740) MOP 8 000 (appr. EUR 695) for wire transfers	No threshold for cash remittances MOP 8 000 (appr. EUR 695) for wire transfers
Malta	EUR 15 00037	EUR 1 000
Mexico	USD 3 000 (appr. EUR 2 086)38	USD 3 000 (appr. EUR 2 086)

35 In EU/EEA countries, there is a difference on the identification of customers depending on whether the money remittance provider is a bank (with the customer holding an account) or not.

36 If the transaction is carried out through an account other than the customer's account.

37 For one-off transactions. Customer identification is not subject to a threshold in the course of establishing a permanent business relationship.

38 *For Centros Cambiarios.*

Country[35]	Threshold (CE)	Threshold (MR)
Moldova	MDL 50 000 (appr. EUR 3 500)	MDL 50 000 (appr. EUR 3 500) for cash transfers and MDL 15 000 (appr. EUR 1 000) for electronic and wire transfers
Monaco	No threshold mandatory	No threshold mandatory
Netherlands	No threshold mandatory	No threshold mandatory
Poland	EUR 15 000	EUR 1 000
Romania	No threshold mandatory	No threshold mandatory
San Marino	EUR 15 000	EUR 15 000
Serbia	EUR 15 000	EUR 15 000
Slovakia	EUR 1 000	EUR 2 000
Spain	No threshold mandatory	No threshold mandatory
Sweden	EUR 15 000	EUR 1 000
"The former Yugoslav Republic of Macedonia"	EUR 2 500	EUR 2 500
Turkey	TRY 2 000 (appr. EUR 948) for wire transfers; TRY 20 000 (appr. EUR 9480) for cash transactions[39]	Mandatory when establishing the business relationships; TRY 2 000 (appr. EUR 948) for wire transfers; TRY 20 000 (appr. EUR 9480) for cash transactions
Ukraine	No threshold[40]	UAH 5 000 (appr. EUR 434)
United Kingdom	EUR 15 000	No threshold mandatory
United States	USD 1 000 (appr. EUR 696)	USD 3 000 (appr. EUR 2086)

39 Mandatory when *establishing* the business relationships.

40 Except for banks that may not identify their customers if the financial transaction is conducted to the amount of UAH 50 000 (USD 6 250) without *opening* an account.

Table 7- Regulatory framework for CE service providers in contributing jurisdictions

Country	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Albania	Yes (licensing)	Central Bank	NA
Argentine	Yes (licensing)	Central Bank	NA
Armenia	Yes (licensing)	NA	No
Austria	Not applicable as only banks provide money exchange		
Bulgaria	Yes (registering)	National Revenue Agency	NA
Chile[41]	Yes (registering)	FIU	NA
Croatia	Yes (licensing)	Central Bank	NA
Cyprus	Not applicable as only banks provide money exchange		
Denmark	Yes (registering)	Danish Commerce and Companies Agency	NA
Estonia	Yes (registering)	Ministry of Economic Affairs and Communications	NA
Finland	Legal requirement for licensing/registration in place but not yet implemented		
France	Yes (registering)	Central Bank	NA
Georgia	Yes (registering)	Georgian Financial Supervisory Authority	NA
Germany	Yes (licensing)	NA	NA
Greece	Yes	Bank of Greece	NA
Hong Kong, China	Yes (registering)	FIU	NA
Italy	Yes (registering)	Central Bank	NA
Japan	No		NA
Latvia	Yes (licensing)	Central Bank	NA
Liechtenstein	Not applicable as only banks provide money exchange		
Lithuania	Yes (licensing)	Central Bank	NA
Macau, China	Yes (registering)	Monetary Authority of Macau	NA
Malta	Yes (licensing)	Malta Financial Services Authority	NA
Mexico	Yes (licensing) Yes (registering)	Ministry of Finance and Public Credit Tax Administration Service	NA

41 No registration/*licensing* required at country level.

Country	Licensing/registration	Licensing institution Authority responsible for registration	Limited for the certain time period/needs updating?
Moldova	Yes (licensing)	National Bank	Yes, every 5 years
Monaco	Yes (registering)	Directorate of Economic Development	NA
Netherlands	Yes (licensing)	NA	NA
Poland	Yes (registering)	Central Bank	NA
Romania	Yes (registering)	Central Bank	NA
San Marino	Not applicable as only banks provide money exchange		
Serbia	Yes (licensing)	Central Bank	NA
Slovakia	Yes (licensing)	National Bank of Slovakia	NA
Spain	Yes (licensing)	Central Bank (+positive report from FIU)	NA
Sweden	Yes (registering)	NA	NA
"The former Yugoslav Republic of Macedonia"	Yes (licensing)	Central Bank	NA
Turkey	Yes (registering)	Undersecretariat of Treasury	NA
Ukraine	Yes (licensing)	Central Bank	NA
United Kingdom	Yes (registering)	HM Revenue and Customs	NA
United States	Yes (registering)	FinCEN	Yes (every 2 years)

Table 8 - Number of referrals, prosecutions and convictions based on STRs received from MR/CE sector (2006-2008)

	2006			2007			2008		
	Number of Referrals	Number of Prosecutions	Number of Convictions	Number of Referrals	Number of Prosecutions	Number of Convictions	Number of Referrals	Number of Prosecutions	Number of Convictions
Bulgaria	12	0	0	26	0	0	32	1	0
Chile	2			1			5		
Croatia	NA			12			11		
Estonia				10	0	0	49	0	0
Finland	1 069			1 293			445		
France	27	6		32	1		26		
Germany									
Greece	1			1			1		
Hong Kong, China	51	0	0	26	0	0	55	0	0
Latvia[42]	155*	25**	0***	146*	62**	3***	151*	29**	10***
Liechtenstein	1	0	0	0	0	0	1	0	0
Lithuania	2		0	2		0	5		0
Macau, China				1					
Malta	5	-	-	5	1	-	6	-	1
Moldova	12	2	0	18	3	0	29	0	0
Monaco							2	2	

[42] * Referrals are based on all received reports, not only on received from MSB sector.

** Only prosecutions sent to court in that year.

*** For convictions the number is for cases where ML is the main accusation.

	2006			2007			2008		
	Number of Referrals	**Number of Prosecutions**	**Number of Convictions**	**Number of Referrals**	**Number of Prosecutions**	**Number of Convictions**	**Number of Referrals**	**Number of Prosecutions**	**Number of Convictions**
Netherlands[43]	28 894	320	275	40 893	515	427			
Nigeria	2	1	1	1	1	0	1	1	0
Peru				4			18		
Poland[44]	5 (20)*	3 (12)	1 (2)	5 (24)	5 (21)	1	5 (59)	5 (48)	
Slovakia	2			2			2		
Spain	169			196					
Ukraine	446	163	1	520	242	25	641	326	76
United States		87			115				

43 *Note*: the authorities indicated that they could not establish that any single one of these prosecutions and convictions was based on an STR related to a MSB.

44 Data in parentheses encompass also reports to the public prosecutor which concern cases of money laundering connected with schemes ending transactions of money remittance (especially laundering of money stemming from unauthorised access to the bank accounts -"phishing attacks").

REFERENCES AND BIBLIOGRAPHY

Financial Action Task Force and FATF style regional bodies reports

FATF (2003) *Report on Money laundering and terrorist financing typologies - 2002-2003*, FATF, Paris

FATF (2005), *Money Laundering and Terrorist Financing Typologies 2004-2005*, FATF, Paris

FATF (2006), *Report on New Payment Methods*, FATF, Paris

FATF (2008a), *Terrorist Financing*, FATF, Paris

FATF (2008b), *Money Laundering and Terrorist Financing Risk Assessment Strategies*, FATF, Paris

FATF (2008c) *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems*, FATF, Paris

FATF(2009), *Risk-Based Approach – Guidance for Money Service Businesses*, FATF, Paris

MENAFATF (2005), *Best Practices Concerning Hawala*, MENAFATF, Kingdom of Bahrain, www.menafatf.org/Linkcounter.asp?rid=646&attached=best practices on Hawala.pdf (accessed September 2011),

Regulatory guidance and reports

CTIF-CFI (2003), *10th Annual Report 2002-2003*, (Dutch and French versions), CTIF-CFI, Brussels

FinCEN (2009) [United States], *Notice of Proposed Rulemaking – Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, Financial Crimes Enforcement Network, United States.

HM Treasury (2006) [United Kingdom], *The Regulation of Money Service Business: A Consultation*, HM Treasury, United Kingdom

International Monetary Fund (2005), *Regulatory Frameworks for Hawala and Other Remittance Systems*, International Monetary Fund, United States

International Monetary Fund (2005), *Approaches to Regulatory Framework for Formal and Informal Remittance Systems: Experiences and Lessons*, International Monetary Fund, United States

Madinger, J. (2006), *Money Laundering. A Guide for Criminal Investigators*, 2nd edition, CRC Press.

SOCA (2009) [United Kingdom], *The United Kingdom Threat Assessment of Organised Crime*, SOCA, United Kingdom

US Department of Justice, National Drug Intelligence Center (2006). *Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*, October 2006, US Department of Justice

US Department of the Treasury (2007) [United States], *Money Laundering Strategy 2007*, US Department of the Treasury

US Department of the Treasury (2005), *United States Money Laundering Threat Assessment*, December 2005, US Department of the Treasury

Articles and papers

Carroll, L. C. (2007), *Alternative Remittance Systems distinguishing sub-systems of Ethnic Money Laundering in INTERPOL Member Countries on the Asian Continent*. Interpol, 2007.

Chene, M. (2008), *Hawala Remittance System and Money Laundering. U4 Expert Answer*, Anti-Corruption Resource Centre, Norway, 2008.

Choo, K-K. R. (2008), *Money Laundering Risks of Prepaid Stored Value Cards*. Australian Government, Australian Institute of Criminology, Sept 2008.

Jost, P. M., H. S. Sandhu (2000), *The Hawala Alternative Remittance System and its Role in Money Laundering*. Interpol, Jan 2000.

KPMG (2005), *2005 Money Services Business Industry Survey Study*. KPMG, 2005

Sienkiewicz, S. (2007), *Prepaid Cards: Vulnerable to Money Laundering?* Payment Cards Center, Federal Reserve Bank of Philadelphia, Discussion Paper, Feb 2007.

GLOSSARY OF TERMS

Agent	any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). (*This definition is drawn from the Interpretative note to the FATF Special Recommendation VI*).
Alternative remittance systems (ARS)	Any system used for transferring money from one location to another that operates in part or exclusively outside conventional banking channels.
Beneficiary	The person who receives transferred funds.
Beneficial owner	The natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Cheque casher	A person that accepts cheques or monetary instruments in return for currency or a combination of currency and other monetary instruments or other instruments.
Currency	Banknotes and coins that are in circulation as a medium of exchange
Currency exchange (CE)	Activity that involves accepting currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries.
Financial institutions	*Financial institutions*[45] means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[46] 2. Lending.[47] 3. Financial leasing.[48]

[45] For the purposes of Special Recommendation VII, it is important to note that the term *financial institution* does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.

[46] This also captures private banking.

[47] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

[48] This does not extend to financial leasing arrangements in relation to consumer products.

4. The transfer of money or value.[49]
5. Issuing and managing means of payment (*e.g.*, credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:

   (a) money market instruments (cheques, bills, CDs, derivatives etc.);

   (b) foreign exchange;

   (c) exchange, interest rate and index instruments;

   (d) transferable securities;

   (e) commodity futures trading.

Participation in securities issues and the provision of financial services related to such issues.

Individual and collective portfolio management.

Safekeeping and administration of cash or liquid securities on behalf of other persons.

Otherwise investing, administering or managing funds or money on behalf of other persons.

12. Underwriting and placement of life insurance and other investment related insurance[50].
13. Money and currency changing.

(Source: FATF)

Funds transfer

Series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order.

Hawala

A specific form of an alternative remittance system.

Informal value transfer system (IVTS)

Any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. Informal value transfers generally take place outside of the conventional banking system through non-bank financial institutions or other business entities whose primary business activity may not be the transmission of money.

---

49 This applies to financial activity in both the formal or informal sector *e.g.*, alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

50 This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Issuer, seller, or redeemer of stored value	A person that issues stored value or sells or redeems stored value.
Money remittance (MR)	Activity that involves accepting currency, or funds denominated in currency, or other value that substitutes for currency from one person and transmission of the currency or funds, or the value of the currency or funds to another location or person, by any means through a financial agency or institution, or an electronic funds transfer network. Often postal service providers fall into this category if they provide fund transfer services.
Money service business	According to the generally accepted definition, *money service businesses* (MSBs) are non-bank[51] financial institutions that provide certain types of financial services. Although the precise scope of the activities that fall into category "money service" vary from country to country (for example, the requirements for MSBs may only apply if the value of individual transactions and/or its turnover exceeds a certain value limit.[52] They may also only apply to businesses that carry out the specified activities on regular basis or as an organised business concern, etc). Typically, the following types of financial activities are carried out by MSBs: • Currency dealing or exchange. • Cheque cashing. • Issuance of traveller's cheques, money orders or stored value. • Selling or redeeming of traveller's cheques, money orders, or stored value • Money transmitting.
Originator/ transmitter	The sender of the payment order in a funds transfer.
Stored value	Funds or monetary value represented in digital electronics format (whether or not specially encrypted) and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically.

51 According to the US financial intelligence unit (FinCEN), the definition *money services business* does not include financial institutions, nor does it include persons registered with, and regulated or examined by, the Securities and Exchange Commission or the Commodity Futures Trading Commission.

52 For example, in US rules applicable to MSBs apply to those currency dealers/exchangers, cheque cashers, issuers of traveler's cheques, money orders or stored value who exchange currency or issue/sell/redeem cash cheques/money orders/stored value in an amount greater than USD 1 000 in currency or monetary or other instruments for any person on any day in one or more transactions.

MONEYVAL and FATF/OECD
July 2010

www.fatf-gafi.org