



**Financial Action Task Force**  
Groupe d'action financière

**MONEY LAUNDERING &  
TERRORIST FINANCING TYPOLOGIES  
2004–2005**

10 June 2005

**© FATF/OECD 2005**

**All rights reserved. No reproduction, copy, transmission or translation of this publication may be made without written permission. Applications for such permission, for all or part of this publication, should be addressed to the FATF Secretariat, OECD, 2 rue André Pascal 75775 Paris Cedex 16, France**

## TABLE OF CONTENTS

INTRODUCTION .....	1
I. ALTERNATIVE REMITTANCE SYSTEMS .....	3
II. MONEY LAUNDERING VULNERABILITIES IN THE INSURANCE SECTOR.....	41
III PROCEEDS FROM TRAFFICKING IN HUMAN BEING AND ILLEGAL MIGRATION.....	65
IV MONEY LAUNDERING AND TERRORIST FINANCING TRENDS AND INDICATORS: INITIAL PERSPECTIVES .....	88

## INTRODUCTION

Since its beginning, the Financial Action Task Force (FATF) has undertaken the study of the methods and trends associated with money laundering – or “typologies” - as a key component of its work. From the start the objective of this work has been not only to share information among law enforcement and other practitioners, but also to provide the necessary basis for informed decisions on anti-money laundering and terrorist financing policy. Typologies work thus plays a key role in the FATF standard-setting process. Additionally, the findings acquired through the annual FATF typologies exercise have served as material for informing a wider audience – regulatory authorities, law enforcement agencies, the financial sector and the general public – on the characteristics and trends of money laundering and terrorist financing.

In early 2004, the FATF began implementing a new framework for carrying out its typologies work, with a view to further increasing the usefulness of the exercise for policy making. The FATF Plenary established a Working Group on Typologies (WGTYP) in February 2004 to provide more focus and deal specifically with this initiative. With the subsequent creation of project teams to examine a series of defined typologies issues, the WGTYP set up a mechanism that could thus deliver more in-depth research and analysis than had previously been the case. This year’s report is a reflection of this new approach and focuses on the following issues, which have all been researched by separate project groups.

- Alternative remittance systems
- Insurance and money laundering vulnerabilities
- Money laundering associated with human being trafficking and illegal migration
- Money laundering and terrorist financing trends and indicators

The last topic is of a different nature and focuses on developing a “methodology” to examine ML and TF. The project is ongoing and a first progress report reflecting the initial steps and general approach taken by the project team is included as a small chapter in this year’s report.

The new approach to investigating typologies has also had an impact on the organisation of the annual experts’ meeting. The FATF decided in June 2004 to re-evaluate the way that the annual experts’ meeting on typologies fits into the whole FATF typologies process and organise the meeting around different parallel workshops that focus on the separate typologies projects. The principal goals of this new approach is to provide a more effective means for exchanging ideas between operational and policy experts on selected typologies issues and to serve as a basis for a more thorough analysis of the subjects. The FATF-XVI meeting of experts on typologies took place in December 2004 in Moscow and examined the four topics mentioned above. Small project teams of experts conducted research on each topic prior to the meeting. In addition a project team investigated the links between narcotics trafficking and terrorist financing but had to conclude that this subject was less suitable for analysis through publicly accessible information.

The project teams were responsible for organising the workshops and used the information and research obtained up to November 2004 as the basis for discussion during the one and a half day sessions. The average number of participants in each workshop was around 40 persons. At the end of the workshops, each project leader had the opportunity to present the findings of the workshop to all of the participants gathered in a plenary meeting.

The Moscow typologies meeting was important for a number of reasons. It was organised as part of joint exercise undertaken by both the FATF and an FATF-style regional body (FSRB), the Council of Europe MONEYVAL Committee. The Russian Federation is a member of both bodies; therefore, meeting was organised and chaired by Mr. Viktor ZUBKOV, Director of the Federal Service for

Financial Monitoring of the Russian Federation (*Rosfinmonitoring*, the Russian financial intelligence unit). This meeting was the first of its kind between the FATF and an FSRB, and it permitted interaction to occur among a much broader range than in previous FATF exercises. Furthermore, one of the projects – money laundering associated with human being trafficking and illegal migration – was led by MONEYVAL.

Following the Moscow experts' meeting, the remaining project teams continued their research as necessary and then drafted reports on their findings. The four chapters of this document are the reports prepared by the project teams. The work reflects the research and analysis carried out by a range of experts from FATF, MONEYVAL and other countries. Invaluable contributions to this work were also obtained from international organisations such as the International Monetary Fund, the World Bank, the International Association of Insurance Supervisors, the Egmont Group and many others.

## CHAPTER I

### ALTERNATIVE REMITTANCE SYSTEMS

Experience over the last decade has shown that ARS can be misused for illegal purposes, including for both money laundering (ML) and terrorist financing (TF). Although the alternative remittance sector is largely composed of legitimate operators, some categories of ARS have nevertheless been involved in the transfer of funds related to illegal activities – or are themselves operating without proper authorisation from an oversight authority. The FATF has focussed on ARS activity in a number of previous typologies exercises.<sup>1</sup> ARS continue to be the source of concern as far as their vulnerability to misuse for ML or TF purposes; however, increasingly other considerations have also become more evident, such as balancing the prevention of misuse with the need to ensure that flows of legitimate funds are not unnecessarily interrupted or pushed underground. The FATF has thus once again decided to examine the subject so as to provide a basis for further discussion of AML/CFT policy implications.

The scope of this report is intended to cover ARS, that is, any system used for transferring money from one location to another and generally operating outside the banking channels. The services encompassed by this broad definition of ARS range from those managed by large multinational companies to small local networks. They can be of a legal or illegal nature and make use of a variety of methods and tools to transfer the money.

On the basis of this broad definition of ARS, the report describes how such systems work in practice, both from the perspective of the customers and from that of the ARS itself. The aim is to identify areas where vulnerabilities and risks are present in terms of exposure to ML and terrorism financing. A better knowledge of ARS working mechanisms will likely allow more effective policies to be put in place to identify undeclared or illegal ARS and to detect misuse of such channels by criminals and terrorists.

The FATF has already developed certain policies or measures that may be applied to ARS through the FATF Forty Recommendations and in the Nine Special Recommendations. A number of countries have introduced specific measures as well. Increasing awareness of the risks of misuse of ARS for transferring, transforming or disguising funds derived from criminal activities or intended for support to terrorism is important. Such an awareness can foster additional initiatives by national authorities in developing appropriate regulatory systems, as well as in strengthening the enforcement of those measures.

The drive to apply FATF standards is in certain cases encouraging countries to seek harmonised legislative solutions. Stronger co-operation favours the detection of criminal activities performed through ARS in the international scenario. Harmonised approaches and international co-operation prove fundamental especially taking into account that countries are invariably linked to each other in a sending – receiving relationship. To highlight existing risks, countermeasures in place and possible weaknesses, the report provides examples of various regulatory frameworks that have been applied to ARS, both in the international standards and at national level.

In their use of ARS, criminals are continuing to develop new and more sophisticated methods to avoid detection and to achieve their objectives more effectively. Analysis of cases and investigations carried out in several countries shows that criminal use of ARS can be significant in certain areas and that new trends are emerging. The report thus focuses specifically on the analysis of concrete ARS activities and cases of ML and TF, according to a two-fold approach: six different ARS categories are identified

---

<sup>1</sup>Notably during FATF-XIII, FATF-XI and FATF-IX.

and the inherent risks highlighted; cases illustrating the use of ARS for ML and TF, submitted by countries, are analysed to identify and update relevant typologies.

The use of ARS for criminal purposes starts with a simple transaction designed to dispose of criminal cash or obscure the audit trail for criminal money held in a bank account. The investigation of these operations from the entry of the funds into the ARS “retail outlet” to the ultimate beneficiary can, however, be characterised by a high degree of complexity. This level of complexity is mostly due to intricate settlement systems used and number of jurisdictions through which a transfer could pass. Each jurisdiction might hold a part of the evidence or intelligence impacting on the transaction. Therefore, obtaining an overall view of particular operations from beginning to end is made more difficult.

This study has attempted to describe relevant patterns in the misuse of ARS through the classification of the cases available. It is hoped that this method will identify key factors related to such misuse and thus ensure a consistent approach to identification of typologies. To organise the material, a matrix was used to permit comparisons among cases in the light of several typologies criteria. It documented examples of ARS, identified the ML and TF risks associated with each system and then highlighted the key indicators of ML/TF activity. The matrix was designed to be a tool to help further the study of ARS and ML/TF, and it is hoped that it might serve as a framework for future documentation and analysis of cases.

The settlement process for illegal or undeclared ARS providers (including both those carried out by underground organisations and those performed by money launderers or terrorist financiers) is often executed – at least in part – by means of conventional banking services. For example, the funds might be collected in bank accounts and then wired to foreign destinations. Banks can be unwittingly involved and, to avoid detection, criminals often adopt deceptive strategies. Other channels are also frequently used for settlement, including the physical movement of cash or the carrying out of commercial transactions that serve as a way of settling imbalances between ARS providers in different locations. Commercial transactions often serve as a means for transferring funds outright: money is collected for remittances and then used for the purchase of goods; the goods are moved to the target location and then sold; the resulting funds are then delivered to the remittance beneficiaries.

The analysis of individual cases would not be complete without understanding something of the larger framework for the detected activity. In the case of ARS, it is important to understand the larger pattern of remittance flows or corridors and how these vary from one geographical area to another. At present, important research is being carried out in this area by other organisations. This report therefore attempts to provide the context and short explanation of the role of such corridors for both sending and receiving countries.

Finally, this report will lay out the main findings of this research and will then attempt to identify some of the key policy implications for policy makers dealing with the AML/CFT area. The points made here are intended to provoke discussion and are clearly not intended to point toward particular solutions to the issues identified. It is hoped that by raising some of these issues and their implications for developing new measures or refining existing ones that this report will contribute to the overall effort to understand and, as necessary, to confront the challenges posed by ARS.

### **A note on terminology used in this report**

Studies published over the past few years — including some of those carried out by the FATF — use a variety of terms to refer to money or value transfer systems. Given the seeming complexity and broad diversity of these systems, it is understandable that a certain amount of confusion often arises in discussions on this subject. At the outset of this report therefore, it is important to be clear about the concepts covered by this study as well as the terminology that will be used.

The FATF defines a *money or value transfer system* as a “financial service that accepts cash, cheques other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer system belongs.”<sup>2</sup> This definition is necessarily broad and is intended to cover the full range of financial services involved in transferring money, including everything from banks to systems operating in full or in part outside conventional banking channels.

The focus of the present study is on this second category of money/value transfer systems, that is, all remittance systems that operate completely or in part outside conventional banking channels. A number of terms have been used to refer to such systems: *informal funds transfer*, *alternative remittance*, *underground* or *parallel banking* and so on. Some of these systems have ties to particular geographic regions or ethnic or migrant groups and are therefore referred to with terms such as *hawala*, *hundi*, *da shu gong si*<sup>3</sup> and *black market peso exchange*. None of these terms is fully satisfactory by itself in capturing the diverse nature of this activity, that is, one which also includes in some cases some parts of the conventional banking system through services provided by internationally franchised money remitters, for example. For the purposes of this study therefore, the term *alternative remittance system* (or *ARS*) will be used. Although this term could be used or interpreted differently, in this study it is meant to indicate that the activity under discussion is *an alternative* to the exclusive use of conventional banking for remitting money (even though ARS operators often make use of their own bank accounts for balancing or settling accounts with other operators). It is understood that *alternative remittance systems* includes money/value transfer systems regardless of their legal status in particular jurisdictions and regardless of whether or not they are currently covered in part or in total by national regulatory systems.

This last point should be emphasised, as the status of ARS varies from one country to another. In some jurisdictions, for example, financial institutions with a banking licence are the only authorised channel for carrying out money or value transfers. ARS are thus prohibited by law. In other jurisdictions, ARS are illegal; however, their existence is tolerated. In still other jurisdictions, national authorities are attempting to bring ARS under some form of oversight through registration or licensing of such activity. It is important to understand these different approaches to dealing with ARS, as money or value transfers may often involve a chain of transactions between ARS providers, each with a different status in their country of operation. For example, a legally registered ARS provider in the United Kingdom may send a transfer payment through a licensed operator in the United Arab Emirates to an illegal *hawaladar* in India (*hawala* is not permitted in India).

Finally, this study very briefly touches on the issue of new payment methods including e-money. Although many of these systems might also be included in the term *alternative remittance systems*, their characteristics are so atypical that they would almost deserve a separate study.

## **ALTERNATIVE REMITTANCE SYSTEMS: HOW THEY WORK**

### **Factors Motivating the Use of Alternative Remittance Systems**

ARS play a significant role in moving funds into and out of the financial sectors of some countries. In countries with large immigrant populations, ARS offer a key service to such communities in providing them with a means for sending funds to their countries of origin. For other ARS users, the systems provide a cost effective and efficient method for transferring money to family or for business reasons. Some ARS can be used to circumvent national currency requirements where they exist. It should be noted as well that the vast majority of funds travelling through ARS – regardless of the legal status of

---

<sup>2</sup> Interpretative Note to FATF Special Recommendation VI: Alternative Remittance, issued in February 2003.

<sup>3</sup> Previously, the term *fei chien* has been used for this particular type of ARS.



the service provider within a particular jurisdiction – are funds of legal origin and/or intended for legal purposes.

While in a few instances ARS provide the only means of bringing funds into or out of a particular country, most such systems operate alongside conventional banking channels. It is useful therefore to understand the factors that may motivate a person desiring to transfer funds to prefer using ARS rather than conventional banking. Some of the perceived motivating factors or incentives for using ARS are included in the following table.

A different issue to consider is that in certain cases individuals may not have the means to identify themselves. For example, a remittance sender may be unable to submit him or herself to identification procedures or other forms of customer due diligence (CDD) because his or her country does not have the institutional capacity to issue identification documents. It is worth noting therefore that a desire for anonymity does not necessarily mean that a particular remittance transaction is related to criminal activity. There is evidence that anonymity, in certain instances, may also be a means of circumventing the pressure from government officials that ask the recipient for bribes or try to impose taxes on cross-border flows. Whatever the underlying reason, the fact that ARS sometimes offer the possibility of transmission of funds without strict identification procedures makes them attractive to some customers. Indeed, the very nature of remittance is based on a “one-off” business relationship with the customer unlike the ongoing relationship that exists between the customer and a conventional bank.

### **The Mechanisms of Alternative Remittance Systems**

The systems used for alternative remittance can be considered as both simple and complex. They are simple in that the individual components of the system involve operations as basic as receiving cash for a transfer or communicating information on individual payment orders. ARS can appear to be complex, as they may rely on a series of seemingly unrelated operations at the clearing or settlement phase of the process. ARS operations may in fact appear to be more complicated in certain situations due to the lack of transparency inherent in certain types of systems. In any case, most ARS activity is carried out in ways that are very similar to those used by conventional banks to move funds. To examine the way the ARS work, it makes sense to view such systems by looking at each of the various components or players in this activity. This breakdown will make it easier to follow each phase in the alternative remittance process.

#### ***The Originator of the Transfer***

For the sending customer (the *originator* of the money/value transfer), a transaction begins by the payment or handing over of funds to the ARS operator. At this point, the originator also specifies the recipient or beneficiary for the transaction along with his or her location. The funds can be paid in cash, cash equivalent, cheques, and other monetary instruments or in stored value cards. In certain situations, the originator may pay funds directly into a bank account belonging to or controlled by the ARS operator. Cash remains the most prevalent form of funds at this stage. In large ARS networks the customers generally have access to the ARS services through local (sub)agents. The originator usually receives a unique reference to identify the transaction. This is then passed to the beneficiary. The originator’s only other role in the transaction will be to follow up with the originating ARS provider if the beneficiary reports a failure of the transaction.

### Factors Motivating ARS Usage

Every remittance operation is initiated by a sender. Therefore, to understand what motivates a sender to prefer using ARS versus conventional banking, it is necessary to look at this activity from the sender's point of view. There are a number of factors or perceived incentives that play a role in the sender's choice of ARS. The incentives identified below have been grouped according to personal, customer service and economic factors; although in practice the perceived incentives may overlap. However, it is equally clear that not all the incentives mentioned in the table apply in all situations and that the incentives vary hugely for different types of ARS (for example, the services of some ARS can actually be rather expensive compared to remittances through conventional banking services).

General Factor	Perceived Incentive	Examples of how perceived incentives have influenced the sender in choosing ARS
Personal	<ul style="list-style-type: none"> <li>• Anonymity / secrecy</li> <li>• Cultural familiarity</li> <li>• Personal contacts</li> </ul>	ARS are frequently more trusted by customers, especially when the service is offered by a member of the same ethnic or immigrant community. Some senders, whose immigration status is not in order or who have another reason to avoid strict identification and CDD procedures, may use certain ARS to avoid attracting the attention of the authorities
Customer Service	<ul style="list-style-type: none"> <li>• Dispute resolution</li> <li>• Accessibility</li> <li>• Class discrimination</li> <li>• Versatility / resilience</li> </ul>	For example, ARS can provide service in places that conventional banking channels often cannot reach (either at the location of the originator and / or at that of the recipient).
Economic	<ul style="list-style-type: none"> <li>• Speed</li> <li>• Cost</li> <li>• Secondary benefits</li> <li>• Legal / regulatory</li> <li>• Environment</li> </ul>	Fees may be significantly lower in ARS than for conventional banking systems. ARS provide a versatile and rapid service (many locations are served; there is no need to open accounts; different means of payments may be used).

Source: "A Proposed Framework to Analyse Informal Funds Transfer Systems" (Chapter 13). Remittances: Development Impact and Future Prospects. D. Ratha; Samuel Maimbo, ed. (Forthcoming)

### ***The Originator's ARS Service Provider***

The ARS provider at the originator's location receives the funds and then sends an instruction for payment to a counterpart at the location of the beneficiary of the transfer. This communication may occur directly or through an intermediary as well as through different communication channels (for example, fax, telephone, Internet). ARS providers normally have a record of their partner ARS providers in the beneficiary's location who make payments on their behalf. With more organised multinational operators this list of partner ARS providers is usually available to the public; in some circumstances, it may be provided on request.

The operator may assign a code to the transaction. In an internationally franchised operation this will usually be an easily recognisable multi-digit unique number. In a *hawala* transaction it may be a banknote serial number. This unique number will be communicated to his customer (originator), and the disbursing agent. The originating customer will usually communicate this unique number to his intended beneficiary who will then be able to be identified by the disbursing agent.

5788 1780	40 Hawala Shop	4/3	ASHA MOHD. ALI Lahore	Mo. MOHD. ALI Tel. 3564240	5000	60	
5789 13391	40 Hawala Shop	4/3	MR. MATHEW ULLAH PESHAWAR	Mo. MOHD. SHAH Tel. 2346024	6,500	71	
5749 17667	40 Hawala Shop	4/3	HAFAIZ KHUSHI Mo. BERKAT ALI	16,700	120		
5749 17667	40 Hawala Shop	4/3	Mo. SOELWAK Mo. JAW SHAMSUDDIN	7448156	75000	843	Bm
5742 13443	40 Hawala Shop	5/3	RASHID QADOM KHAN Mo. ABUL QADOM KHAN	843943	30,000	357	Bm
5743 13443	40 Hawala Shop	5/3	FAZULLAH Mo. ALI KHAN	2263628	20,000	238	

Figure 1: Example of initial record of ARS transfer with reference number. Source: United Kingdom

### The ARS Service Provider at the Transfer Destination<sup>4</sup>

The ARS operator at the destination for the remittance makes the corresponding payment on instructions from the originating ARS operator, to the beneficiary specified by the originator who meets the identification procedure. This may be a formal and recorded identification procedure or simply the person who knows the unique reference number. The ARS operator may have to satisfy two standards of compliance, depending on differences in compliance regimes in the sending and receiving country.

AS SOON AS POSSIBLE

PAGE 1 04/05/01 PAGE1

NEW DELHI

445 SENDER : - KAY RECEIVER : - SATWANT KAUR W/O BALDEV SINGH NEW  
DELHI TEL : - 220 8203 1000//=

484 SENDER : - HARISHA BHRAR RECEIVER : - MRS SUHAG RANI BHRAR C-19  
KRISHNA PURA GARDENS NEAR TILAK NAGAR TEL : - 559 2785 NEW DELHI  
1330//=

PUNJAB

467 SENDER : - AMERJIT SINGH DHALIWAL RECEIVER : - SWARAN SINGH S / O  
JAGIR SINGH (GURDITTEY KAY) PATTI LODH BADI MALLAN ROAD VILLAGE  
LOPON TEHSIL NIHAL SINGH WALA TEL : - P.P. ( RAGHEIR SINGH  
CHACHA OF AMERJIT SINGH) 01636 53721 (OLD) 01636 52121 (NEW)  
DISTT. MOGA 1000//=

470 SENDER : - RAM PRAKASH VIRDI RECEIVER : - BALBIR CHAND S / O  
RAMJI VILLAGE DAULATPUR P.O. LAWALPUR TEL : - 181 715430  
DISTT. JULLUNDHUR 1500//=

471 SENDER : - SURJIT SINGH AUJLA RECEIVER : - JASVIR SINGH AUJLA  
BROTHER OF HAWALDAAR KANKAR SINGH AUJLA VILLAGE AUJLA ( HOUSE  
NEAR THE GURDWARA ) NEAR KOT TAPAI TEL: - 1822 33872 DISTT.  
KAPOORTHLA 3000//=

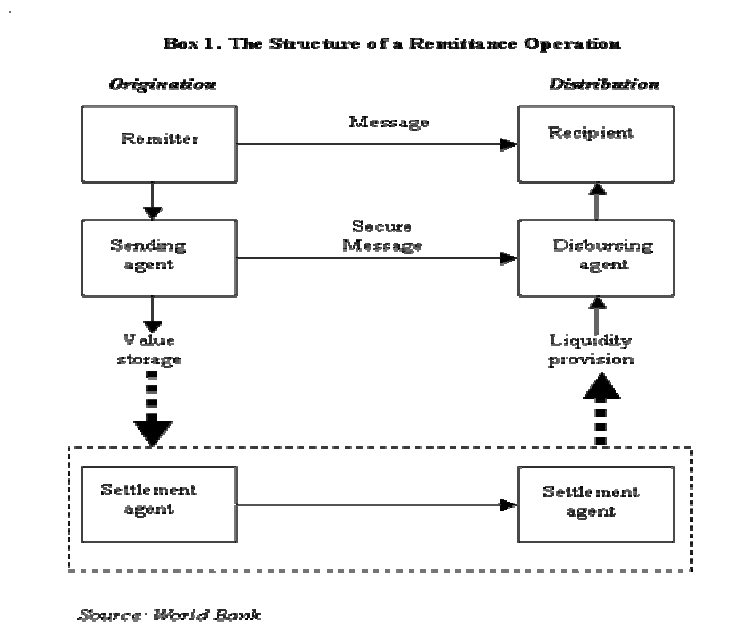
Figure 2: Example of a genuine payment instruction from a shop front ARS to intermediary ARS at destination; Source: UK

### The Transfer Beneficiary

The money, once received at its destination, may be delivered directly to the beneficiary (the recipient in the diagram below), or else the beneficiary will be notified to go to the premises of the destination

<sup>4</sup> It is however possible that a system consists of one operator, receiving funds in one place and paying out in the other place

ARS operator to receive payment. Payments may be received in local currency, hard (international) currency or in the form of a cheque or bank draft. An identification code may be used to validate the payment. In a jurisdiction with ML controls, the ARS operator could apply CDD-procedures to the beneficiary. The beneficiary will inform the originator of any failure of the ARS transaction. These roles are summarised in the following table from a World Bank study.



### Emerging Trends in Alternative Remittance Systems

ARS operators are flexible and progressive in finding new, profitable and efficient methods of transmitting money. It is important to note that these services are being developed to respond to a particular consumer demand and for the most part have not been designed to circumvent existing AML/CFT measures.

For example, ARS and credit card companies are developing new products allowing debit cards to be bought for cash and then the value moved or paid out via automated teller machines (ATM) and purchases by anyone holding the personal identification number (PIN). This is an efficient way to move money securely and provides a flexible way for the money to be stored and retrieved. The card providers place limits on the value that can be stored in the cards, some of which can only be loaded with value once. AML measures are limited to the card purchaser.

In Africa bus companies with scheduled routes are in some cases furnishing remittance services. The drivers use cash received for tickets to pay out remittances. This gives the bus operators extra revenue and improves security for drivers who previously had to carry the cash proceeds of ticket sales. In other countries taxi firms operate similar systems, delivering money to customers' homes.

Mobile phone companies are using the ability of SIM cards to be loaded with value and have that value removed to use phones as a method of storing, exchanging and remitting value in countries with developing mobile phone infrastructure.

#### Internet-based Remittance Services

At least one Internet-based remittance agency – "IBR" – has been encountered by the authorities in Hong Kong, China. The IBR in question is based in the United States and uses the global Integrated Funds Transfer System (GIFTS). In conjunction with a major credit card service provider, it provides for the transfer of funds to any beneficiary worldwide through the issuance of an ATM card, and settlement for the transactions occurs by direct debiting of the nominated credit card of the remitter.

Remitters simply open an account with the web-based service provider. The service provider dispatches an ATM debit card to the nominated beneficiary in any one of 130 countries. The ATM debit card can be utilised at any ATM carrying the service of the major credit card or used to make purchases worldwide within seconds of being credited by the remitter.

The remitter simply enters a secure area of the IBR web site and authorises the transfer of funds to the beneficiary's account. The funds are then immediately available to the beneficiary anywhere in the world through the worldwide ATM network. IBR even allows for beneficiaries to request money from the remitter via the IBR website. The beneficiary simply completes a request message, and then the system automatically forwards an e-mail to the remitter requesting that he or she authorise the further remittance of funds.

The ATM cards used in this process are easily transferable thus allowing for greater anonymity than the more traditional use of supplementary credit cards. Regulators and investigators face great difficulty in monitoring such activities, and there is an obvious potential for misuse by criminals and terrorists.

For example, even in jurisdictions where regulated ARS exist, individuals in one jurisdiction can make remittances to a second jurisdiction without leaving easily traceable records that could be used by competent authorities. The only information available is credit card activity relating to the remitter in the sending country, which will only reflect payments to the web-based remittance agent. Checks on the beneficiary would then have to be routed through many agencies in a number of jurisdictions including the sending and receiving jurisdictions as well as the location in which Internet-based transfer service is located.

### ***Settlement***

ARS transfers may occur in both directions, that is, the service providers may process both outgoing and incoming transfers at their particular location. Ideally, the transfer amounts should balance out so that the neither side has a surplus or deficit. In reality however, ARS operations seldom balance out between the service providers in two different jurisdictions. The originating ARS operator will accumulate a sum of money, whilst the destination ARS operator will have a deficit. This deficit has to be balanced out or settled in the longer term. In general, settlement of the amounts owed within a network of operators will not occur on a transaction-by-transaction basis. Often, settlement is effected on a weekly, bi-weekly or monthly basis. Given this length of time, the pricing of the final set-off transaction will often depend on a fluctuating exchange rate which takes account of the movements in currency over the period in question. Methods of settlement may vary according to the type of ARS service or its links to other commercial activities. Whatever method is used, the ARS service provider also seeks to preserve or enhance profits. Some of the more common ARS settlement procedures are indicated below.

#### *Transfers through Conventional Banking Systems*

The ARS service provider holding funds use wire transfers, the Internet or other methods of payment to make payment to the account specified by the deficit ARS provider (who has paid out remittances at the destination). This may be a simple operation but involves bank fees and exchange rate costs that have to be allowed for in the costing of the transaction. These payments may be made to an ARS provider who acts as a clearing agent (settlement agent in the structure of a remittance operation diagram above) for the transaction.

#### *Offset of Remittances*

Settlement by back to back transfers<sup>5</sup> is a preferred method as it is the easiest and the most efficient. In this system each ARS provider is the originating ARS for one transaction and uses the funds to act as the destination ARS for another. No funds need to be moved and two commissions are shared between the two ARS providers. This is the principal on which multi-national franchised ARS operations work, but it is equally the ideal solution for informal systems.

This category also includes manufactured offset of remittances. For example, an ARS operator in a country with a high level of migrant remittances may pool the proceeds of multiple transactions in order to use this money to make a single commercial remittance to a third party. This activity is

---

<sup>5</sup> Formally, this process could be more precisely qualified as “clearing”

common between Europe and South Asia, but it is a high risk as a method of settlement as it may facilitate export and import fraud.

The settlement flows will usually be different from individual customers' remittances flows. The ARS provider may pool the cash from the individual remittance transactions, and a large single transfer may then be made at a later date in order to settle all the previous remittance transactions. This both limits costs and allows the exploitation of cash balances and means that settlements cannot necessarily be traced back to the specific transactions. Unscrupulous ARS providers can use this method to cloak transactions relating to ML or TF.

### *Physical Cash Movement*

Cash deposits can be a logistical problem for unlicensed or illegal ARS. Cash couriers and smuggling is a common method of moving value to jurisdictions which have less experienced banks and cash wholesalers operating. It also allows profits to be taken on currencies in high demand by ARS providers.

### *Cash pooling accounts*

Cash pooling accounts are a common feature of complex ARS systems. They are used by multinational ARS providers to reduce the losses of currency exchange. Equally, they are used by informal ARS providers to facilitate complex settlements between different countries. The holder of the cash pooling account will have a series of accounts in different currencies; however, the US dollar has always been the predominant currency.

Money is transferred into the cash pooling account from customer transactions and used by the originating ARS provider. The value remains to the credit of the destination ARS provider. The originating ARS provider can use the money to settle past, current or future transactions anywhere in the world. These settlement transactions may be effected by making personal or commercial remittances. This allows a great deal of flexibility in pricing and completing transactions in a variety of currencies.

### ***Remittance Corridors***

Observing the settlement ARS flows it is possible to identify net sending countries and net receiving countries. In these circumstances those countries are linked to each other through a *remittance corridor*.

The term *remittance corridor* describes the bilateral flows between two economies, a sender and a receiver, the components of which include the *first*, *intermediary* and *last miles*.<sup>6</sup> The corridor is shaped by a market structure in the origination (*first mile*) and the distribution (*last mile*) defined by the stage of development of the financial sector and the access to formal funds transfer systems available in both ends of the corridor. The differences among remittances corridors are defined by the nature of the migrant sender, the type of flows that are transferred, the channels, the technology available and the incentives to choose a particular channel, among them the cost to transfer funds.

---

<sup>6</sup> These terms are used by the World Bank for the three stages of bilateral flows within a remittance corridor.

<b>Workers' Remittances<sup>7</sup> to Developing Countries (1990-2004)</b>								
<i>In USD billion</i>	1990	1995	2000	2001	2002	2003	2004e	Change 2004-2001
<b>Developing countries</b>	31.3	56.7	76.8	84.6	99.0	116.0	125.8	41.2
<b>Lower middle income</b>	17.5	34.8	41.9	44.1	49.1	54.8	55.6	11.5
<b>Upper middle income</b>	5.7	8.6	13.1	16.8	18.7	24.4	26.8	10.0
<b>Low income</b>	8.1	13.3	21.7	23.8	31.2	36.7	43.4	19.6
<b>Latin America &amp; the Caribbean</b>	5.8	13.4	20.2	24.2	28.1	34.1	36.9	12.7
<b>South Asia</b>	5.6	10.0	16.0	16.0	22.3	26.7	32.7	16.7
<b>East Asia &amp; the Pacific</b>	3.2	9.0	11.2	12.9	16.6	19.5	20.3	7.4
<b>Middle-East &amp; North Africa</b>	11.7	13.0	13.5	15.2	15.5	16.8	17.0	1.8
<b>Europe &amp; Central Asia</b>	3.2	8.1	11.0	11.4	11.5	12.8	12.9	1.5
<b>Sub-Saharan Africa</b>	1.9	3.2	4.9	4.9	5.1	6.0	6.1	1.2

Source: Global Development Finance 2005.

Significant remittance corridors include bilateral flows from the United States and Canada to Latin America and Asia<sup>8</sup>; from the European Union to Eastern Europe and North Africa; and from the Arabian Gulf to South and Southeast Asia. Other remittances corridors are present between developing economies (South-South remittances corridors)<sup>9</sup>. Early research reveals that the US-Mexico remittances corridor is a “mature” market for formal remittances, while the Canada-Vietnam corridor is at a “nascent stage” in the shift to formal systems. Both share some of the same challenges. But whereas a mature market has formal channels for remittances, one that must be maintained and expanded, the nascent market must focus first on setting the conditions for efficient remittances mechanisms that promote the entry of more formal market players and trigger the interest of the private sector on developing new transfer products.

This report outlines the importance of remittance corridors developed by ARS providers in response to the demands of migrant workers. These corridors are dominated by the need for migrant communities to maintain family and business ties with their home country but can also be exploited by unscrupulous ARS providers to effect illegal transactions which are buried among the many legitimate migrant remittances. These corridors converge in countries with large resident migrant Diasporas who wish to make payments home to their families in countries such as Pakistan, India, Philippines and South America. It is estimated that the largest corridor could be between the Middle East and South Asia, with a full range of ARS providers capitalising on the genuine desire of expatriate workers to send parts of their income home. These migrant remittances are numerous but small. A study carried

<sup>7</sup> The term *remittances*, as used here, includes the sum of workers' remittances, employee compensation and migrant transfers.

<sup>8</sup> Visit [www.amlcft.org](http://www.amlcft.org) for further information regarding the World Bank's work pertaining to the United States-Mexico and Canada-Vietnam remittance corridors.

<sup>9</sup> The World Bank's Bilateral Remittance Corridor Analysis (BRCA) is aimed at developing a better understanding of the incentives and other factors that shape the remittance markets in sender and recipient countries in order to promote effective policies that will induce a shift from “informal” to “formal” funds transfer systems. Currently the World Bank is conducting the following case studies: United Kingdom – Nigeria (in partnership with the UK Department for International Development (DFID)); United States – Guatemala; Germany – Serbia and Italy – Morocco (in partnership with the *Ufficio Italiano dei Cambi*). Additional studies are planned between the Middle East and South Asia and between Southeast Asia and South Asia.

out by the UK Department for International Development (DFID) suggests that a family average of GBP 250 per month is remitted from the UK to the country of origin of the migrant. In the US-Mexico corridor, according to the Mexican Central Bank, the average remittance amount is USD 327 per month. The average amounts remitted from the Middle East may be smaller.

Some ARS transfers between countries are not direct. ARS transfers to South Asia, for example, tend to be routed through the UAE. Similarly, worldwide remittances to Somalia often pass through the exchange houses of Dubai. This is a regulated sector that is prepared to act as a regional bridge between the regulated and unregulated sectors. Examining the remittance corridors highlights the role of regional financial centres in remittance activity.

Although regulations can have a strong impact on the form and characteristics of the remittance market, the supply of ARS services is in principle strongly demand-driven. Apart from demand, there are other factors that influence the supply of ARS providers. One of these is the clear connection to the size and composition of immigrant communities and / or the existence of a strong informal economy. The tendency of ARS to shift spontaneously to the formal/regulated sector has been detected in some regions, most likely determined by the intention of conventional banking or other legal financial services to exploit the market of immigrant remittance payments by developing economic incentives to attract this potential source of customers. In such circumstances, the cost of the legal/regulated channels may tend to decrease, as an effect of enhanced competition.

## **REGULATORY SYSTEMS**

As becomes evident from the table on regulatory framework (see Table on Regulatory Framework at the end of this chapter), which gives an overview of the regulatory framework in a sample of 12 countries, the way ARS are regulated in different jurisdictions varies substantially. At one end of the range, there are countries that require a banking licence for all institutions that transfer money. Although there are no such countries included in the table there are also very few countries (mainly in the developing world) where there are no regulatory requirements for ARS at all. The large majority of countries is between those two extremes and applies some kind of specific regulatory regime to money remitters outside the banking sector.

In most cases there is one regulatory regime that applies to the entire ARS sector, although there are examples where countries apply a lighter or voluntary regime to certain categories of providers (*hawaladars*) or where a distinction is made between smaller and larger providers.<sup>10</sup>

The most important distinction is between countries that only require the registration of money remitters and those that have a licensing procedure. Both systems are mentioned as legitimate options in the FATF-recommendations (recommendation 23 and SR VI). Countries with a licensing regime use various criteria for the granting of a licence, including fit and proper tests for the owners and managers and the existence of business plans. Many of these countries also apply additional regulatory requirements, such as an appropriate internal organisation as well as certain financial criteria to protect customers.

In countries with a registration regime there is no requirement to obtain a licence before an operator can start providing money remittance services, even though there is a requirement to register. In addition the regulatory regime in these countries is often relatively light and in most cases does not entail other provisions than those which are required to combat ML and TF.

The differences in the regulatory regime in different countries are largely mirrored in the way these entities are supervised or monitored. Supervision in a licensing regime is often in the hands of a financial supervisor, entails regular on site visits and strict reporting requirements and goes beyond

---

<sup>10</sup> The UAE, for example, has developed a registration system for hawala operators. For additional information, visit: [www.cbuae.gov.ae](http://www.cbuae.gov.ae)



AML-CFT-requirements. Under a registration regime the checks are substantially less frequent or more “risk-based”; the monitoring focuses mainly or exclusively on AML-CFT-requirements and is often implemented by other entities, such as the FIU, the tax authorities or the customs authorities.

Whether a country has a licensing or registration regime, most countries apply the regular AML/CFT-requirements to the ARS-sector, in particular the requirement to keep records, identify customers and to report suspicious transactions. Relevant differences occur in the thresholds that are applicable for the identification of customers, which vary from zero to EUR 15,000, and in the fact some countries require all transactions above a certain threshold to be reported (in addition to the reporting of suspicious transactions irrespective of the amount). Countries that apply a high threshold for identification will have to shift to a lower (or no) threshold to meet the requirements in Special Recommendation VII (a maximum threshold of USD 1,000).

The need to prevent criminals or their associates from holding or being the beneficial owner of significant controlling interest or holding a management function in a financial institution is dealt with differently in different regulatory systems. While most licensing systems have some kind of fit-and-proper test that includes a check on the criminal records of owners and operators, registration systems often make use of more risk-based methods to prevent criminals from penetrating the remittance market. There is an ongoing debate on the effectiveness of both systems. It is clear that country specific circumstances will have to be taken into account.

Finally, it is worth mentioning that money remitters are now subject to the revised FATF Recommendations of 2003, which require countries to impose additional obligations on all financial institutions (and certain other professionals), such as the identification of the beneficial owner of customers and the development of internal policies, procedures and controls. Although these requirements can be implemented in a risk-based fashion, this will of course ask for additional measures in the sector.

## **TYPOLOGIES**

### **Categories of Alternative Remittance Systems**

The cases available show that some uniform categories of ARS are identifiable based on the structure of the business. The relevant categories are the following:

- Franchised multinational companies
- Multi premises or franchised national companies
- Signed shop-front premises (one or more premises)
- Overt ARS within another business
- Covert ARS within another business
- Covert ARS – no premises

#### *Franchised Multinational Companies*

This category includes ARS products offered by various large and often well-known international corporations that provide money transfer service through franchises. These operators tend to have a high degree of compliance with local legislation, also by providing effective procedures to prevent misuse. This is reflected in the relative expense of the service. The providers are household names, and their services are accessible around the world.

With franchised multinational companies, there is a fixed fee structure, and exchange rates used are often less competitive. These operators provide an accessible, quick and reliable service. They are undercut by a whole range of ARS operators but are still used by ordinary customers in preference to other ARS operators. This is an indication that some ARS customers value a reliable and legitimate service above other factors in selecting an ARS provider. They have sophisticated computer systems to ensure transactions are completed accurately and to prevent fraud against their services. All transactions can be traced, and they tend to have clear policies on identifying customers and reporting suspect transactions.

Multinational companies are increasingly providing online and remote payment services. This increases the volume of transactions to be examined for detecting suspicious activity and may lead to problems in defining risk. Online services require use of bank accounts that provide a better audit trail.

Terrorist financing through this form of ARS will be difficult to identify. Embedded terrorist groups will be able to provide identification, and the amount transferred by each individual element of a terrorist operation will not lead to suspicion. The computerised tracking systems do however mean that historic transactions can be scrutinised effectively.

#### *Multi-Premises or Franchised National Companies*

These ARS are the next level in scale after the multinational companies. Within a particular country or community, these businesses are a recognised brand. They tend to support efforts to licence or regulate ARS services often have established and effective methods for identifying their customers and reporting suspicious transactions.

ARS operators from this category servicing migrant workers in the UAE, for example, have developed “membership” schemes to streamline and reward frequent customers. This allows the ARS operator to conduct a high level of *know-your-customer* (KYC) procedures when enrolling a customer, who is given a unique number and photo identification card. Beneficiary names and, where possible, account details are also embedded in the card data file. Monitoring this “account” then allows the identification of suspect transactions against a profile of normal activity. These operators will often act as franchisees of the multinational companies but will also provide their own rival services. They tend to provide remittances to or through banking channels, making use of electronic transfers or bank drafts.

Franchised national companies compete with banks and multinational companies by knowing their market and using economies of scale to provide better exchange rates or cheaper charges. This tier of ARS tends to be vigilant. Where they serve a particular ethnic group or community they are well placed to identify normal levels of transfer and so identify what is abnormal. The risks they face are similar to multinational franchised operations. In addition, they are vulnerable to organised smurfing which exploits the availability of rival companies servicing similar communities.

Where they offer commercial services they can be abused in large scale frauds, either as the remitting or receiving company. This means they have to be particularly careful to identify the source, destination and business reason for transactions. Cash is a risk as with all ARS but bank to bank transfers via ARS in this tier are a particular risk.

#### *Signed Shop-Front Premises (one or more premises)*

These are familiar premises wherever ARS can operate legally. They generally serve a particular ethnic community and provide it with a cost effective and valuable service. They tend to be family run and are sometimes identified as “Mom & Pop” operations within United States.

They can provide a cost effective service by using efficient settlement methods and making economies of scale on bank transfer costs. They may use the services of another ARS to make transfers if this is most efficient.

Customers either make cash deposits at the shop-front premises or make payments directly into the ARS provider's bank account. Direct cash deposits into their bank account help the shop-front ARS provider to streamline cash control, but there is a risk that they do not truly know their customer. The ARS operator will have a series of linked payment agents in the countries they serve. These payment agents may range from similar operations to individual *hawaladar*. The ARS will use an exchange rate agreed with their partner agents in the destination countries. These rates will constantly fluctuate.

Settlement will be by a form agreed with the destination agent. This tier will be particularly likely to use cash pooling accounts, back to back transfers and third party payments. A family business of this nature is particularly vulnerable to ML, either through having inadequate internal controls or through becoming complicit with criminal groups.

#### *Overt ARS Operations within Another Business*

These operators are visible, but do not necessarily advertise their services. This tier of ARS operator can be similar to a shop front ARS operator, with the same risks. In the same way as a franchise agent of a multinational ARS operator, they offer remittance services to local customers in addition to their normal business. The provision of remittance services may complement their normal business activity or be a totally separate venture.

Where there is a registration or licensing regime, these ARS operators can be effectively controlled as long as their services are identified. Risks include those generated by possible commingling of funds coming from different activities. That could cause difficulties in the proper application of AML/CFT measures, also breaking the audit trail.

#### *Covert ARS Operations within Another Business*

Covert ARS operation within another business is the first category where the operator will actively seek to work outside the regulatory regime. A covert ARS operation will be illegal in that it operates without a licence or registration. It also violates regulatory provisions by performing ARS operations without carrying out necessary AML/CFT measures, such as identifying customers, recording transactions or reporting suspicious transactions. It is also likely to commit banking offences such as "structuring" where deposits are made below a disclosure limit to avoid identification of the ARS activity.

ARS operators in this category tend to serve a particular migrant or ethnic community. They rely on referrals within the community they serve. This category will include most *hawaladars*, unless they are registered or licensed. This category of ARS operator is particularly strong in communities where mainstream banking is not freely available in the destination country. This has been demonstrated in Somalia where overt and covert ARS operators dominate home remittances worldwide since there is little if any developed formal banking system.

This category will be most likely to use forms of settlement that do not rely on bank transfers, but because their transactions will tend to flow to one country they may still rely on depositing cash into a bank account in the other country in order to effect an offsetting settlement.

Suspicious transaction reports from banks or referrals from another FIU are the most successful methods of identifying these ARS operators. Information gleaned from the community these operators serve is also valuable. In some cases, this category of ARS operator will be resistant to AML procedures. Their informality is key to their selection by individuals who may be operating illegally or within the "grey" or "cash" economy.

To law enforcement this tier is high risk for ML and TF. Even many “bona fide” ARS operators in this sector hide the volume and detail of their transactions. This secrecy or lack of transparency is a product of their history and business methods; however, it is this aspect of their operations that arouses suspicion among law enforcement personnel, since a lack of transparency is often a key factor exploited by criminal misuse of certain financial channels.

The success of criminal money launderers is directly related to their ability to handle large amounts of cash covertly. Law enforcement experience has shown that successful covert ARS operators involved in criminal ML quickly attract levels of cash that make detection easier. Having an entire business that is cloaked in secrecy where illicit and genuine transactions take place, allows the criminal money launderer to hide more of the illegal business. In some cases, criminal money launderers may also progress to overt operations to ensure they can obtain banking facilities to service criminal customers.

In TF significant transactions may be small. There is no way of measuring the importance of covert ARS operators in TF without better intelligence on their activities. However, logic suggests that a covert ARS operator embedded in a community which also contains covert terrorist cells will be the natural first port of call for transactions. Terrorist cells have used franchised multi-national ARS operators, but this was in a situation where they were operating in a country where they were not supported by an embedded ethnic community.

#### Case Example 1

An investigation was conducted based upon the filing of four suspicious transaction reports on A Inc. of USA, a licensed ARS service provider operating in New Jersey. Although A Inc. of USA was a licensed service provider, the owners and operators of the service conspired with four unlicensed money remitters (couriers) operating out of New York to commit the criminal acts. The four couriers brought large sums of cash to A Inc. that were deposited into the business' bank accounts and then wired to the Middle East. A Inc operated with a very limited number of clients, but was responsible for over USD 100,000,000 in cash deposits over a 30 month period – all of which was ultimately transferred to Pakistan. A . Inc failed to complete the appropriate currency transaction reports and created fraudulent foreign exchange records. An unidentified employee attempted to deposit over USD 10,000 in cash and refused to provide identification when requested by a bank official. The bank then contacted the ARS owner and advised him of US Bank Secrecy Act regulations and bank policy.

Source: United States

#### *Covert ARS Operation – No Premises*

A covert ARS operator having no specific premises may operate in the same way as the previous category. They also include criminal ML groups who act as purely criminal ARS operators. These ARS groups will use the services of overt and covert ARS operators to move money within their systems, but they also act as their own network. The UK has reported a series of criminal ML operations from 2000-2005 which have led to the definition of roles of key players within these networks.

The roles of key players within criminal ML networks can be broken down into three distinct functions: *control*, *collection* and *cash disposal*.

- **Control.** The controller organises the ML activity and thus has a complete overview of the operation. He buys cash from criminal groups and arranges payment at the destination chosen by the criminal. The controller may be associated with an ARS operator and is normally based in a third country, often in South Asia or the Middle East. The controller employs collectors to gather cash and disburse the money on his behalf. Finally, he uses various ARS techniques to move money or value from the originating country to cash pooling accounts, third party accounts or to settlement accounts via back-to-back transfers.

- **Collection.** The persons carrying out the collection function serve as the interface between the ARS operators and the criminal customers. The collector receives instructions by mobile phone or SMS from the controller with details of criminal customers who are holding cash. He may use pre-paid mobile phones to contact the criminal and collect the cash in a covert meeting. The collector counts the money and reports any shortages or counterfeit notes and stores the cash in a safe house and then disposes of the money on instructions from the controller.
- **Cash disposal.** For this function, funds may be sent to destination parties or third parties by money transmission through complicit ARS operators. Cash may be moved by organised cash couriers to jurisdictions where the banknotes can be safely sold. The funds may also be used to complete back to back transfers through *cuckoo smurfing* (see below). Finally, the money is handed over to individuals or criminals who want to receive cash. This may complete a separate criminal ARS transaction, including “grey economy” transactions

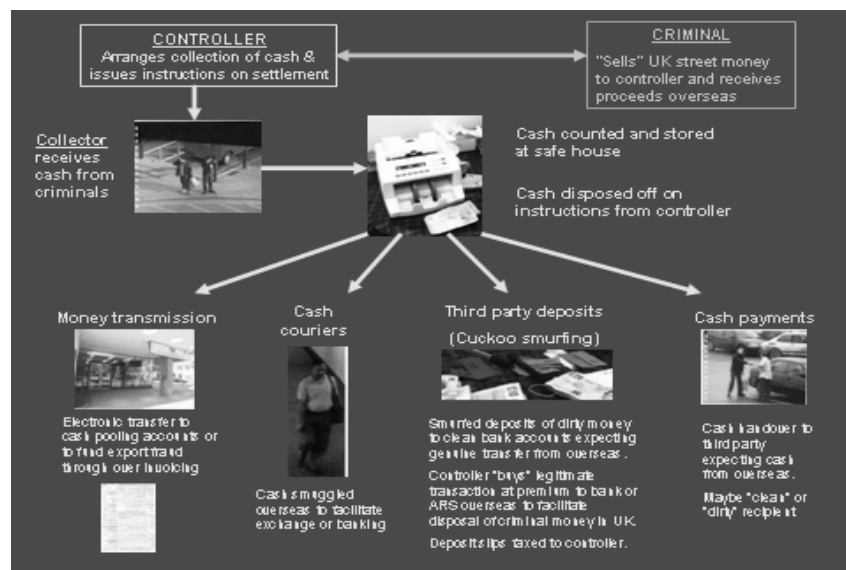


Figure 3: Key players within a criminal ML network; Source: United Kingdom

### Some Typologies Illustrated by Specific Case Examples

The cases obtained as part of this study showed a number of different ways that ARS could be misused for ML or TF purposes. The cases have been grouped into the following three areas:

- ARS operations in which the provider is fully involved in the ML/TF activity;
- ARS operations in which the provider has some knowledge of the ML/TF or other criminal activities carried out by the customer;
- ARS operations in which the provider has no knowledge of the ML/TF or other criminal activities carried out by the customer.

#### ***ARS operations in which the provider is fully involved in the ML/TF activity***

##### *Typology 1: Cuckoo Smurfing*

Cuckoo smurfing is a term used to describe an increasingly common ML technique associated with ARS that has been identified in the UK and elsewhere in Europe. The process involves the transfer of criminal funds through the accounts of unwitting persons who receive funds or payments from overseas.

## Case Example 2

An ARS in South Asia or Middle East contracts or otherwise obtains private and commercial transfers to Europe. In some instances, bank managers in Pakistan have been known to sell – ARS operators – genuine personal electronic transfers to be performed on behalf of their customers.

The controller uses criminal cash held in Europe to complete the transfer. The collector is provided with the account details of the recipient, who is expecting a transfer from the ARS or bank. The collector pays the criminal cash into the recipient's bank account. He uses multiple branches of the bank and makes a series of deposits at a level that is unlikely to raise the cashier's suspicion.

The collector faxes the payment slips to the controller as proof of payment to the customer. The operator of the bank account will then be contacted to be told the transfer is complete with copy payment slips if necessary.

This system exploits the bank's relationship with its customer. The recipient is a bona fide bank customer who has passed all KYC requirements. He has no control over the origin of the deposits or who is making them, and banks currently conduct no identification on the depositors of cash into a third party account.

Source: United Kingdom

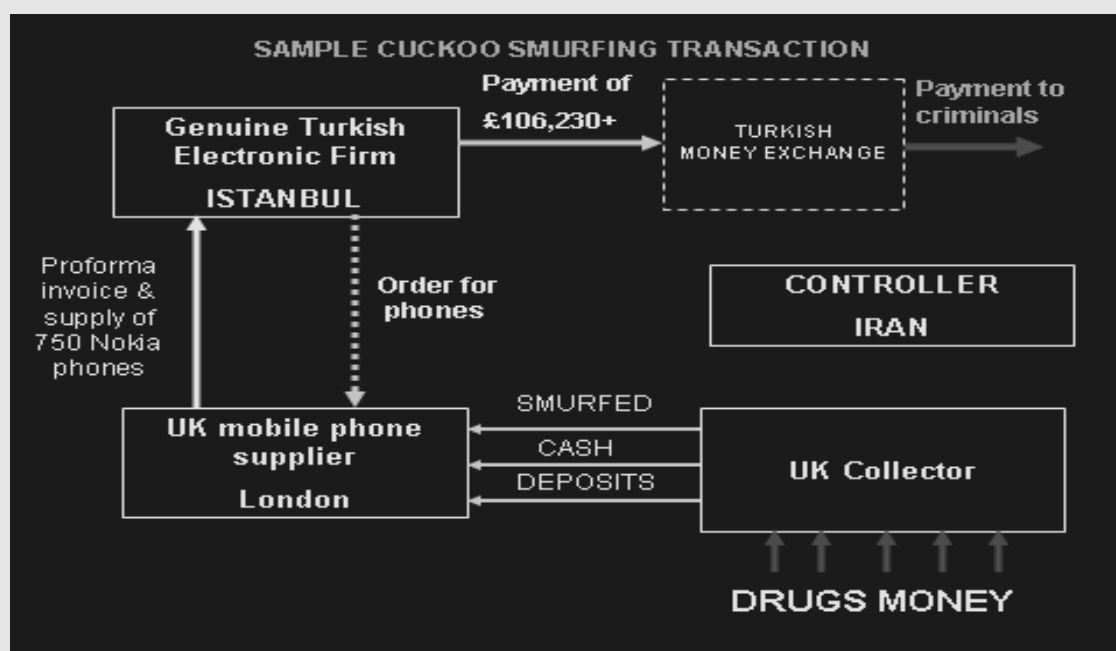


Figure 4: Sample "Cuckoo" Smurfing Transaction. Source: United Kingdom

### Analysis of Case Example 2

*Cuckoo smurfing* allows a controller and an ARS to oversee payments made in another country without the risk of being detected. They operate the system to dispose of large amounts of criminal cash without having to hold bank accounts in their own names.

Banks can recognise this type of activity by looking for unusual cash deposits that are structured in smaller amounts or made away from the customer's branch. They can prevent the activity by challenging depositors for identification when they pay cash into a third party bank account.

Banks have a good record of identifying the activity and making suspicious transaction reports after the event, but they have no means of identifying the collector. International exchange of intelligence

between FIUs and law enforcement can help to disrupt the ARS operators who collect legitimate transactions to sell to the controller. This technique can be operated alongside cash pooling accounts.

### *Typology 2: Anomalous Use of Bank Accounts*

#### **Case Example 3**

An investigation was started by the police following anonymous tip on the activity of Mr. B, who was the manager and the principal shareholder of company C, believed to be part of a ML network between France and Colombia.

In his shop, Mr. B sold prepaid phone cards, Colombian food products, airplane tickets and above all, provided to the Colombian community living in France and to Colombians working illegally, short term credits, money exchange services, cheque cashing and money transfers to Colombia. International remittances were the largest activity for company C (approximately 85 % of its turnover).

Mr. B organised a system that allowed money transfers between France and Colombia with the direction of remittances primarily from France to Colombia. Mr. B had bank accounts and capital available in Colombia. He arranged for family members in Colombia to give pesos to the beneficiaries of these transfers. The people who sent the money deposited French francs or US dollars directly into Mr. B's account in Paris. So, at the beginning, there were operations of clearing or settlement without any money being transferred from France to Colombia.

The service provided by the company C had two advantages: confidentiality and speed. The increasing amounts of the money transfers from France to Colombia forced Mr. B to use cash couriers who, for reasons of friendship or in exchange for airplane tickets, accepted to transport bundles of cash that weighed up to 40 kg.

In order to ensure the security of cash transfers, Mr. B started to use, at the beginning of 1999, a company specialising in international remittances. The company E, based in Madrid, held a bank account in bank F in Paris, and similar companies G, H and I, were later used.

Company E's transfer orders were directly completed by the client on a company E dispatch note. Then, Mr. B sent it by fax to the company E. The investigators discovered that the transfer orders were also sent by e-mail. Mr. B deposited cash into the account opened by company E in bank F. Mr. B generally required his clients to divide their transactions into smaller amounts whenever they were above USD 3 000.

The fact that company C was primarily an illegal transfer business became evident through the study of dispatch notes. From 4 September 1999 to 30 September 1999, intercepted faxes indicated some 3,600 transfers to Colombia. They represented an amount of FFR 13 million (approximately EUR 2 million). These operations involved 1,300 recipients in 78 cities in Colombia and 900 bank accounts in 40 different banks.

As of March 2000, the investigators saw a dramatic increase, in the number and volume, of transfers made by company C. It corresponded to the fact that Mr. B was allowed to deposit checks into company E bank account in bank F. If company C made the transfer without middleman, it received a 5 % commission of the amount of the transfer. When the cash went through companies E, G, H or I, Mr. B shared the commission. The use of these companies presented the advantage of minimising the risk of loss or the risk of confiscation.

Mr B was sentenced to 3 years imprisonment (including 2 years of suspended sentence) in 2004. Other members of the system also received jail sentences.

Source: France

#### *Analysis of Case Example 3*

In this case an ARS operator has exploited different regulatory regimes to enable him to operate in a jurisdiction that prohibits all ARS. A combination of offset remittances, anonymous bank deposits and bank transfers are used to remove the proceeds. The operator services legitimate and criminal customers. He is identified through anonymous information, although the bank deposits should lead to his identification. Criminal ML is disrupted through prosecuting an ARS operating outside the regulated sector.

### *Typology 3: Book Keeping Practices*

#### **Case Example 4**

Individuals involved in informal ARS activities maintained two different sets of books. The official set of books for the tax authorities only indicated the batch transactions between the relevant bank accounts and foreign transfers. The second set of books indicated details of all the deposited money, including the names of the depositors, the names of beneficiaries, the countries of destination, informal ARS partners in the country of destination and the transferred amounts. This second set of books was maintained in the native language of the representative, and it included bookkeeping records, receipts of deposited money, fax message lists to ARS partners in the countries of destination with information about the people who deposited the money, who received money and the transferred amounts.

Source: Sweden

#### *Analysis of Case Example 4*

This example illustrates the importance of appropriate attention to bookkeeping practices by competent authorities.

### *Typology 4: Over-invoicing Exports*

#### **Case Example 5**

An ARS service provider operating in the European Union had a genuine relationship with an ARS provider in South Asia. The South Asian provider made payments for remittances originating from Europe, but asked that the ARS in Europe pool the cash it received for these remittances. The European ARS provider then issued instructions to make single large payments to third parties in South Asia. The beneficiaries of these electronic payments were exporters who had overstated their exports to . The receipt of funds from Europe was then used to validate their claim for a tax rebate for business on the direction of the ARS.

Source: UK

#### *Analysis of Case Example 5*

In this case, the ARS operator controlling the pool of cash uses the money to finance a fraud. In so doing it can also obscure the audit trail of criminal funds. The involvement in fraud to generate funds that can subsidise their legitimate activities. This is a key element to the offsetting of remittances.

Sharing of intelligence between jurisdiction and an understanding of frauds in the destination countries is necessary for banks and regulators to identify this activity

### *Typology 5: ARS Operation Used as a Cover for Drugs Money Laundering*

#### **Case Example 6**

In this case, an ARS operator in the United Kingdom was complicit in laundering funds generated from heroin trafficking. Money was collected from criminals and deposited at his shop-front ARS premises run as a family business.

The ARS operator acted as a genuine remittance business for the local South Asian community. At the counter there was a list of associated payment agents, and cash was accepted for genuine migrant remittances. This money was transferred electronically to the destination country in bulk transfers, and remittances were paid out at the receiving end in cash or by cheque.

Separately the ARS operator also received deposits of GBP 50,000 to GBP 500,000 that had been collected from criminals. The ML was controlled by key individuals located overseas. They recorded the deposits in a second set of books.

The ARS operator used his banker's security van service to collect the cash from his premises to be deposited into his GBP account. The ARS operator transferred the proceeds into his US dollar account at the same bank. He then transferred the



money to cash pooling accounts on the direction of the controller. These accounts were US dollar accounts held by money exchanges in the UAE. The money was then disbursed on instructions from the controllers, who used back-to-back transfers to break the audit trail.

The banks submitted suspicious transaction reports but generally accepted that the money originated in the local migrant community. Better KYC and understanding of the community would have identified that the cash volumes were highly suspicious. Cash volume and regularity of deposits were the key ML indicators.

The cash received by the ARS operator was highly contaminated with heroin, cocaine and ecstasy.

Source: United Kingdom

### **Case Example 7**

A travel agency serving a South Asian community provided money transmission services for families and migrant workers. An overt ARS section was set up within the business. The ARS services were openly disclosed to the business's bankers. These offences occurred before a registration scheme was set up, but there is no doubt the firm would have registered.

Genuine remittances were performed, but large criminal deposits were also knowingly accepted. Collectors received money from criminals and after counting the money deposited in the accounts of the ARS operator. Deposits were sometimes accepted away from the business premises to avoid surveillance.

The ARS recorded the deposits in a separate informal set of records:

The ARS operator deposited the cash received in a bank account and then made transfers on instructions from the controller in the UAE.

Payments were made to cash pooling accounts controlled by the ARS operator in the UAE and were then also used to complete separate commercial remittances. The scale of deposits, inability to explain the source of the cash and documentation that was maintained helped to prove the ML case. The principals of the ARS pleaded guilty to drugs ML.

Source: United Kingdom

### *Analysis of Cases Examples 6 & 7*

Both of these cases show that the banks should have better understood their customers' business and the community they serve in order to detect this activity. The key indicator was the regular high level of cash deposited, which was far in excess of the money that could be justified by migrant remittances.

As part of their KYC the banks would have had to question the commercial reasons for the use of bulk US dollar transfers to third parties. This is not in itself an indication of criminal activity, but the ARS operator making the transfer should normally have been able to explain the purpose of the transfer.

For regulators, a comparison of the records maintained by the ARS operator and its bank account would have shown an excess of cash deposited. ARS operators have been noted creating elaborate false records of customers to hide deposits of large amounts of cash. Often customers that have been falsely cited as having made remittance transactions by an ARS operator can become good witnesses for the prosecution.

The ARS operator maintained a second set of books to record the criminal transactions. These were hidden but discovered in the searches of the premises. Increasingly ARS operators are aware of law enforcement techniques and thus maintain their second set of books — containing records of the cash taken in and processed on behalf of criminals — at locations other than their business premises.

Timely international judicial co-operation can be essential to obtain further evidence for the lack of legitimate business explanations for remittance transactions and for disrupting the activity overseen by the controller of the ML operation.

*Typology 6: Regulatory Investigation Detects and Disrupts Terrorist Activity*

**Case Example 8**

MH and his brother were arrested during a crackdown on Somali ARS outlets operating across the United States. In August of 2000, the ARS operator filed an application with the Massachusetts Division of Banks and Loan Agencies for a licence to receive deposits and to transmit money overseas but was never issued a licence. In fact, the Massachusetts Division of Bank and Loan Agencies warned the brothers on two occasions that it was illegal to engage in the business of transmitting money overseas without a licence. The investigation found that the Hussein brothers wired about USD 2.8 million to an account in the United Arab Emirates between September 2000 and November 2001, even though the brothers knew they were breaking the law by not having a state licence. It has been alleged that the profits supported terrorism. MH was convicted in April of 2002 of two counts of illegally transmitting money abroad.

Source: United States

*Analysis of Case Example 8*

This is a case where investigation and prosecution for operating an unlicensed ARS service can be used as a method to disrupt a perceived threat of TF. In some jurisdictions, evidence that an ARS operator is acting illegally is more easily obtained than evidence of the larger offence. Disruption of this kind can prompt the formation of a licensed sector serving migrant groups. Education and outreach programmes can help ARS operators to understand their obligations and can serve as the basis for a future prosecution.

Handling large amounts of cash make the ARS visible to banks and law enforcement. Understanding the settlement methods and sharing intelligence with the authorities in jurisdictions holding the cash pooling accounts can be effective in identifying the activity and disrupting money laundering or terrorist financing.

*Typology 7: Multiple Bank Accounts Opened to Facilitate Cash Deposits*

**Case Example 9**

Several individuals originating from the same region in Asia and residing in Belgium opened accounts, generally with different banks. Deposits were made to the accounts mainly by cash deposits and, to a lesser extent, by transfers from individuals of the same origin also residing in Belgium. These accounts were then used as transit accounts, and the funds were immediately transferred to Asia. The total sum of the transferred funds was very large, up to several thousands Euros. These large sums did not correspond to the socio-economic profile of the account holders involved, who generally received social welfare benefits or who were asylum seekers. The funds were transferred to accounts of individuals or legal entities active in underground banking systems in Asia. Several individuals were known to the police for trafficking in human beings. These files were transmitted to the judicial authorities for further investigation and prosecution of the human being trafficking offence.

Source: Belgium

*Analysis of Case Example 9*

Criminal proceeds, including those involved with human being trafficking, are normally in cash. An ARS operator acting covertly without premises will need access to bank accounts to process large amounts of cash. Personal accounts operated by members of the ARS operators' community can be abused. These accounts can be detected because of the high frequency of deposits, the large number of banks used and the transfer of money to pooling accounts. Identifying and closing the cash pooling accounts disrupts the whole activity.

### *Typology 8: ARS Operators Involved in Trade-Based Money Laundering*

Trade-based ML as an alternative remittance system provides illegal organisations the opportunity to earn, move and store proceeds in a global arena in what appears to be legitimate trade. Unlicensed ARS operators also utilise trade as a method to transfer value to foreign destinations. Unlicensed ARS can transfer value by purchasing commodities and sending them to foreign destinations. The commodities are then sold and the proceeds remitted to the intended recipient. The following series of five cases illustrate this typology.

#### **Case Example 10**

An investigation of individuals operating an ARS revealed a method for converting large amounts of funds into commodities. Funds were collected in the United States, placed into a corporate account with a US communications company and used to purchase pre-paid telephone calling card personal identification numbers (PIN). The PIN numbers were then sold in Bangladesh, thus converting the commodity back to cash prior to distribution to the intended recipients. Storing the funds as a commodity via the corporate account allowed for the movement of funds without utilising the formal banking system in Bangladesh.

The subject of the investigation wired the collected funds from the bank account into a corporate account with a large US telecommunications company on behalf of the ARS operator's Bangladeshi counterpart. The Bangladeshi counterpart controlled the corporate account. The Bangladeshi had set up the account based on a previously established business relationship with the US telecommunications company to sell phone card PIN numbers in Bangladesh. The Bangladeshi counterpart used the funds that the ARS operator deposited into the corporate account to purchase phone card PIN numbers from the US telecommunications company. The Bangladeshi then sold the PIN numbers in Bangladesh, thereby generating cash in Bangladesh for distribution to the intended recipients of the money service transfers originating in the United States. The scheme involved the transfer of USD 200,000 to USD 400,000 per month.

Source: United States

#### **Case Example 11**

A Washington DC based cab driver operated a money transfer business between the United States and Pakistan. Pakistani immigrants used the *hawaladar* (ARS operator) to send remittances to family members in Pakistan. The operator accepted cash, money orders and cheques, and he never charged his customers for the transactions. The ARS operator had several bank accounts at different financial institutions. Some of the accounts were opened using fraudulent identification. The ARS operator ensured that his cash deposits were under USD 10,000 to avoid currency transaction reporting requirements. The ARS operator conducted business from his apartment and his taxi. He also received money in the mail from New York and other Cities in the US. Information on the beneficiaries for individual transactions was sent to partners in Pakistan by fax. He maintained a handwritten log in Urdu to record customer information.

Settlement was accomplished by transferring the value of the currency to Pakistan via manipulation of trade. The Government of Pakistan provides exporters with a rebate on Value Added Tax (VAT). This creates an incentive to overvalue export shipments to receive a larger VAT rebate. In this particular case, the ARS operator had business relationships with several surgical instrument manufacturers/exporters in Pakistan. These exporters advised US Importers that they had to overvalue the cost of the goods but that they would have someone give them the additional funds. Many US exporters went along with the scheme primarily because the items were imported duty free.

The ARS operator provided the money he collected to US importers to make up the difference between what was owed and what was indicated on the invoice. These funds were then wire transferred by the US importer to the Pakistani exporter. The Pakistani exporter provided rupees to the ARS operator in Pakistan. He made his profit from the Pakistani export transactions. The rupees were then provided to the beneficiaries as indicated in the faxed instructions.

Source: United States

#### **Case Example 12**

Traffickers in Colombia exported gold bullion, which they falsely described in export documents as another commodity. The gold was then imported into the United States, and correctly described in US import documents. Jewellers in New York, who

were co-operating with the traffickers, melted the bullion and recast it into other shapes, such as nuts, bolts, wrenches and other tools. These were then exported to Colombia, where the “tools” were reformed into bullion, so that the cycle could be repeated.

Colombian export laws allowed the traffickers to earn credits for exporting a manufactured product from Colombia. By concealing that they were exporting gold, they were also able to conceal the transfer of value. The US importation of properly declared gold bullion allowed the traffickers to transfer funds offshore. The melting and recasting of the gold into common shapes allowed the traffickers to return the gold to Colombia while concealing the transfer of value. The reuse of the gold allowed the traffickers to earn additional export credits for the export of the same merchandise.

Source: United States

***ARS operations in which the provider has some knowledge of the ML/TF or other criminal activities carried out by the customer***

*Typology 9: Multi-Trader Intercommunity Fraud (MTIC)*

**Case Example 13**

In cases of this type, MTIC fraudsters engineer a chain of transactions within the European Union in order to allow an importer to disappear with a value added tax (VAT) debt that is collected by an exporter at the end of the chain. Vigilance within the domestic banking community has identified and disrupted the financial activities associated with this type of case.

ARS operators have been used unwittingly to receive money on behalf of a missing trader and then to remit the money to another ARS operator overseas. This allows the fraudster to use the ARS operation as a “client account” and provide a double break in the audit trail.

The transaction will appear normal to the ARS at each end of the transaction unless they are aware of the fraud profile. Knowing and understanding the nature of business performed by the remitter will generally reveal that the size of transaction can not be supported by the purported commercial activity.

Source: European Union countries

*Analysis of Case Example 13*

This type of case can involve an ARS operation misused by criminals or an operation that is involved more or less directly in the conspiracy. Transactions are typically large and frequent.

The ARS operator remitting the money and the ARS operator holding the cash pooling account can detect this type of activity by examining the business details behind the transaction. The money typically moves on very quickly to avoid possible detection. ARS operators receiving the electronic payments would need to compare details of the originator and ultimate beneficiary to determine whether the transaction makes business sense.

***ARS operations in which the provider has no knowledge of the ML/TF or other criminal activities carried out by the customer***

*Typology 10: ARS Used to Pay Costs of Drug Trafficking*

**Case Example 14**

A criminal group smuggling cocaine by courier from the Caribbean region to Europe used a multinational franchised operation to pay emergency courier fees. The organisation regularly recruited female couriers and sent them to the Caribbean on package holidays. The maintaining the supply of drugs to the islands was frequently difficult, requiring the couriers to stay longer.

The organiser used false names to pay cash to agents at a level not requiring identification. The couriers collected the money, which was sent to them in variations of their true name. This allowed them to await delivery of the drugs. Similar transfers were also made to the couriers bringing drugs from South America to the Caribbean.

This method was only detected when the principal was arrested for drug trafficking. Administration of the system meant he had had to record the transaction code, sender and recipient details to be passed on to the courier.

Source: United Kingdom

#### *Analysis of Case Example 14*

This is an example of a multi-national ARS with established AML controls being used by criminals to facilitate crime. The transactions are conducted using real or false transactions but rely on being merged with legitimate transactions to avoid detection.

Detection by the ARS operator requires an understanding of the role of the destination country in drug trafficking and in questioning the remitting customer about the purpose of the transaction. Law enforcement relies on good record keeping by the ARS to demonstrate the use of false identities in the prosecution of such cases. Access to records at both ends of the transaction is also essential.

### **ASSESSMENT OF RISK AREAS**

#### **General risk factors**

##### ***Terrorist Financing***

The level of vulnerability for ARS to misuse for terrorist financing differs from that associated with money laundering. In the terrorist financing area, the level of vulnerability may also differ according to whether ARS operations are used in providing funds for a specific terrorist action or if such operations are used in transmitting funds that have been collected from legitimate (or illegal) sources to support future terrorist activities. TF is difficult to detect and can involve clean sources of funds. It is important that ARS providers screen transactions and customers against relevant TF related lists.

The expenses of an individual terrorist or terrorist cell may well be small. Often cells are largely self-supporting and may derive funding from crime. The best defence against these transactions is the application of normal AML policies, that is, customer identification, know-your-customer procedures and suspicious transaction reporting.

With fund raising activities, know your customer procedures are equally important. Any sector may be used for these activities, but as AML procedures are implemented worldwide, covert ARS will become increasingly attractive to terrorist organisations.

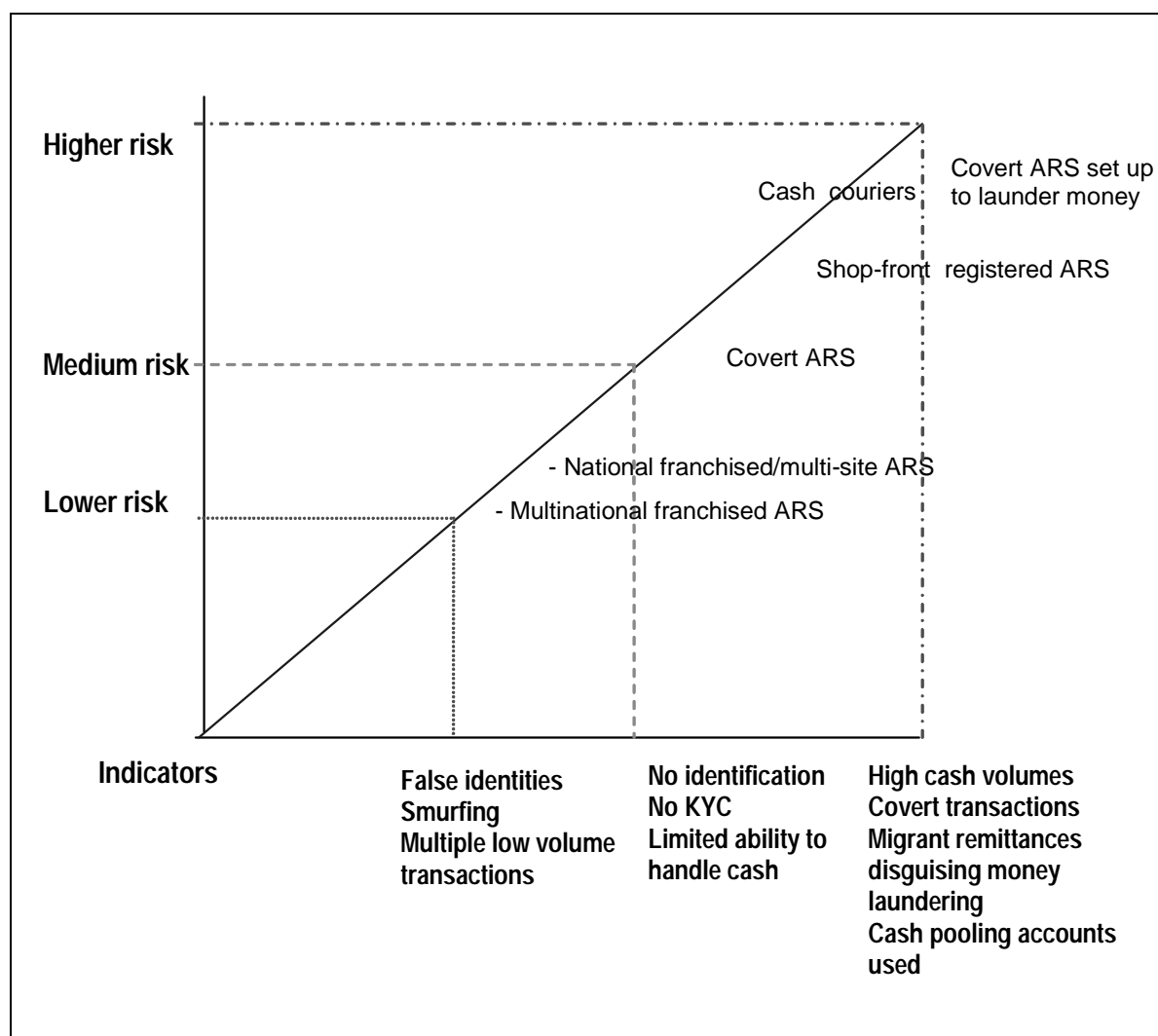


Figure 5: UK Risk Assessment; Source: United Kingdom

### ***Money Laundering***

The risks in ML are clearer. Any ARS can be misused to launder the proceeds of crime. The use of false identities and structuring are common techniques to which ARS is vulnerable. The highest risks, however, are to the ARS that can efficiently handle large volumes of cash. While specific risks will vary from one jurisdiction to another, several common elements can be identified. Some of the factors to be considered in assessing risks are:

- The effectiveness or existence of the regulatory regime;
- The volume and destinations of criminal money flows (criminal remittance corridors);
- The number and types of ARS operators;
- The extent of law enforcement interdiction and effectiveness of the suspicious transaction reporting regime;
- The extent to which banks provide accounts for ARS operations; and
- The size, origins and locations of migrant communities.

The risk analysis for each country will be different and should inform the regulatory and banking sectors. For example, a developing country relying heavily on domestic ARS and without the infrastructure to verify identity will face different regulatory challenges to a country with a developed formal sector. Although risk assessments may vary depending on jurisdiction, the chart in Figure 7, which illustrates the situation in the United Kingdom, may serve as an example of such an assessment.

### **Risk Associated with Specific Types of ARS**

Analysis of the corridors — both for legitimate remittances and for the flows of criminal funds — should also be considered when determining the level of risk to a particular national remittance sector. As mentioned above, the general risk factors vary somewhat from one jurisdiction to another. Likewise, the risk-related features associated with specific categories of ARS are different depending on the location, although common elements can be identified.

#### ***Franchised Multinational Companies***

This sector typically requires identification for low transactions as well as limitations on the maximum amount that can be transferred. ML activity is most likely to involve the use of false identities and structuring. Complicity of franchised agents at the originating or beneficiary end of the transaction increases the potential for large scale laundering. The speed and good reputation of the operators means that they will be selected by criminals and terrorists for important transactions, such as in Typology 2. (This sector is quickly diversifying into e-money, cash-backed credit cards and trade payments, which each hold their own risks.) Strong AML monitoring and analysis of transactions are the key to identifying illegal activity.

These operators have relatively low thresholds for identification and performance of customer due diligence. It should be noted that large scale ML – for example, involving amounts greater than EUR 100,000 per day – would generally pose more of a risk of detection for the money launderer. For this type of ARS operator, large scale criminal operations may therefore employ such methods as carrying out sophisticated smurfing operations, as well as using false identities. Otherwise, such operations may have to resort to attempts to co-opt employees of the ARS provider. Computer surveillance systems can be effective in identifying misuse of their services.

#### ***Multi Premises or Franchised National Companies***

The degree of risk to this sector varies according to the level of effective regulation in its centre of operations. Typically, these companies have implemented robust AML procedures that are tailored to match the customer base they serve. Domestic top tier companies in jurisdictions such as the UAE have set up personalised photo ID schemes which allow the monitoring of transactions and the comparison of volumes to assessments of the customer's lifestyle. The risks in this sector are likely to be similar to franchised multinational companies but can differ greatly in an unregulated country or where the operators are complicit. Bankers for this sector should be familiar with their customers AML program and should be vigilant that the accounts are not operated as cash pooling accounts.

#### ***Signed Shop-Front Premises (one or more premises)***

This sector operates openly and should thus be subject to effective regulation. Individual cases have shown that, when such ARS operators are complicit in criminal ML, they can be the largest volume offenders.

#### ***Overt ARS within Another Business***

This sector has the same potential as the previous sector but with turnover limited according to banking arrangements of the individual operator. There is a risk that the turnover may be disguised by mixing money in ARS and trading accounts. The indicators are the same as above.

### ***Covert ARS within Another Business***

The extent of criminal activity is limited by the level of cash deposits that can be made without arousing suspicion. Suspicious transaction reports from banks and referrals from financial intelligence units are key ways of identifying this activity. This sector tends to be tied to specific ethnic or immigrant groups and may therefore in some cases be a higher risk for terrorist financing.

### ***Covert ARS – No Premises***

This sector is limited by its ability to handle cash, but is high risk for criminal ML. It is particularly high risk in jurisdictions where ML activity through ARS has been detected and disrupted.

In this study, the highest volumes of criminal cash were handled by shop-front ARS that provided their services to a specific ethnic community. These operations have tended to be located in an urban area with a high concentration of the ethnic or immigrant population. Collectors in such money laundering operations have generally come from the same communities. These “collectors” have interacted with and provided ML services to a full range of criminals. The size of individual transactions has been between GBP 100,000 and GBP 500,000.

While the key evidence for these activities has come primarily from one or two jurisdictions, the activities and typologies described are common and recognised in a wider range of jurisdictions. Disruption of established overt ARS laundering criminal money has increased the role of “controllers” and “collectors”. Their activities increasingly have all the hallmarks of covert ARS set up to launder criminal money.

## **DETECTION**

The issue of detection of illegal activities conducted by or through ARS is crucial. Different relevant aspects are involved which need to be considered and dealt with separately.

ARS operating covertly are a source of risk since their lack of transparency makes them particularly suitable for ML/FT purposes. Probably the most effective methods for detecting covert ARS operations is to focus on settlement activities, as such activity may involve the conventional banking system or other ARS providers operating openly.

This requires vigilant know your customer procedures by these institutions, in particular where customers regularly transfer substantial amounts of money abroad. It is also important that banks and money remitters apply appropriate procedures in order to understand the business of their counterparts or corresponding money remitters in third countries. In addition it requires active suspicious transaction reporting, based on an understanding of the kind of operations that criminal money remitters are engaged in. The following factors could be useful as indicators of covert ARS operations and or some sort of ML/TF activity.

### **General ML/TF Indicators for Banks and Regulators**

- Regular high levels of cash deposits.
- Cash deposited at banks located at a distance from the suspected ARS business premises.
- Regular high-volume international transfers to third party accounts in countries which are not destination countries at the end of known or usual remittance corridors.
- Regular return of cheques for insufficient funds.



- Cash volumes and international remittances in excess of average income of migrant accountholders and/or in excess demand for migrant remittances in the areas (taking account of other operators)
- No business explanation for the size of business or cash volumes; and international remittances that are incongruent with the normal resources of legal entities (for example, foundations) in migrant community; wholesale *hawala* used to explain source of cash.
- Structuring of deposits to avoid reporting thresholds or simply in an attempt not to draw attention.
- Large volume transactions recorded informally, using unconventional book keeping methods or in “off-the-record” books.
- Large transfers from account to potential cash pooling accounts.

Particularly relevant for regulators are:

- Book keeping records do not match banking operations.
- Transfers to jurisdictions where the suspected ARS operator has no apparent relationship.

### **Specific Indicators for Banks in Connection with Cuckoo Smurfing**

“Cuckoo smurfing” – In this type of activity, the bank accounts used will be held by legitimate customers. Banks, however, are well placed to identify the cash deposits by third parties into these accounts. The existence of these deposits are not necessarily grounds to reconsider the relationship with the customer; however, they could be the indicator of this type of laundering activity and thus should be subject to a suspicious transaction report. The banks should consider that law enforcement will need to identify the depositor and seek identification or preserve CCTV footage to support the suspicious transaction reports.

Cash deposits – The disruption of cuckoo smurfing leads to a surplus of cash held by collectors. Cases have shown the collectors resorting to the delivery of cash to third parties expecting a genuine remittance from overseas. Unusually large cash deposits by a customer with personal or business links to an area associated with drug trafficking may indicate that the customer has received cash from a collector in lieu of a payment by transfer or cheque thus involving the customer unwittingly in a money laundering operation.

### *The Role of the Financial Intelligence Unit*

FIUs play a key role in detecting illegal activities conducted through or by ARS. In regulated systems, they receive suspicious transaction reports from banks and legal ARS that may indicate ML or TF transactions carried out by criminal ARS (especially in the settlement stage) and by individual customers exploiting remittance services. FIUs can also identify relevant cases through their own analysis, accessing available data bases and co-operating with other domestic authorities and foreign counterparts. Given the international nature of ARS activities, both as far as customers’ individual remittances and the settlement stage are concerned, international co-operation between FIUs proves fundamental.

However, remittance transactions related to ML or TF are more frequently than not carried out by occasional customers that do not enter into any durable relationship with the ARS provider. This lack of a continuing business relationship thus makes know your-customer and evaluation procedures more

difficult to carry out. Moreover, one-off transactions can be disguised using a number of different deception techniques, and often no anomalies can be detected in the first instance.

Money flows in the settlement stage may also be particularly difficult to identify and to assess, both in terms of possible links to covert ARS activities and of the illegal origin or intended destination of the funds. As the cases and the indicators show, there are a number of different aspects to be considered, and all relevant information is not always available. In these circumstances, the detection and analysis of suspicious transactions can prove particularly difficult.

### *The Role of the Supervisor*

In order to detect illegal activities in the ARS sector, the critical task for any oversight authority – regardless of the regime – is to have the means (1) to detect undeclared ARS operations that may or may not be involved in ML or TF and (2) to be able to determine when “declared” (that is, licensed or registered) ARS operators are involved in some sort of illegal activity. The role of the supervisor can vary from jurisdiction to jurisdiction. Regimes that require close oversight to ensure compliance with AML/CFT rules may have more direct access to the internal workings of ARS operations through regular compliance inspections. In a regime requiring the licensing of ARS operators, the supervisor is often also required to monitor actively the market for unlicensed ARS activity. This is also important in view of the risk that ARS operators may avoid the licensing requirements by operating underground. In instances where the supervisor also oversees conventional banking, there may be additional value in the direct access and sharing of information obtained from banks in helping to detect undeclared ARS operators. In oversight regimes that require registration of ARS operations, the supervisor may play less of a role in the detection of undeclared operations (with a relatively large role then for law enforcement), although again this can vary from one jurisdiction to another. Some of the more successful detection methods observed as part of this study include the following:

- Reaching out to and/or more intensive contact with the public (public information and complaints desk; awareness programmes).
- Co-operation and exchange of information with other supervisory or enforcement agencies (including tax authorities).
- Obtaining information through legal entities (“declared” ARS operators).
- Screening registers at Chamber of Commerce (also other databases as yellow pages).
- Regular review of various types of public media (newspapers, radio and internet through computerised searching engines).

### **Active Detection by Law Enforcement and Customs Authorities.**

Effective investigation by law enforcement or supervisors to detect illegal activity of money remitters are of course also a very important tool. Different aspects are involved:

#### *Investigations by law enforcement and supervisors to detect illegal money remitters.*

Suspicious transaction reports from banks are the first source of intelligence to identify undeclared ARS activity. The use by financial institutions of the indicators already set out above could help to initial assessments of such institutions when confronting activity that could be subject to suspicious transaction reports.

Another key source of intelligence is to be found at the other end of the transaction. Each ARS transaction begins and ends at an ARS. The study has shown how a remittance may move from the regulated to the unregulated sector. Examining the nature of remittance corridors related to the

originator jurisdiction and establishing a dialogue with the regulators at the other end of the corridor and at hub points could also be an effective way of identifying undeclared ARS within the corridor.

#### *Investigations by law enforcement to detect ML/TF.*

Investigations of predicate offences remain an effective source of information that could lead to ARS operations. Each investigation into serious crime will discover details of the ML personalities and/or methods. This is a source of information that can be exploited for ML prosecutions; however, it can also serve as valuable intelligence for FIUs and regulators in detecting potential illegal ARS operations.

The challenge for law enforcement is to identify, prosecute and disrupt ML/TF activity operating through ARS when there is no proven link to a crime. Good quality suspicious transaction reports on complicit ARS, customers of ARS or cuckoo smurfing are all nevertheless useful in generating an effective investigation. Criminal cases can also be further enhanced by developing evidence on the volumes of money and methods used by a legitimate ARS.

Where collectors are identified, it is important to determine the person controlling them. This person normally operates in a separate country. Ultimately reaching and immobilising this controller has more impact than just prosecuting the collector. Disruption of the operation can only be achieved by the fast and effective sharing of intelligence and evidence. Mutual legal assistance in these cases is thus vital.

Law enforcement should be aware of the criminal cash couriers and money flows associated with crime in their country. When these are known, it makes identifying ML activity easier. Part of this process should involve identifying the overseas ML hubs exploited by criminals in their country and then working with law enforcement and regulators in the hub countries.

Criminal misuse of ARS operations can often be detected through focus on the settlement stage of such operations. When ARS operators make regular use of cash couriers – who then avoid declaration at the border (or make false declarations) – there is the strong possibility that the operator fears detection that might occur if settlement takes place through conventional wire transfers through the conventional banking system. Customs and law enforcement should therefore be well aware of the possibility that cash couriers are linked to illegal money remitters in their country or in other countries. The sharing of intelligence on cash courier profiles and techniques, combined with intelligence from the jurisdiction where the banknotes are eventually sold is an effective method of modelling and attacking this activity. A declaratory regime can provide useful data to support this activity. Declaration and disclosure systems at the border, in accordance with Special Recommendation IX, are also important to deter such illegal activities and to be able to hold or seize the money and effectively investigate cases of false or no declaration/disclosure.

Each detection of a cash courier gives law enforcement the opportunity to identify the collector who has passed them the cash, the controller who has recruited and directed them and the ARS or bank where the cash will be taken. Each of these factors should be examined in every case. Where the debriefing indicates a ML/TF operation based or impacting in another jurisdiction the sharing of intelligence and evidence is crucial.

#### **General ML/TF Indicators for Law Enforcement**

Indicators of potential ML/TF activities carried out through ARS include the following:

- Volume of cash handled cannot be explained by legitimate business practices;
- Migrant remittances claimed to be handled exceeds volumes expected produced by local community (based on income levels, economic activities, etc.);

- Collectors avoid suspicious transaction reporting by using multiple complicit ARS operators;
- Collection of cash from identified criminals;
- Heavy contamination of bank notes with heroin, cocaine or other illegal drugs;
- Depositing large volumes of cash with ARS operators;
- Use of safe houses with cash counting machines;
- Cash transported by cash couriers; and
- Members of family used as cash couriers.

### **How ARS Operators Can Detect Criminal Misuse**

ARS service providers should be sufficiently vigilant to be able to detect potential exploitation by individual criminal customers. This largely corresponds with what was already said above to the extent that they are dealing with criminal settlement procedures. Nevertheless there are also indicators that are more likely to signal this kind of misuse for individual ML or TF transactions, in particular customers that clearly engage in smurfing operations. Again appropriate know your customer and suspicious transaction reporting procedures are the key.

### **Indicators for ARS Operators**

- Remittances in excess of norm for the customer's economic background, based on income levels, economic activities, etc. or without logical business reasons;
- Escalating levels of remittance for an individual customer above what was to be expected from original know-your-customer assessments;
- Personal remittances sent to destinations that do not have an apparent family or business link;
- Remittances made outside migrant remittance corridors.
- Reluctance of customer to give an explanation for remittance;
- Personal funds sent at a time not associated with salary payments;
- Requests for a large transfer but settling for smaller amounts – potential structuring;

## **FINDINGS**

The various types of ARS examined in this study have differing levels of vulnerability to ML and TF. Despite this vulnerability, ARS do provide a legitimate and often necessary service to a wide customer base. The largest identified risk is probably the danger posed by underground operators that are set up expressly to support criminal purposes. Other underground or undeclared ARS provide remittance services for non-criminal customers, and they therefore run a large risk of being misused in the absence of appropriate CDD and record keeping measures. However, this study also shows several examples of registered and AML/CFT-regulated entities that deliberately engage in criminal activity. Indeed criminal money remitters sometimes change from covert to overt and registered services to acquire an air of legitimacy and a front for using banking services for large-scale transfers to third countries. There are examples of legitimate money remitters that are unwittingly misused by criminals for ML/TF. Furthermore, the high volume of transactions in the franchised part of the money

remittance sector in itself makes it likely that this channel is also sometimes misused for this kind of activity.

ARS providers that do not operate openly can be divided between those who operate “underground” because they are criminal money launderers, and those who are not part of the regulated sector, either deliberately or unwittingly. The first of these categories is the highest risk, for obvious reasons. They are prolific and committed money launderers who cause serious harm through their direct support of criminal activity. The second category of covert ARS providers frequently only handles “legitimate” money from the shadow economy. They may also handle criminal and terrorist money. The risks for this second category are significant because of the inherent lack of transparency to both regulatory and law enforcement authorities.

While ARS operators may perform a large part of their remittance transfers outside conventional banking channels, settlement or clearing of accounts between various ARS operators may take place through such conventional channels. For this reason, ARS activity is susceptible to detection by financial institutions or declared ARS operators during the settlement phase. Although it is not always possible to distinguish whether such activity is by itself related to ML or TF, detection of ARS operations – particularly when carried out by undeclared ARS operators – may provide important investigative leads.

Given the international nature of ARS, detection of undeclared activity and/or potential ML/TF in one jurisdiction apparently only presents part of the picture.

Because of the short and often superficial business relationship that exists between most ARS operators and their customers, it is more difficult for such operators to recognise suspicious transactions or behaviour.

An important indicator of possible ARS settlement procedures performed by undeclared or criminal operators is the regular use of cash couriers, which avoid declaration at the border (or make false declarations).

A number of cases examined as part of this study involved the use of commercial operations – especially under- and over-invoicing as part of import or export transactions – to serve as a vehicle for settling accounts between various ARS operators. The technique of *cuckoo smurfing* is also associated with this activity and apparently is particularly prevalent in relation to ML operations co-ordinated from South Asia and the Middle East. The volumes of cash laundered are significant, and the criminal cash provides the support for further criminal activity. The lack of consistent identification or know-your-customer policies with regard to depositors of cash into third part bank accounts appears to be an important weakness exploited in this ML technique.

Several other features that were highlighted in the typologies complicate the investigations into possible involvement of ARS operators in ML or TF. One such feature is the regular and organised use of cash pooling accounts in the settlement procedures between money remitters. Commingling of funds coming from different commercial activities into the flows of remittances is also a source of risk, both because it provides opportunities for criminals to disguise their money and because the proper application of AML/CFT measures is made more difficult in those circumstances. An additional risk may come from dubious bookkeeping practices. As some cases show, ARS may not maintain “official” records of the money received or paid out to each individual customer but only the aggregated transfers executed for a number of customers through the bank accounts.

## **ISSUES FOR CONSIDERATION**

At the outset, it should be noted that work remains to be done to develop a harmonised terminology related to ARS. The research conducted by this project team may be able to contribute toward an improved understanding of concepts involved; however, over the longer term the efforts to examine

ARS and identify potential weaknesses would only benefit if all players eventually worked with common definitions.

A relatively effective way to detect undeclared ARS-operators is the detection of the settlement transactions of these entities. Although it is not always possible to distinguish between the detection of money remitters carrying out ML or TF and money remitters that are simply providing underground services, the detection of such activity can provide a useful lead in ML or TF investigations. Since settlement transactions are often carried out through banking channels, vigilance by banks in applying know-your-customer and suspicious transaction reporting procedures can be very helpful in this respect. Banks and money remitters should be provided with appropriate guidance for CDD and suspicious transaction reporting, in particular when dealing with (other) money remitters as customers. Several indicators have been provided in the report.

Because ARS settlement is international, this does mean that the regulator, FIU or investigator who identifies the activity will need to communicate their suspicions to their equivalent bodies in the originating and receiving countries. This emphasises how important the sharing of intelligence and evidence between countries is to the effective disruption of criminal ML or TF groups using ARS.

It is also worthwhile to highlight the positive experience of some countries with currency transaction reports. Such reports can be particularly helpful for detecting criminal activity in the money remittance sector. Since money remitters normally have very short and superficial business relationships with their customers, it is more difficult for them to recognise suspicious or unusual transactions or behaviour. Reporting all large transactions and allowing the FIU to (electronically) analyse these transactions, for example by comparing them to other data bases, could have a large added value in this context. In the Netherlands for example about 20% of all ARS-transactions above euro 2000 are found suspicious after such an analysis.

Other countries have also had success with a risk-based approach, which focuses efforts on studying the ML techniques associated with ARS to help orient future investigative activity. There is an argument that a declaratory regime collects most of its data from the legitimate sector and diverts resource from intelligence work on criminal ML.

Possible ARS settlement activity can be indicated by the regular use of cash couriers who attempt to avoid declaring cross-border carriage of funds. The sharing of intelligence on cash courier profiles and techniques, combined with intelligence from the jurisdiction where the banknotes are eventually sold is thus a potentially effective method of targeting and attacking this activity. Information provided by competent authorities according to Special Recommendation IX could provide useful data to support this activity. In addition, under a declaration system general information on declared cross-border cash transport above the designated threshold could also be useful for the detection of settlement activities.

Some cases show that money remitters engaged in ML or other illegal operations make use of commercial operations – in particular under- and over invoicing - to hide their settlement transactions. Further study is required to develop detection methods for this phenomenon. The same applies to the phenomenon of cuckoo smurfing. This technique was reported by one country, but the activity was recognised by contributors from other jurisdictions. The activity is particular associated with ML co-ordinated by ARS in South Asia and the near and Middle East. Cuckoo smurfing can be effectively disrupted by the consistent use of identification and know-your-customer procedures for the depositors of cash into third party bank accounts. This would provide suspicious transaction reporting for investigators and further work for the criminals. We recommend that banks include details of this technique in their AML training and devise methods of identifying and reporting the activity, coupled with a policy of refusing the depositing of cash from unknown third parties.

The use of cash pooling accounts by ARS operators, as well as incomplete or inaccessible book keeping techniques, would seem to require appropriate regulation and supervision. Individual cash

pooling accounts have been identified handling USD 100 billion or more in a year. This represents the concentration of criminal money from a large number of countries. Identification and closing of these accounts improves the reputation of the whole sector, and is one of the most effective international steps to combating serious organised ML.

Another measure that could be useful in dealing with cuckoo smurfing or other ML techniques that rely on use of the accounts of unwitting third parties would be to stress obligations to identify depositors that do not have an apparent tie to the account holder. It may also prove useful to establish or reinforce identification obligations on the part of beneficiaries of ARS transactions.

The study of cases showed some very effective law enforcement action against money launderers that have exploited the lack of transparency in the ARS sector. There have been cases involving international action, but effective end-to-end disruption of such operations has been frustrated by barriers to intelligence sharing, differences in the legal status of ML offences, predicate offences and unwieldy systems for mutual legal assistance. FIUs have proved to be effective in Scandinavian countries, for example, where there is the real-time exchange of information backed up with inter-jurisdictional legal support. The international community will need to find ways of sharing intelligence on current cases and then allowing joint intelligence-led investigations along the criminal ARS corridors. Successful prosecution or disruption of ARS ML controllers benefits many jurisdictions. The controllers of money laundering operations that exploit the vulnerabilities of ARS will necessarily base their operations in country where they feel safe from detection. It is a challenge for the international law enforcement community to ensure that the controller of a ML scheme is not safe regardless of the jurisdiction from which he operates. Disruption is a valid tool in these cases and relies on close co-operation between investigators, regulators and criminal intelligence practitioners.

This study does not allow the drawing of straightforward conclusions about the most expedient regulatory system, in particular about the choice of a registration or licensing regime. In any case it should be noted that the common basic element of any regime remains the need to identify ARS operators. Although it is difficult to determine which factors drive money remitters underground, overly strict regulation and monitoring and associated costs could indeed play a role. However, given the evident involvement of registered money remitters in ML and TF schemes, it is equally clear that adequate regulation and supervision, including background checks on managers and owners of ARS-services, as well as legal measures to remove unsuitable managers after a negative background check are equally essential.

Similarly, the study did not allow for the examination of the issue of thresholds that countries apply for identification. While the lack of a threshold could be one of the factors that drives customers and therefore also operators underground (the study was not able to draw any definitive conclusions on this issue), the study is clear about the importance of structuring and therefore about the risk of (high) thresholds for identification. Suspicion-based identification below the given threshold is a recommended tool to combat smurfing. Automated analysis of ARS accounts, both by the ARS themselves and by banks, is also a useful tool for identifying and reporting this activity.

The study recognised that identifying the ML/TF risks in each jurisdiction is important for developing an effective regulatory regime, whether registration or licensing. These risks will be influenced by the country's chosen form of regulation, as well as the criminal ARS corridors, the role of cash in the economy and the availability of cheap/formal alternatives to ARS. A comprehensive national risk assessment for ARS shared through international bodies is a very useful tool in helping the sector raise its levels of compliance and reputation.

The risk is very real that money launderers and terrorist financiers will use "regulatory arbitrage" in exploiting ARS, that is, they are likely to channel their money through markets with limited supervision/monitoring of ARS or where it is easy to operate underground. Since money remittance (and settlement) can flow to different entities in different countries, it is relatively easy to take

advantage of such weakness even if money is eventually remitted between two well-regulated markets. This underlines the need for a global implementation of AML/CFT standards in this sector.

Given the flexibility of the methods of money launderers and terrorist financiers and the evolution of new methods it is important that the competent authorities as well as the banks and money remitters maintain an up to date knowledge of such methods and techniques. An important tool to this end is the matrix of typologies and their main characteristics that is referred to in the introduction. This tool should be further developed and exploited for future use.

Another conclusion to this report should be that the ARS community includes providers at all levels who in the majority strive to provide good service and meet their AML/CFT responsibilities. These providers are frustrated by the reputation of the sector and the perceived risks to supplying banking facilities to ARS operators. If the honest and compliant ARS cannot provide these services in the future, the business will be driven down as well as up. A healthy, well-regulated and competitive ARS sector supports the effective combating of international ML and TF. There remains a need, however, to maintain a balance that includes and recognises the needs of migrant communities but prevents abuse of ARS. No regulatory system can ever be considered perfect, and there cannot be a “one-size-fits-all” solution. There is furthermore a need to maximise controls where the risks are highest while minimising the administrative burden on the industry and consumers. Covert ARS tend to serve specific communities. Therefore, creating a strong AML regulatory regime within which ethnic ARS can be included but still retain their traditional values is the best defence.

Whilst this report has focussed on transmission of funds by alternative means to conventional banks, there is a need to recognise that, at some stage in the process, nearly all remitted funds will use conventional banking facilities and have an essential role to play. Getting the balance right in each jurisdiction is hard, because local factors vary enormously. International co-operation on intelligence, investigation and regulation are the most important tools in generating a respected global ARS sector.



## ALTERNATIVE REMITTANCE SYSTEMS

	Regulatory system (number of registered / licensed ARS)	Competent authority	Fit and proper	Experience	Criminal records	Business plan / AML/CFT programme	Off-site information	On-site visits
<b>Austria<sup>1</sup></b>	Banking license [See response following this table.]	Financial Market Authority (=integrated financial supervisor	Performed	3 years managerial experience required	Checked	Detailed business plan required	Reporting obligations	On occasion
<b>Canada</b>	Currently, no registration/licensing obligation	FIU				AML/CFT procedures and internal controls required	No reporting	Risk-based
<b>France<sup>1</sup></b>	Banking license	Banking Supervisor		Checked	Checked	Detailed business plan required	Reporting obligations	On occasion
<b>Hong Kong, China</b>	Registration (1,373 as in March 2005)	FIU	No	Nil	Checked	Nil	Upon registration in the name of company, business registration documentation must be produced.	Yes
<b>Germany<sup>1</sup></b>	Licensing (43)	Financial supervisor	Performed	3 years managerial experience required	Checked	Detailed business plan required	Quarterly	On occasion, reliance on audit reports
<b>Italy<sup>1</sup></b>	Licensing (25) Applicable also for agents	FIU and Financial Police	Not performed	3 or 5 years experience required	Checked	Internal procedures and controls required	Reporting obligations	On occasion, based on information
<b>Netherlands<sup>1</sup></b>	Licensing (30)	Central Bank	Performed	Not required	Checked	Required for integrity issues	Monthly	Two to four times per year
<b>Spain<sup>1</sup></b>	1) Hawaladars: Prohibition 2) Legal Money transfers, licensing: 46 (Agents are not included)	Central Bank and FIU		Not required	Not Checked	Internal procedures and controls required	Reporting obligations	On occasion reliance on audit reports
<b>Sweden<sup>1</sup></b>	Licensing (40) <sup>4</sup> . Agents of WU and Moneygram are registered by the main operator, who is licensed.	FSA	Performed	Checked	Checked	Required by those ARS actors who are obliged to the AML regulations	On demand	Not allowed by the regulations.
<b>Switzerland</b>	Licensing - if turnover over CHF 2 million or gross income + CHF 20,000 (200)	SRO or ML supervisor	Performed	Required	Checked	Required, internal procedures	No reporting	On occasion, reliance on audit reports
<b>Thailand</b>	Licensing (3) –	Central Bank and Finance Ministry	Performed	Not required	Checked	Required, internal procedures and controls	Reporting obligations	Not yet implemented
<b>United Arab Emirates</b>	1) Hawaladars: voluntary registration (123) 2) Exchange houses: licensing (108)	Central Bank	1) Not performed; 2) Performed	1) Has to be existing hawaladar 2) Required	1) Checked, no consequences 2) Checked	1) Not required 2) Required	1) Quarterly, all transactions 2) Monthly balance statements	1) Friendly visits 2) Once per year
<b>United Kingdom<sup>1</sup></b>	Registration (1500)	HM Revenue & Customs	Not applicable	Not required	Checked & used in risk based regulation	Program set out in AML law	Annual turnover, SARS & visiting regime reports	Risk-based
<b>United States (federal)<sup>2</sup></b>	Registration (22,000)	FIU & Tax authority	Not performed	Not required	Not checked	AML program required	No reporting	Risk-based

## REGULATORY FRAMEWORK OF SELECTED COUNTRIES

Identification/CDD (specify threshold)	Record keeping (specify threshold)	Suspicious transactions report	Currency transactions report	Use of formal banking channels	Sanctions	Perceived extent of the underground sector (where applicable)	Fees on entry / Annual fees
Transactions over 15,000 EUR and all transactions if suspected ML/TF	5 years	Required	Not required	Not required	Warnings, order, withdraw licence, fines		None
Transactions over CAN 3,000	5 years	Required	International wire transfers and cash transactions above CAN 10,000	Not required	Criminal sanctions		
Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Required record details of identity for transactions over HKD 20,000 (USD 2,500)	6 years	Required	Nil	Must register the details of the bank accounts utilised.	Warnings and prosecution	Noticeable immigration/ethnic related underground sector	No charge No annual renewal requirement
Transactions over EUR 2,500	6 years	Required	Not required	Not required	Warnings, order, withdraw licence, fines		EUR 1,000/ Percentage over annual turnover (min EUR 650)
Transactions over EUR 12,500	10 years	Required	Not required	Not required	Criminal and administrative	Significant immigration/ethnic related underground sector	None
All transactions	5 years	Required	2000 EUR	Not required	Warnings, order, withdraw licence, fines, prosecution		Percentage over annual turnover with a minimum of EUR 3,000
All transactions	6 years	Required	Transactions over EUR 3,005.07 (voluntary nature)	Not required	Administrative sanctions	Significant immigration/ethnic related underground sector	
Transactions over 15,000 EUR and all transactions if suspected ML/TF.	5 years	Required by those who are obliged to the AML regulations.	Not required	Not required	Warnings, order, withdrawal of licence	As a result of the explanation in footnote 1 there is not a known demand of any underground sector.	1000 EUR
All transactions	10 years	Required	Not required	(not required)	Warnings, order, withdraw licence		None/None (SRO membership)
All transactions	5 years, under AMLA	Required	Not required		Fine, revoke licence		None
1) All transactions 2) Transactions over AED 2,000	1) Not required 2) All trans. over AED 2,000	Required	Not required	Not required	1) None 2) Revoke, restrict licence	None	
On suspicion or transactions over EUR 15,000	5 years	Required	Not required	Not required	Criminal sanction (max 14 years) Civil fines up to GBP 5,000		GBP 60 per premise
Transactions over USD 3,000	5 years	Required when trans. is over USD 2,000	Transactions over USD 10,000	Primary transaction account must be disclosed	Civil and criminal fines		None

## REGULATORY FRAMEWORK OF SELECTED COUNTRIES

### NOTES

**[AUSTRIA]** Regulatory system (number of registered / licensed AR) Licensing of money transfer institutions (1) and bureaux de change (7). Kindly note that credit institutions in Austria may offer all banking services, including the business of money transfer business and bureaux de change business, under their universal banking licence. It is only when these services are provided as a stand-alone business, under a licence for just this activity outside a credit institution that you find them listed separately.

**[1]** All EU members are moving towards a common position regarding oversight of ARS.

**[2]** This number reflects the approximate number of federally registered money services businesses in the United States, which includes ARS providers.

**[3]** Those Swedish ARS actors that operates through the Swedish regular banks are not required to registration and therefore they are not obliged to the AML regulation, as the AML regulations are to be fulfilled by the banks in question.

## CHAPTER II

### MONEY LAUNDERING VULNERABILITIES IN THE INSURANCE SECTOR

The global insurance industry provides risk transfer, savings and investment products to a variety of consumers worldwide, from individuals to multi-national corporations and governments. The insurance sector, like other financial services, is exposed to the threat of money laundering (ML)<sup>11</sup>. The insurance sector could be attractive to money launderers seeking to place funds into a financial product that will provide them with a reliable, clean return of funds invested. If a money launderer is able to move funds into an insurance product and receive a payment made by an insurance company then he will have made his funds appear legitimate.

Previous FATF typologies research has observed that the inherent characteristics of the insurance sector may give rise to ML risks unique to the insurance industry, increasing its vulnerability to ML. Inconsistent regulation and supervision across the industry was noted as providing opportunities that could also be exploited by money launderers. FATF typologies research indicated that there was a low detection of ML within the insurance industry in comparison to the size of the industry and in comparison to other parts of the financial services industry.

#### Issue and aims of the project team

The FATF-XV Typologies Exercise examination of the insurance sector concluded that it remained unclear to what extent the insurance sector is exposed to ML. Accordingly, the FATF February 2004 Plenary decided to examine further the ML vulnerabilities in the insurance sector as part of the FATF-XVI Typologies Exercise. To facilitate this work a project team of experts from a number of different backgrounds (FIUs, central banks and insurance supervisors) was formed from jurisdictions with significant insurance industries, together with representatives from the International Association of Insurance Supervisors (IAIS). This project team was tasked with performing a study on ML vulnerabilities in the insurance sector. To this end, the mandate of the project team was defined so as to take a broad approach to examination of the factors that may make the insurance sector vulnerable to ML. The objectives of the work to be undertaken were:

- to examine the money laundering vulnerabilities in the insurance sector taking into account the differences among the various parts of the sector and among insurance products;
- to develop industry specific money laundering indicators that may assist both the financial services sector and national competent authorities in detecting money laundering through insurance;
- to highlight possible policy implications, if any, in the context of anti-money laundering measures for the insurance sector.

The team's findings were to contribute to the FATF-XVI annual typologies exercise and to produce a report to be published by the FATF.

#### Brief history of the work undertaken

A project leader with relevant experience in examining ML and Insurance was appointed, who drew up a project plan which was agreed by the Working Group on Typologies (WGTYP). The project team formulated a two stage data collection plan to gather the information required to answer the questions posed in the project plan. In stage 1, a comprehensive questionnaire<sup>12</sup> designed to gather the

---

<sup>11</sup> For the FATF scope of ML please see FATF 40 Recommendations 2003 at [www.fatf-gafi.org](http://www.fatf-gafi.org).

<sup>12</sup> Responses to WGTYP/06 – see Annex A

bulk of the required information was produced by the project team and circulated to all FATF and IAIS members. This questionnaire sought to gather information on 3 areas:-

- Details of the size and structure of the insurance market and the extent of Anti Money Laundering (AML) regulations and supervisory regime for each jurisdiction.
- Details of suspicious transaction reports (STRs) made in respect of insurance in the period 1999 to 2003 for each jurisdiction.
- Details of actual money laundering cases.

The team received replies from 46 jurisdictions and in some cases sought further clarification. In addition information was received from 6 major insurance companies (see Annex A). In stage 2 a subsequent request for information<sup>13</sup> was circulated to FATF and MONEYVAL members, aimed primarily at understanding jurisdictions' perceptions of the vulnerability of their own insurance industry and at broadening the request to include those cases where insurance has been misused in more general economic crimes. The second request was intended to identify further cases where ML was not initially recognised as the primary issue. 25 jurisdictions provided a response to this questionnaire (see annex A).

The project team received replies from jurisdictions making up a sizeable part of the worldwide insurance business: eventually 58 jurisdictions provided information. Although the quantity and quality of the information provided was, as anticipated, variable we believe the analysis that follows fully reflects the current understanding of ML vulnerabilities of the insurance industry.

## **ANALYSIS AND COMMENTARY ON QUESTIONNAIRE RESPONSES**

The responses of both national jurisdictions and representatives from the insurance industry provided a valuable pool of information, the systematic analysis of which allowed a number of significant conclusions to be reached on the way the sector operates and how AML regulation within it is enforced.

### **Details of the size, structure and operation of the insurance market**

Worldwide the insurance sector generates premiums of some USD 2.941 trillion per annum<sup>14</sup> and in many jurisdictions it is a significant part of the financial services industry generating substantial flows of money.

The insurance market is a dynamic sector offering increasingly sophisticated products to its customers and providing competition to other parts of the financial services industry. The insurance sector's growth is particularly noticeable with some jurisdictions reporting a doubling of premiums in the last decade.

The picture of the insurance market emerging from the questionnaires is that of a competitive highly globally-integrated market, but with local circumstances influencing the exact nature of services and products on offer. In over half (27 out of 48) of the jurisdictions who responded on this point, the level of concentration reported was not significant. Insurers operating globally feature a significant participation, direct or indirect as it may be, in many national markets. The degree of integration with the other parts of the financial services industry appears considerable, since sizeable shares of national markets are controlled by insurers belonging to financial conglomerates, which may be headed either by insurers or by other financial institutions, most notably banks.

---

<sup>13</sup>Responses to WGTYP/16 – see Annex A

<sup>14</sup>Information obtained from [www.swissre.com](http://www.swissre.com).

An important feature of the way the insurance sector operates is that most of the business is channelled through intermediaries, either tied agents or independent brokers. With reference to the life sector (as for non-life the role of intermediaries is even more significant), 10 jurisdictions stated in their response that intermediaries, are the major, or even sole, channel of distribution for insurance products. In a further 9 jurisdictions, intermediaries account for over 80% of the total turnover of the insurance market, and in another 4 jurisdictions the intermediaries share is equal to or greater than 50%. Only 5 jurisdictions reported that life insurance products are mainly sold directly by the insurers.

An ever increasing share of the market is sold by intermediaries belonging to other parts of the financial services industry, usually banks. Branch offices of banks are widely used for selling insurance products, in particular those with enhanced investment characteristics.

Currently, in most jurisdictions only a small share of the business is sold through other channels, such as phone marketing and the internet. Any significant increase business through these distribution channels may have an affect on the way ML risks are perceived.

As will be highlighted in the next sections, the way in which insurance products are sold has relevant implications as far as AML regulation is concerned.

### **The extent and limits of AML regulation**

From the responses jurisdictions provided, no noticeable differences have emerged in the extent to which AML regulation applies to the life insurance sector when compared with other parts of financial services industry. With some exceptions<sup>15</sup>, all jurisdictions subject insurers to the whole set of AML obligations, including customer identification and verification, record keeping and suspicious transaction reporting. Notably, ten<sup>16</sup> jurisdictions responded that there were some exemptions on AML regulations on the life insurance industry. Frequently AML regulation does not apply to the same extent to the non-life sector and is very often absent in the reinsurance sector. This reflects the current position of FATF Recommendations which do not specifically include general insurance or reinsurance.

Due to the way the insurance market operates, compliance with AML regulation is required (with exceptions in four jurisdictions<sup>17</sup>) of both insurers and the intermediaries who distribute insurance products on their behalf. However, AML regulation may sometimes be applied at an unsatisfactory level, as will be described in more detail (in paragraph 59). Here, suffice to say that, as for identification and verification obligations, intermediaries sometimes consider, incorrectly they do not bear the responsibility for AML compliance. They believe this responsibility only remains with the insurers, to whom the business relations with the customers have to be ultimately referred.

This misconception may be reinforced by the fact that, rather than filing STRs directly to the FIUs, intermediaries are usually required to report unusual behaviours to the insurer on behalf of whom they operate. AML regulation is usually applied to a limited extent in the general insurance sector. General insurance is generally viewed as prone to fraudulent schemes to the detriment of insurers, as in the case of false claims, rather than be the conduit of money laundering operations. As a result, where AML provisions do apply carve-outs and exceptions are permitted usually to reflect the perceived lower ML risk in the general insurance market.

As in other parts of the financial services industry, prudential supervision is applied to insurers, involving some kind of initial authorisation process and ongoing prudential standards checks.

---

<sup>15</sup> Two jurisdictions (Uganda and Sri Lanka) responded in the questionnaire that they had no AML coverage for life insurance

<sup>16</sup> Finland, France, Luxembourg, Mexico, Norway, Singapore, United States, Bermuda, Gibraltar, Mauritius

<sup>17</sup> Bermuda, Macao, UAE and United States

Generally insurers are registered at a centralised supervisory authority, whilst the businesses owners and management are usually required to undergo integrity checks. In the life insurance market prudential supervision is extended to intermediaries, although often in milder forms. Against this general picture, however, regulation and supervision have emerged as being applied unevenly across the insurance industry which may provide opportunities that can be easily exploited by criminals. For instance, the findings concerning the reinsurance sector seem to be quite significant. In devising the questionnaires, special attention was devoted to this sector, since little analysis had previously been undertaken of the reinsurance sector from an AML perspective (see paragraph 79). As will become clear, especially from the analysis of the cases provided by jurisdictions, reinsurance businesses have suffered from criminal infiltration, facilitated by seemingly ineffective supervision and integrity checks, where these exist at all.

### **Analysis of STRs made in respect of insurance in the period 1999 to 2003.**

The FATF-XV Typologies Exercise identified low levels of STR reporting by the insurance sector. It was argued that a low suspicious transaction reporting rate within a certain sector signals that the ML risk associated to that sector is broadly perceived to be negligible. Alternatively it was thought that a modest amount of STRs filed by those operating in one sector just reflects a low rate of detection and/or compliance.

As far as reporting entities operating in the insurance sector are concerned, the number of STRs filed, measured as a share of the total amount of STRs submitted by the FIUs of the respondent jurisdictions, appears uniformly low: Of the 37 jurisdictions that responded on this matter the average share of total STRs that were reported by their insurers in the period 1999 to 2003 is as shown below:

<i>% of total STRs received...</i>	<i>...above 20%</i>	<i>...between 20%-3%</i>	<i>...below 3%</i>	<i>None received</i>
<i>Number of jurisdictions</i>	2	6	23	6

Furthermore, of the 26 jurisdictions who responded on the perceived vulnerability of their insurance sector to ML risks, 10 said there was some risk, 10 replied low risk and 6 said it was unknown or they did not specify. Usually the only justification for the responses given was the low level of STRs and money laundering cases.

In the experts' view, the generally low suspicious transaction reporting activity relating to insurers is remarkable in and of itself. However, it may not be entirely surprising given the differing characters of banking and insurance and when also considering that in many jurisdictions AML regulation in the insurance sector is relatively recent. Nevertheless, the small amount of reporting from the insurance sector is noteworthy for two reasons:

- Firstly, the insurance sector's relative size within the financial services industry of each jurisdiction is such that one would expect it to be exposed to the risk of being infiltrated by money launderers and criminals in general to a much wider extent than the number of STRs would indicate.
- Secondly, the identified vulnerabilities (see above) clearly show that the sector is exposed to reasonable degree of ML risk.

## Details of money laundering cases<sup>18</sup>

The collection of a wide range of ML cases involving insurance businesses or insurance products is one of the most significant results achieved by the experts, thanks to the productive cooperation of respondent jurisdictions.

In total 94 specific cases were reported. 66 cases were reported by 14 FATF jurisdictions, whilst non-FATF jurisdictions reported 4 cases. In addition the industry provided a further 24 cases. In several instances jurisdictions, rather than providing specific details on all their cases, described typologies relating to unspecified numbers of cases. Consequently, the overall number of cases, as indicated above, needs to be considered as being merely indicative of the size of the phenomenon being investigated.

The most striking data concerning the cases illustrated by the respondent jurisdictions is the amount of funds involved, which equalled approximately USD 525 million, with one single case accounting for USD 370 million. The 66 cases reported by FATF jurisdictions involved USD 140.6 millions, with an average of USD 2.1 millions for each case which quantifies the seriousness of the threat posed to the industry. It is worth stressing that the overall amount, as indicated above, does not include all the cases in which the transaction was not eventually finalised. Most, but not all, respondent jurisdictions could also provide further details on the cases allowing us to make the following observations.

In those instances in which respondent jurisdictions explicitly indicated the origin of the information, it has emerged that 20 cases were linked to STRs and 15 from other sources, mainly investigations carried out by law enforcement. Moreover, it was reported that 16 cases led to judicial proceedings, whilst 12 are still under investigation. The range of predicate crimes underlying the money laundering cases reported in the questionnaires was relatively narrow, being mainly drug trafficking, financial-type frauds, such as tax frauds, financial and corporate scams, false accounting and embezzlement.

As for the type of products used in the various cases for laundering illicit proceeds, in the majority of cases (about 65%) it was life insurance products that the funds were directed to, with an overall amount of USD 520 million involved. The remainder of the cases were split between general insurance (approximately 30% of the cases, totalling USD 1m) and reinsurance (5% of the cases, amounting to USD4m).

## TYPOLOGIES

Nine typologies were identified from the information provided to us, as follows.

### ***Typology 1: The use of life insurance single premium policies.***

This typology, which has already been identified in previous typologies reports, is still an often found typology in many jurisdictions. The availability of bespoke policies of this nature enables the laundering of large sums by making substantial payments into life insurance single premium policies, which serve as a wrapped investment policy. The customer actually does not seek insurance coverage but an investment opportunity. A variation on this is the use of large premium deposits used to fund annual premiums. Such policies, which are comparable to single premium policies, again enable the customer to invest substantial amounts of money with an insurance company. Since the annual premiums are to be paid from an account which has to be funded with the total amount an apparently lower ML risk life product will bear the features of the higher risk single premium policy.

---

<sup>18</sup>Note: values in USD are approximate based on the exchange rates of end 2004 (USD 1.3 to the euro).



### **Case Example 1**

A fraudulently bankrupt subject used an account in the name of a family member to pay cash in and withdraw it out via a cheque to a lawyer. The lawyer then gave some money back in a cheque to the family member while the rest went to the subject's single premium life policy which was immediately surrendered. The surrender value was paid out to the family member's account.

Source: Belgium

### ***Typology 2: Early policy redemption, especially when uneconomic or unusually early***

This typology, which could be found in cases of several jurisdictions, is a means to receive clean funds at an early stage. It is very often combined with high single premium or deposit account life insurance policies. A conspicuous fact is that some of the respective customers opted for early redemption despite uneconomic consequences. In the case illustrated below the money launderer surrendered his policy despite a loss of 40 percent of the original investment. In some cases the money launderers redeem their policies very soon after purchasing them.

### **Case Example 2**

The subject deposited 1m euros in cash with a life insurance company in 2 single premium life policies which were surrendered early incurring a loss of 40% of the investment cashed outside the jurisdiction concerned in an effort to evade creditors seeking remuneration from the subject's fraudulently declared bankrupt company.

Source: Belgium

### ***Typology 3: General insurance claim fraud in insurance involving high value goods which were purchased with illicit funds.***

The cases which illustrate this typology represent a general structure of criminal behaviour in the insurance sector by transferring illicit funds into clean money paid by an insurance company. It has to be kept in mind however that the prime motivation for the transaction need not be ML (although it could be the case that premiums have been paid using dirty money, as described in the following case). Only these cases require special attention from an AML perspective.

### **Case Example 3**

In Norway in January 2004 a person reported a break-in in his house to his insurance company. The person reported that some of the stolen goods were jewellery worth NOK 110,000. Pursuant to his report he had sold a boat for NOK2.7m and received jewellery worth NOK 500,000 as part of the payment for the sales amount. This person was on a low income and had no assets. In 2000 he had no income or assets at all. In 2001 his income was NOK 43,000 and in 2002 his income increased to NOK 233,000. Either it was not possible for him to have been the real owner of this valuable boat or it was the case that he paid for the boat with illicit funds.

Source: Norway

### ***Typology 4: Cash payments to purchase insurance***

Cash payments still play a certain role in insurance business, predominantly but not only in developing markets. Where large cash amounts are accepted in developed markets it is usually via intermediaries.

### **Case Example 4**

Two subjects who lived outside the jurisdiction concerned deposited large cash sums in 4 single premium life policies. Subsequent premiums came from bank accounts which had been previously investigated for trade in illegal narcotics from Latin America to Western Europe.

Source: Belgium

***Typology 5: Cooling off periods, which allow for refunds of premiums with clean money within the contract cancellation period***

A vulnerability which relates to the easy access to products is to be seen in this specific typology. In some jurisdictions a number of life products provide the customer's right to cancel the contract within a short period of time ("10 days free look" or "cooling-off period"). The customer will then get a refund of the paid premiums with clean money.

**Case Example 5**

Mr P invested £25,000 in an Investment Bond [an investment type insurance policy], the monies had come from the sale of a house, which was confirmed by a letter from his solicitor. The monies having come direct from the solicitor's client account. The bond was taken out by Mr P's sister who has power of attorney over his financial affairs because Mr P is in prison.

Within the cooling off period the bond was cancelled, Mr P's sister stated that her brother was not happy with the chosen bond. The funds were returned to Mr P's sister. This appears to be an attempt to layer monies that may have been obtained through the proceeds of crime. By divesting his assets Mr P may be attempting to frustrate any attempt by law enforcement to confiscate his assets

Source: UK Based Insurance Firm

***Typology 6: Collusion of customer intermediary and / or insurance company employees***

Several cases showed collusive behaviour between either the customer and the broker or intermediary or between the intermediary and the insurance company. The intermediaries involved accepted illicit funds and transferred them in exchange for high commissions.

**Case Example 6**

A drug trafficker purchased a life insurance policy with a value of USD 80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the client had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in this policy.

Source: Canada

***Typology 7: Third party payments of premiums***

This typology refers to the funding of insurance policies by third parties/ persons different to the policyholder who have not been subject to the regular identification procedures when the insurance contract was concluded. The source of funds and the relationship between policyholder and third party is unclear to the insurance company.

**Case Example 7**

A husband and wife had taken out a life-insurance policy each in their own name with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policy-holders but a company abroad of which they were directors. However, this was a life-insurance policy taken out privately by the couple and not by the company. Investigation revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organized tax fraud for which the couple involved was known.

Source: Belgium

**Typology 8: Risks involved in international transactions - both where this is source of business or a destination of policy payouts.**

International transactions exist in a variety of constructions: a rather simple pattern is the payment of premiums from a foreign bank account or the payout of policies to a foreign jurisdiction. Typologies include those with more complex transfers of money via bank accounts or cheques through different jurisdictions, which complicates the control of the (legal) source of funds by the insurance company. Other forms are foreign customers and customers domiciled abroad who seek insurance policies via domestic or foreign intermediaries. The policy payout is usually to a foreign jurisdiction.

**Case Example 8**

An insurance company was approached with an offer to conclude 4 life policies against one-off payments of 75m for euros each policy. The structure was to be: the policyholder and his 3 partners were to be granted a loan of 340m euros by a large foreign bank. Each would pay 75m euros of this into a deposit account with the insurer. The remaining 40m euros were to be held and invested by the bank to service the loan. The bank would guarantee annual interest of not less than 6% over the entire term of the loan. The loan would be settled in full on maturity by the insurance payments. The policies would be ceded to the bank.

Source: Germany

**Case Example 9**

A number of insurance companies, domiciled in the Isle of Man and the Bailiwick of Guernsey, were identified through information received in a narcotics smuggling investigation as having numerous policies which were paid for with drug proceeds. It was determined that narcotics proceeds were deposited into life insurance policies over a substantial period of time prior to 2001. These policies were primarily established by one "master broker" who operated in Colombia and other South American jurisdictions. For the policies that were identified as containing drug proceeds, the funds entered the policies in several ways. First, and most common, were via third party wire transfers. These wire transfers often originated from money brokers or *casas de cambio*. In many instances, one bulk wire transfer was sent to the institution on the order of the broker. Once credited to the institution's account, the broker provided detailed information of how to break up the wire and which accounts to credit the funds to. The insurer also received payments via third party cheques and structured money orders (to avoid reporting thresholds). Finally, some policies were paid with funds from the commission accounts of the brokers. In this scenario, the brokers accepted cash from the client in Colombia and credited the client's policy with funds from his business operating account or as a piece of his commission cheque.

Source: United States / Isle of Man

**Typology 9: Fraudulent customers, insurance companies and reinsurance companies**

Cases were noticed where criminals established or took over complex corporate structures and then entered into business relationships with insurance companies to get insurance coverage. The purpose of the various commercial insurance contracts was to invest illicit funds. Sometimes this was facilitated by the fraudulent setting-up of insurance or reinsurance companies for ML purposes. Thus the criminals are able to invest proceeds of crimes and to apparently undertake legal business and initiate transfers of money behind the veil of an insurance company or reinsurance company.

**Case Example 10**

Corporation A is an insurance company operating in the US. Law enforcement determined that Corporation A had accepted narcotics proceeds into policies sold by the firm between 1995 and 2003.

A subsequent investigation determined that Corporation A was committing money laundering. Funds were taken into Corporation A and applied as a percentage of a life insurance policy that was being sold by a terminally ill policyholder. In some instances, these funds remained on deposit at Corporation A, awaiting the termination of the policyholder's illness. In the more common instance, the policies were transferred among Corporation A's clients, creating a paper justification for fund transfers into and out of the Corporation A's escrow accounts.

Additionally, for one particular laundering client, Corporation A established a sub account in their escrow account, in effect operating as an unlicensed bank by taking deposits and transferring funds on behalf of this client without any sale of insurance product.

Source: United States

### Case Example 11

Company "Z", was part of a holding structure, jointly with affiliated companies, it established two insurance companies.

The founders of the insurance companies did not have sufficient funds for their authorized capital, so company "Z" grants a loan of 1000000 roubles to one of the established insurance companies. The insurance company in question in one day conducts 40 mutual financial operations for this sum with the other insurance company. The authorized capital of both companies is, allegedly, filled with funds, sufficient for receipt of license for undertaking insurance activities.

The newly established insurance companies obtain legal and fictitious clients (the legal clients are necessary for mixing legal and criminal incomes). Up to 90% of the insurance premium received by the given insurance companies is referred to a group of Russian reinsurance companies who perform repeated reinsurance, transferring a significant part of reinsurance premium to off-shore reinsurance companies in Cyprus and Montenegro.

The remaining funds are used to purchase bills of exchange, issued by the investment company, which is interested in the implementation of the specified scheme. The reinsurance off-shore companies also buy non-secured bills of exchange of the investment company. The latter knows that its bills of exchange will never be presented for payment and freely uses the received "legal" funds for its own investment activity.

Source: Russia Federation

### Case Example 12

A group of persons with interests in home construction effected a payment in favour of construction company "A" under contracts connected with their participation in investment construction (at cost price).

Insurance company "P" accepted possible financial risks to these contracts under a contract of financial risks insurance and received an insurance premium. At the same time the insurance company "P" concludes with the construction company "A" a secret agreement providing that the difference between the market cost of housing and the cost price is transferred in favour of the insurance company as a premium under the contract of financial risks insurance.

When the funds are received by the insurance company "P" they are transferred as insurance premium under the general reinsurance contract in favour of insurance company "X". By way of fictitious service contracts and commission payments made under an agency contract, insurance company X channels the funds to several off-shore shell firms. Beneficiaries of the actual profit, being withdrawn abroad, are owners and directors of the construction company "A".

Source: Russian Federation

## Pervasiveness

The proportion of cases represented by the described typologies is:

Risks involved in international transactions	14%
General insurance for goods likely to have been purchased with illegal funds	13%
Early redemption of policies	12%
Large premium deposits funding annual premium	9%
Collusion of customer, broker, intermediary, insurance employee	9%

Third party payments	9%
Single premium life insurance	7%
Cash payments to purchase insurance	7%
Fraudulent customers, insurance companies and reinsurance	7%
Others	2%

In addition to the above, 11% of cases related to general insurance claim fraud (see below).

The risks ML poses to the insurance sector are distributed throughout the insurance cycle. In a third of the single premium and premium deposit ML cases suspected ML was detected at the underwriting stage of the policy. At the purchase stage of the cycle, suspicion was triggered by the use of cash, or by the fact that payments for finalising the purchase of the policy were performed by apparently unrelated third parties, i.e., individuals other than the policyholder and the beneficiary. And at the end of the insurance cycle, in over 12% of the cases unexpected early termination of the policy, carried out by redeeming it before its maturity, was employed by money launderers.

The most frequently observed individual typology relates to international transactions, which is evidence of the cross-border reach that insurance-related ML operations feature. Clearly where proceeds from illicit activities are invested in insurance products, transferring them abroad represents a further step in disguising the original source of the funds.

24% of cases involved the use of general insurance products. In 13% of all cases criminals or their associates sought insurance coverage of goods and assets purchased with funds of illegal origins. A further 11% of the reported cases involved fraudulent general insurance claims. Whilst fraud itself is a predicate crime for ML, we believe that in the first instance a criminal complaint report should be filed with the competent LEA's fraud investigation team, with subsequent referral by the fraud team to the FIU only if such fraud cases lead to evidence of underlying money laundering operations.

There are a number of cases involve colluding intermediaries or businesses established for the purpose of laundering money. This raises some well-placed concern over the scope and effectiveness of integrity checks, which will be dealt with more in depth later in this report (section IV, 4. Incomplete supervision).

## FINDINGS

Bearing in mind the mandate the experts was entrusted with, the analysis of the wide stock of information provided by respondent jurisdictions was given a two-fold focus:

- Identifying indicators that may help detect potential ML in the insurance sector.
- Identifying vulnerabilities, both at an operational and a regulatory level, that may offer criminals access to the insurance businesses and products.

Furthermore, the experts' aim was to draw some conclusions on what can be done to ensure the insurance sector has an effective system of safeguards to prevent it from being used for ML.

In this section, the main findings in relation to these objectives will be illustrated. Most of the findings result from the analysis of the cases, as illustrated in the previous section, which represents by far the most valuable set of information that the experts could rely on. In addition, especially as far as the sector-specific vulnerabilities are concerned, respondent jurisdictions succeeded in providing an extensive representation of both the operational and the regulatory framework of their insurance sector, including the weaknesses and the shortcomings it may feature.

### ***Finding 1: ML Indicators for the Insurance Industry***

From analysis of the extensive collection of case studies it has been possible to define a broad set of ML indicators specifically aimed at those operating in the insurance sector. We distinguish the different indicators according to the following groupings:

- Indicators not unique to the insurance industry.
- Policyholder characteristics and behaviour.
- Policy characteristics and policy maintenance.
- Other indicators.

#### ***Indicators not unique to the insurance industry***

It goes without saying that the set of ML indicators applicable to all other parts of the financial services industry still applies to the insurance sector. However, some specific indicators emerged as particularly common in the cases submitted by respondent jurisdictions.

**Large one-off cash transactions.** The use of cash often provides an unambiguous mark of suspicious activity, all the more significant the more widespread becomes the use of alternative means of payment; however, on the basis of the picture emerging from the case-studies analysed, the insurance sector, particularly in jurisdictions with a well developed financial services industry, seems less cash-intensive than expected.

**Use of false addresses or post office boxes.** Given the number of cases in which fraudulent customers were involved, accounting for 7% of total cases, market participants need to check key personal data their customers provide and heighten their attention whenever unreliable or patently false information is supplied.

**Overseas business from higher risk jurisdictions.** International transactions turn out to be the riskiest from the scenario emerging from the collection of cases examined. This does not mean that insurance businesses involved in cross-border business are normally used as conduit for ML operations; however, it demonstrates that enhanced identity verification and monitoring procedures have to be undertaken whenever business relations are established with overseas customers. This is particularly true for business coming from NCCTs and tax havens, since the re-routing of funds through foreign locations and intermediaries is commonly used to further screen the origin of the funds.

#### ***Policyholder characteristics and behaviour***

A customer's profile, both financial and personal, represents the main benchmark against which the rationale for the transactions they perform or of the business relationships they entertain can be assessed. Some of the indicators illustrated that follow are applicable across all of the financial services industry; some are highly insurance sector-specific indicators. Clearly there may be innocent reasons why the policyholder acts in a way that initially raises suspicions, but it is for the insurer/intermediary to seek to verify such reasons.

**Where the policyholder is a known criminal, or a relative or an associate of a known criminal.** It would be unfair to relate a transaction or a business relation to ML only because it is connected to someone with criminal precedents, but such connections can certainly be used as an indicator of risk. Clearly it is not always possible for insurers and intermediaries to gain relevant information, such as the personal criminal records of their own customers or of their relatives or associates, which are rightly deemed to be confidential. However, effective customer due diligence procedures and the use

of differentiated sources of information may provide a deeper insight of both actual and potential customers. To this end, the implementation of channels for the exchange of information, to the extent permitted by legislation, within the insurance sector (or even wider) is desirable.

**Erratic or abnormal behaviour by the policyholder.** This includes sudden and unexplained lifestyle changes of the policyholder, unanticipated and inconsistent modification of customers' contractual conditions, unforeseen deposit of funds or their abrupt withdrawal, unjustified intervention of third parties, unacceptable refusal to provide information about himself or about a transaction. Again, insurers' and intermediaries' knowledge of their policyholders should be such to enable them to assess any such event properly and evaluate its consistency with the customer's profile.

**High premium payments compared to verifiable legitimate income.** Data concerning a customer's economic standing is crucial for assessing the consistency of his behaviour and of the transactions he undertakes. With particular attention to individual customers, many insurance products in the life sector have a long-term investment nature, rather than the more speculative, short-term one, that other financial instruments often feature. Accordingly, funds used for purchasing such life policies (particularly where periodic, such as annual or monthly, premiums are paid) are usually directly related to the policyholder's personal earnings, rather than being originated from other financial sources. Any inconsistency between a customer's verifiable economic profile and the scale of investment in insurance products should, therefore, be held to be a particularly significant indicator of ML risk, requiring further investigation.

**Lack of concern by the policyholder over charges/early redemption costs.** Lack of concern by the policyholder of the cost, which is normally far from negligible, a policyholder may decide to incur for the sake of terminating an insurance contract (particularly long-term investment type life insurance) before its maturity signals an increased degree of ML risk, since by way of liquidating the value of the policy, the customer screens the initial source of the funds, which now appear to originate from the insurer. Money launderers appear willing to accept such costs involved in laundering their dirty money.

**Policyholder's undue interest in early payout options.** Related to the previous point, should a customer give the impression of being relatively uninterested in the return of his investment in a life policy, but rather more concerned with the conditions attached to the early redemption of the policy that may provide a particularly well-grounded reason for suspicion. Furthermore this indicator anticipates future suspicious behaviour that the customer may exhibit at a later stage.

**Change of beneficiary.** A widely observed and most effective indicator of risk relates to any change in the beneficiary of a policy that the policyholder requests in the course of the business relation. Repeated and unexplained changes increase the chance that ML is occurring. Such events gain further significance in those cases when the relationship between the policyholder and the beneficiary is not clearly established.

**General insurance coverage for assets of a value that appears inconsistent with the customer's economic profile.** It has been observed that criminals will invest at least part of their ill-gotten income in assets for which they subsequently seek insurance coverage. In order to detect instances of this sort at an early stage, one effective indicator lies in inconsistencies between the customer's economic profile and the value of the assets coverage is sought for.

**Early or suspicious claims in general insurance.** Typologies demonstrate that general insurance is affected from ML risk. Any inconsistent or uneconomic behaviour of a client should be used as an indicator of risk, as in life insurance. Accordingly, any claim placed by customers after a very short period from the initiation of a general insurance contract may be related to frauds or, of more relevance here, may signal that the coverage was sought for ML purposes, with a view to creating as soon as possible the circumstances for placing the claim and thus receiving clean money in the form of compensation from the insurer.

### ***Policy characteristics and policy maintenance***

Once an insurance policy is purchased, depending on its contractual characteristics, insurers and intermediaries are able to collect further insight into the customer's financial conduct and of the interests underlying the business relation. The way the customer manages the contract and his relationship with the insurer/intermediary may provide further effective indicators of ML risk.

**Policy payments made by third parties.** The involvement of third parties, especially when they pay the premiums on an insurance policy, could signify that the policyholder may operate as a figurehead on behalf of the real provider of the financial resources invested in the policy, thus aiming to provide a screen to the actual origin of funds.

**Multiple sources of funds to pay premiums.** It is unusual for funds used to pay policy premiums to originate from different sources, such as different banking institutions, even if all sources could eventually be referred to the policyholder himself. Accordingly, the purchase of the insurance policy in this manner may indicate operations at the layering or integration stage of ML.

**Significant premium top-ups to a policy.** Sizeable or regular premium top-ups, particularly if not anticipated at the commencement of the policy is a key indicator of ML risk for investment type life policies.

**Overpayment of premium, particularly where followed by a request for repayment to be made to a third party and/or another jurisdiction.** The overpayment of a policy premium with the subsequent request of the repayment of the surplus directed to third parties represents an effective method for screening the origin of funds. However we understand that insurers, have in general learnt to detect such instances and consequently either refuse to finalise the transfer of the funds and/or report the transaction to the competent authorities.

**Using an insurer like a bank to move funds around.** Insurers are now in the position of offering ever increasingly sophisticated products to their customers, increasingly competing with other parts of the financial sector. Many investment type life policies offer considerable flexibility in the making of additional premiums and early redemption. However where such products are used by a policyholder in a fashion similar to the way one would make use of a bank account, namely making additional premium payments and frequent partial redemptions, this is an indicator of possible ML. This risk is increased when transferring funds are received or paid to numerous accounts or to foreign jurisdictions (especially if a risky/non cooperative jurisdiction is involved or foreign exchange restrictions are in force in the receiving jurisdiction).

**Early redemption of the policy.** Any peculiar interest that a policy holder may show in early payout options or, conversely, any lack of concern that may be displayed over particularly high charges applied to such redemptions have already been pointed out as useful indicators. Likewise, insurers and intermediaries should examine with particular attention whenever the client actually exerts his right to terminate a policy before its maturity. As for all key events in the policy life, the insurer should gain an understanding for the customer's behaviour. Any doubts in the insurer's mind over the reason for early redemption should be increased if the early redemption takes place in the absence of a reasonable explanation or when the whole transaction turns out to be significantly uneconomic, or defeats the original advantage of holding the policy e.g. taxation breaks. An enhanced indicator for insurers of the possibility of ML risk is the situation where in addition to the above circumstances there is no return of commissions paid to intermediaries by the insurer at the inception of the policy.

### ***Other indicators***

**Unusually high commission charges.** Cases illustrated by respondent jurisdictions demonstrate that if intermediaries applied particularly high commission charges, i.e. in excess of the usual commission or fee charged for that type of product, to the policyholder then this indicated a high ML risk. It was



the case that either the intermediary was directly or indirectly involved in a ML operation., or simply that the intermediary, either because he knew funds of dubious origin were involved in the transaction or since he could sense that the transactions featured a higher risk to himself, demanded a higher than normal commission.

**Involvement of recently established insurance or reinsurance companies or companies whose background does not appear particularly transparent.** The use of fraudulent insurance businesses has emerged among the case studies contained in the questionnaires. Thus, whenever insurers or intermediaries have as their counterparts companies that are relatively new or have an opaque corporate and ownership structure, they should investigate more accurately their counterparts' background, with a view to ascertaining whether it is real companies they are dealing with and not fake undertakings or shell companies, which may be effectively used for ML purposes.

## ***Finding 2: ML Vulnerabilities in the Insurance Sector***

The analysis of the information submitted, and the case studies in particular, revealed that the insurance sector is exposed to a series of vulnerabilities offering criminals a wide range of opportunities for using insurance products for ML purposes. In addition to those vulnerabilities experienced by all financial and non-financial sectors, which usually arise from internal fraud and collusion with criminals, the insurance sector features a comprehensive set of sector-specific weaknesses, that may be classified as follows:

- Vulnerabilities emerging from the way AML regulation is applied in the insurance sector.
- Vulnerabilities connected to specific market characteristics.
- Vulnerabilities associated with the insurance sector's inherent difficulties in identifying ML.
- Vulnerabilities originating from inadequate and incomplete prudential supervision.

### ***Inadequate application of AML regulation***

As has been illustrated at length in the previous sections, in the insurance sector most of the business is channelled through intermediaries. As a result, on most occasions it is intermediaries that in actual fact apply AML regulation on behalf of the insurer. This may cause AML regulation to be undertaken at an unsatisfactory level on two accounts.

Firstly, on the basis of the evidence emerging from the questionnaires, intermediaries are not directly subject to AML regulation in all jurisdictions, but held to operate as mere executors of CDD procedures which they undertake on behalf of the insurers.

Secondly, even though intermediaries are indeed required to comply with AML obligations, since it is the insurers to whom the business relations with the customers have to be ultimately referred, intermediaries are incorrectly considered not to bear the responsibility for compliance.

The involvement of credit institutions in the distribution of insurance products may be viewed as a positive development, given the higher degree of AML regulation compliance that the banking sector normally features.

**Reliance on third parties to undertake customer due diligence (CDD) procedures.** The quality of CDD is one of the pivotal factors on which the system of AML controls hinges, since it allows the identification of ML risks. Failure to undertake identification and verification procedures in an adequate and timely fashion increases the possibility of ML going undetected. More generally, CDD should be considered as a specific feature of financial intermediaries' risk management. Therefore, not only does an inadequate client assessment (because of lack of expertise, time pressure, poor controls

etc.) increase the risk of involvement with ML, but it also undermines the establishment of a correct business relation. As has been explained above, intermediaries undertaking CDD procedures on behalf of the insurer they operate for may not be deemed accountable for any inadequate procedures that fail to prevent ML.

**Suspicious transaction reporting.** It is self evident that customers placing business through an intermediary have a direct contact with the intermediary rather than the insurer. Therefore, on account of the face-to-face relationship with such clients that intermediaries enjoy, it is the intermediary who is in the position of appreciating any factor, or change, in the client's behaviour and economic profile that may justify the filing of a STR. Therefore compliance with AML provisions by intermediaries is essential

**Lack of AML regulation in the general insurance and reinsurance sectors.** Most jurisdictions, unsurprisingly taking their lead from FATF Recommendations, extend the scope of application of their AML regulation only to life and investment type insurance. However, the collection of typologies illustrated in the previous sections demonstrates that criminals may have an interest in seeking general insurance cover for their assets. In this respect, regardless of whether the funds used to purchase those policies are proceeds from illegal activities or not, general insurance is clearly a potentially invaluable source of information from a CDD perspective. By virtue of the much larger transactional values the general lack of AML regulation in the reinsurance sector creates substantial opportunities for the laundering of large amounts of money.

### ***Market characteristics***

**Long distribution chains.** The weaknesses in AML regulation, as illustrated above, is exacerbated where distribution chains are long (as can often occur in the insurance sector) and undue reliance is placed on CDD supposedly carried out earlier in the chain. In this case, the availability of adequate customer's data may be imperilled because of inadequate coordination and breakdown in the information flow. Money launderers can exploit this situation by entering the market through the weakest link in the chain.

**Intermediary incentives.** The dichotomy between legal responsibility and accountability for AML regulation discussed above is all the more evident if the different set of incentives that insurers and intermediaries respond to is taken into account. At its most basic level intermediaries may have no reason for responding to incentives other than pure economic ones, upon which their relationship with the insurer is normally mainly structured. The desire to generate income may lead disreputable intermediaries, or their staff, to either fail to undertake AML compliance satisfactorily or to take advantage of ML situations. Symptomatic, in this respect, is one of the case studies illustrated by respondent jurisdictions, in which a broker charged higher commissions to a customer known to be using funds of illegal origin.

**Increasing volumes and competitive pressures.** The picture of the insurance sector emerging from the questionnaires is that of a rapidly expanding market, competing with other parts of the financial services industry for the customer's attention. To this end, highly diversified products are being designed whose features are much closer to that of investment products than to traditional insurance ones. Moreover, the insurance market is increasingly acquiring a consolidated international dimension, with competitors striving to get access to new and often riskier, markets. Taking a ML perspective of these long-term trends in the insurance sector, it may be the case that the regulatory framework and AML compliance has not kept apace with such rapid developments, and thus the safeguards and the risk-mitigating mechanisms in place are no longer as effective as previously, thus opening up increased opportunities to money launderers.

### ***Difficulties in identifying ML***

As the responses to the questionnaires clearly showed, insurance is widely believed to be a sector featuring a relatively low ML risk. However, actual risk, as measured by the amount of cases involving insurance businesses and products and the extensiveness of the weaknesses the sector suffers from, is far from negligible. The apparently erroneous belief that insurance is relatively safe from criminal infiltration could be the result of two coincident factors: the very nature of the stage of the ML cycle at which insurance products could be used and a generally poor exchange of information among the sector's main participants.

**The insurance sector is primarily vulnerable at an advanced stage of ML.** Insurance products, by their character and the function that is required of them, are usually deployed at an advanced stage of the ML process. At the placement stage of the ML cycle the funds of illegal origin are introduced into the financial services industry. With the notable exception of cash premium payments, insurance products are targeted at the next stages (layering and integration) of the ML process. The purposes that criminals pursue at the later stages are more related to the return they expect from the asset they purchase and its degree of liquidity, that is to say, the ease by which the asset can be liquidated and the associated costs. Since the placement has already occurred and the link between the illegal activity originating the proceeds being laundered and the proceeds themselves has been weakened, if not severed altogether, ML is generally more difficult to detect at such advanced stages and so indicators of risk are more difficult to identify.

**There is insufficient knowledge sharing about ML in the insurance sector.** The picture emerging from the questionnaires indicates that the sector is affected by a generalised lack of effective information channels which may be used for disseminating knowledge relevant to ML prevention. In some of the replies just general information could be provided, e.g. the number of STRs, but not further detailed information with respect to, for instance, reported cases. This information was obviously not readily available to those answering on behalf of the responding jurisdiction. As for the presentation of the information there was no common format used. This might be an indication that among jurisdictions there is no coordination of the way statistical information is collected or stored. The reason for this variation in responses and for the missing information is unclear. It is however possible that this originates from formal barriers to the exchange of information between public authorities involved in AML or other practical difficulties. Similar shortcomings appear to affect commercial operators. Contrary to what is widely observed in the banking industry for example, insurers appear not to have established information-sharing devices in the field of ML. In both respects, it seems clear that the deeply-rooted belief that insurance is generally uninteresting from the perspective of money launderers has played, historically, a crucial role in reducing the attention authorities and market players have paid to this issue.

### ***Incomplete supervision***

The vast majority of respondent jurisdictions indicated that insurance is, not unlike all other parts of the financial services sector, subject to a system of prudential supervision, centred on a monitoring authority which is in charge of safeguarding the stability of the whole sector. Nonetheless, such checks do not seem to be in place, or enforced, evenly across the sector and across different market participants.

**Poor supervision of intermediaries.** A number of case studies featured instances of collusion between criminals and intermediaries. In some cases, businesses placing insurance products were reportedly set up explicitly for laundering money. The possibility of ML schemes making use of colluding intermediaries is curtailed to a major extent where there exists an effective system of licensing checks at the point of establishment of new undertakings operating in the sector (including the integrity of the owners and management), and ongoing supervision.

**Opportunities afforded by international regulatory arbitrage.** The remarkably fast rate at which the insurance sector seems to be expanding, especially in jurisdictions with a far from mature financial sector, causes many jurisdictions to suffer from a lack of effective supervision, since it is not uncommon, as observed also in the other parts of the financial services sector, for supervisory resources to be made available at a much slower rate than that at which the insurance sector is developing.

**Poor supervision in the general insurance and reinsurance sectors.** A number of cases involved the establishment of fraudulent businesses in the general insurance and the reinsurance sector. Such corporate structures emerged as particularly effective instruments for ML, especially given the total or partial absence of supervision in many jurisdiction's general insurance and reinsurance markets, or where a jurisdiction's insurance sector is developing at a rapid pace. The existence of a stringent supervisory system seems an adequate countermeasure to prevent criminals' infiltration of these sectors.

**Secondary markets.** As a result of the development of the insurance sector, formal or informal secondary markets for insurance products have been established in some jurisdictions. Where such markets exist they are seldom included among the scope of prudential supervision, be it that enforced within the insurance sector or the regulation of markets of financial instruments. The lack of controls of these secondary markets is such that, for instance, changes in the holder of a policy or its beneficiary do not need to be notified to the insurer, transforming any such insurance policy into a powerful vehicle for ML.

## CONCLUSIONS

The overall picture of the insurance sector emerging from this review is that of a rapidly expanding and substantial market, with insurers offering increasingly sophisticated products to their customer, competing with other parts of the financial services industry. However, this expansion and increasing sophistication has not been accompanied by a corresponding widespread awareness that insurance products at the same time have become increasingly more attractive to criminals. The perceived risk of the sector's criminal infiltration has historically been low and the responses to the questionnaires generally indicate that no noticeable change has taken place in this respect.

Within this general framework it is possible to spell out in more detail the main reasons why the insurance sector could be attractive for money launderers.

### Life insurance

Across the whole insurance sector, life insurance appears to be by far the area most attractive to money launderers. Substantial sums can be invested in widely available life insurance products and many feature a high degree of flexibility, whilst at the same time ensuring non negligible rates of return. Such characteristics, whilst of considerable value to the honest policyholder, also offer money launderers various opportunities to legitimise their ill-gotten funds.

From the analysis of the information provided we conclude that the typologies support the current approach taken in the FATF Recommendations in respect of life insurance.

### General insurance and reinsurance

Far from being completely immune from criminal infiltration, a well-grounded and considerable set of evidence shows that there are various instances of crimes related to general insurance and reinsurance, which may not be confined to mere instances of fraud, but possess all the features of ML. Some cases provided demonstrate that there is also a risk of corporate structures (such as insurance or reinsurance companies) being set up in order to channel funds to disguise their origin. Identifying fraudulent

insurers is primarily the responsibility of prudential authorities upholding jurisdictional industry standards through licensing, examination and enforcement. Although it is arguable that the funnelling of funds through fraudulent insurers constitutes a trend, one should not exclude the likelihood that on a global scale more cases exist.

Moreover, the focus by the general insurance industry on claim fraud may underplay the extent of ML from two different perspectives. Firstly, where goods are purchased with illegal money, the subsequent taking out of a policy and payment of a claim by the insurer results in funds of illegal origin being laundered, regardless of whether the underlying claim is fraudulent, or not. Secondly, law enforcement agencies, when investigating the misuse of general insurance products, may direct their main effort towards establishing proof of fraud, without tracing the origin of the funds further.

Regardless of the AML focus of the industry on "pure" ML (rather than that arising from illicit claims), it is in the interest of insurers to control the risk of being involved in illegal activities, whatever their nature, because of the reputation of the company / the industry together with the increased operational risk and legal risks involved.

### **Intermediaries**

Intermediaries play an important role in the distribution of insurance. Because they often also market other financial products such as investment products and mortgages and have a face-to-face contact with clients, intermediaries have the best opportunity in the insurance industry to perform CDD.

One of the most important findings emerging from jurisdictions' responses is an insufficient degree of compliance with AML requirements by intermediaries with respect to life insurance. A possible reason for low compliance could be that intermediaries - especially if independent from the insurer – perceive the risk of ML as low and are focusing more on sales figures as the driver for their commission. Insurers, on the other hand, might be reluctant to push for more compliance by intermediaries because of their dependency on these organisations for new business. Therefore, for commercial considerations the subject of client integrity might get too little attention. In extreme cases this has extended to collusion between the intermediary and the money launderer. Whatever the reason it is clear that money launderers have recognised that using intermediaries is a successful way of accessing insurance products.

### **Regulation and supervision**

Based on the typologies examined during this study, it may be that there are no specific amendments necessary to the current regulatory frameworks, except possibly in those jurisdictions which have not already established appropriate measures regarding insurance, such as, for example, requiring intermediaries to file STRs. Enforcement of AML regulations should be ensured by adequate supervision.

The findings showed that there are various instances of crimes related to reinsurance and general insurance with both elements of fraud and ML. The fact that the ML aspects are not always emphasised in such cases might be because of a lack of focus on this area or an understanding of how ML may occur in these sectors. Currently there does not seem to be enough supporting evidence to require extending the scope of the FATF Recommendations to general insurance or reinsurance, though this should be kept under review (see 2.1 below). However, there is wide scope for enhancing risk-mitigating policies and procedures, particularly crime preventing controls that address insurance claims fraud, since these controls most likely address the risks of criminal involvement in a broad sense, thus including ML.

It is also worth repeating here that, on account of the typological evidence respondent jurisdictions made available, international transactions appear to involve a relatively high risk of ML. Enhanced

CDD procedures by insurance businesses when dealing with foreign counterparts thus seem to be necessary, especially if connections with high risk jurisdictions can be established.

## **ISSUES FOR CONSIDERATION**

The findings and conclusions set out in previous sections of this report raise a wide range of issues that need to be considered in order to strengthen AML control mechanisms in the insurance sector and, in more general terms, to mitigate the risk that it may be misused or infiltrated by criminals. In the following paragraphs, we address the main areas where effective action may be taken.

### **Raising ML awareness**

In general a low degree of awareness of the threats posed to the insurance sector by criminal infiltration, and of ML in particular, emerged as a common feature of the attitude of the sector's main participants. Similarly, respondent jurisdictions' widespread perception is that the vulnerability of the insurance sector is relatively low. Conversely, the data on reported cases clearly indicate that there is no room for complacency. Accordingly it would be useful to keep insurance supervisors and the insurance industry aware of possible new typologies and trends. In this respect, what is needed is the introduction of mechanisms supporting the dissemination of information within the sector and the establishment of coordination devices among competent authorities. This would help to ensure that the actual risk of ML in the insurance sector is kept under review, and any increase in the ML risk is promptly acted upon. We believe FATF, IAIS and the Egmont Group have an important role to play in this work.

#### *Issues for consideration:*

##### **1.1 At an international level:**

- The International Association's (IAIS) Guidance paper on AML and combating the financing of terrorism could be promoted among national competent authorities.
- The FATF and the IAIS could cooperate more intensively in sharing typology material with a view to enable both organisations to provide more detailed and updated guidance.
- Analysis of ML risks and threats in the general insurance and reinsurance sector could be carried out on a regular basis.
- Consideration could be given to an improved centralised availability of data and statistics, about which the FATF could liaise with the Egmont group.

##### **1.2 Within each jurisdiction:**

- The ability of national competent authorities to exchange information regarding insurance should be enhanced, by, for instance, removing any formal and informal barriers to information sharing, and establishing effective mechanisms for the provision of feedback to law enforcement organisations and supervisors.
- FIU and law enforcement organisations should have available insurance expertise.
- LEA's anti-fraud units should, if they are not already, be sensitive to ML issues in their fraud work, and refer such issues to AML units such as FIUs and supervisors.

##### **1.3 Insurers and intermediaries:**

- Could set up industry-wide information sharing facilities in the area of crime prevention and ML.

### **Strengthening AML controls and enforcing effective supervision**

This report has identified weaknesses in AML controls undertaken by insurers and intermediaries and weaknesses in the supervision of market participants. Such weaknesses will need to be fully addressed to counter the threat of ML in the insurance sector.

Of particular relevance here is that intermediaries' incentives seem to differ from those applicable for the insurers on behalf of which they operate. As intermediaries relationships with insurers are mainly built upon commercial bases, such as sale volumes and the number of contracts, their sensitivity to reputation issues may be unduly low. CDD undertaken by intermediaries should be undertaken to appropriately high standards. It should be for the insurers and intermediaries to work together to ensure that consistently high standards of AML are being applied. This is particularly true in respect of cross-border transactions, which appear particularly vulnerable to ML.

Supervisors too must play their part. The role of the intermediary is so important that supervisors should pay special attention to their AML activities, and expect to be challenged on their supervisory efforts in this area.

In view of the cases reported on corporate structures being set up in order to channel funds to disguise their origin, it is particularly important that national supervisory bodies give sufficient attention to monitoring beneficial ownership of companies and group corporate and ownership structures. Moreover, fit and proper testing of managers, directors and controllers should apply.

Checks by competent authorities should be applied, in the appropriate scale and form, to both insurance undertakings and the intermediaries operating on their behalf in all branches of the insurance sector. In addition to specific AML compliance checks authorities' monitoring activity should specifically include anti-fraud control mechanisms and customer screening procedures.

At the international level we believe FATF should work with the IAIS to help supervisors identify insurance companies which may be used for illicit purposes

#### *Issues for consideration:*

##### **2.1 Within each jurisdiction:**

- National supervisory bodies could enforce entry and integrity checks in all parts of the insurance sector.

##### **2.2 At an international level:**

- The FATF could liaise with the IAIS to ask it to provide guidance for insurance supervisors on the misuse of insurance companies for illicit purposes.
- Within the framework of AML evaluation exercises, assessors should pay particular attention to supervision / regulatory oversight with respect to intermediaries.

### **2.3 Insurers and intermediaries:**

- Insurers and intermediaries could ensure that intermediaries undertake CDD to the required standards.
- Intermediaries could be required, where this is not already established, to file STRs directly to the FIU, instead of passing them to the insurer(s) they operate for.
- In non-life insurance and reinsurance, highly effective general risk management mechanisms could be encouraged, with a view to help prevent involvement in criminal activity in any shape or form, including ML.
- Insurers and intermediaries could be reminded that particular attention should be devoted to international transactions.



## **List of Acronyms**

<b>AML</b>	<i>Anti-money laundering</i>
<b>CDD</b>	<i>Customer due diligence</i>
<b>EU</b>	<i>European Union</i>
<b>FATF</b>	<i>Financial Action Task Force</i>
<b>FIU</b>	<i>Financial intelligence unit</i>
<b>IAIS</b>	<i>International Association of Insurance Supervisors</i>
<b>KYC</b>	<i>Know your customer</i>
<b>MONEYVAL</b>	<i>Council of Europe Select Committee of Experts on Evaluation of AML Measures.</i>
<b>STR</b>	<i>Suspicious transaction report</i>
<b>WGTYP</b>	<i>FATF Working Group on Typologies</i>

## Glossary of Terms

**Agents:** Professional person (both natural and legal) who is involved in the negotiation of insurance contracts, mediating and aiming at the conclusion of the contract between customer and insurance company for remuneration. He has contractual relations with one or more insurance companies on whose behalf he acts.

**Brokers:** Professional person (both natural and legal) with the same function as an agent but who acts independently from any insurance company. He does not act on behalf of a company but of the customer.

**‘Cooling Off Period’:** This term refers to a contractual regulation in some jurisdictions allowing for the cancellation of an insurance contract and the refund of premiums within a certain contract cancellation period. The customer is as a matter of fact refunded with clean money.

**Commission:** Refers to the remuneration sum of money which is paid by an insurance company or by the customer to the intermediary for the conclusion of a new, or prolongation of, an existing insurance contract.

**General Insurance:** All types of insurance other than life insurance and reinsurance

**Intermediary:** Refers to both agents and brokers as a third party who take up or pursue insurance mediation

**Life Insurance:** The term refers, according to the FATF recommendations, to life insurance products and other investment-related insurance products.

**Placement:** The process of money laundering can be divided into three stages. In the placement stage the launderer introduces his illegal profits into the financial system (e.g. depositing the money with a bank or an insurance company).

**Layering:** In the second stage the launderer separates the criminal proceeds from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. He will process the funds in possibly several transactions through the financial services sector by purchasing various financial instruments. Purpose of the transactions is to break the (paper) trail between funds and their origin.

**Integration:** In the final stage of integration the criminal proceeds are treated as legitimate. If layering has succeeded, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

**Premium:** Refers to the payment of the customer on the insurance policy (his contractual obligation); sum of money to be paid according to various patterns; a single or a few high amount premiums possible; normally premiums are paid in periodic instalments (e.g. yearly or monthly).

**Redemption:** Refers to the refund of a certain amount (percentage) of the surrender value of the insurance contract if the policy is surrendered before maturity.

**Reinsurance:** Insurance business which insures the risk of primary insurance companies.

## **Annex A Questionnaires**

*The following jurisdictions responded to the first questionnaire circulated in relation to this project:*

- |                           |                    |
|---------------------------|--------------------|
| 1. Argentina              | 24. Luxembourg     |
| 2. Austria                | 25. Malaysia       |
| 3. Belgium                | 26. Malta          |
| 4. Belize                 | 27. Mexico         |
| 5. Bermuda                | 28. Netherlands    |
| 6. British Virgin Islands | 29. New Zealand    |
| 7. Canada                 | 30. Norway         |
| 8. Czech Republic         | 31. Portugal       |
| 9. Denmark                | 32. Italy          |
| 10. Finland               | 33. Romania        |
| 11. France                | 34. Russia         |
| 12. Germany               | 35. Singapore      |
| 13. Gibraltar             | 36. Slovenia       |
| 14. Guatemala             | 37. Spain          |
| 15. Guernsey              | 38. Sri Lanka      |
| 16. Hong Kong             | 39. Switzerland    |
| 17. Iceland               | 40. Thailand       |
| 18. Isle of Man           | 41. Turkey         |
| 19. Israel                | 42. UAE            |
| 20. Jamaica               | 43. Uganda         |
| 21. Japan                 | 44. United Kingdom |
| 22. Latvia                | 45. Ukraine        |
| 23. Lithuania             | 46. United States  |

*The following jurisdictions responded to the second questionnaire circulated as part of this project:*

- | <b>FATF Members</b>     | <b>MONEYVAL Members</b> |
|-------------------------|-------------------------|
| 1. Austria              | 14. Armenia             |
| 2. Belgium              | 15. Cyprus              |
| 3. Canada               | 16. Czech Republic      |
| 4. Germany              | 17. Georgia             |
| 5. Hong Kong, China     | 18. Liechtenstein       |
| 6. Italy                | 19. Lithuania           |
| 7. Japan                | 20. Monaco              |
| 8. Netherlands          | 21. Macedonia           |
| 9. Netherlands Antilles | 22. Moldova             |
| 10. Norway              | 23. Malta               |
| 11. Singapore           | 24. Romania             |
| 12. United Kingdom      | 25. Serbia              |
- APG Member**
13. South Korea

*Responses were also received from 6 insurance companies: Aviva, CNP Assurances, Munich RE, Prudential Insurance, SCOR and Swiss RE.*

## CHAPTER III

### PROCEEDS FROM TRAFFICKING IN HUMAN BEINGS AND ILLEGAL MIGRATION/HUMAN SMUGGLING

Human trafficking and illegal migration/human smuggling represent a core business of international criminal organisations. They are now thought to be among the most lucrative of their world-wide activities. Together they are now believed to represent a global challenge of the same proportions as the illegal trafficking of drugs and firearms.

Therefore, devoting a research project to the laundering of proceeds from human trafficking and illegal migration appeared to be timely.

As set out in the initial work plan, the aims and objectives of this project were:

- To obtain case examples of how money is laundered by criminals or criminal organisations involved in the facilitation of human trafficking or illegal immigration.
- To make an assessment of the characteristics of money laundering associated with human being trafficking and illegal migration, and to assess whether these are distinct from other types of money laundering activity.
- To see if significant regional differences exist in money laundering related to human trafficking or illegal immigration.
- To examine best practices and obstacles to successful preventive and repressive policies in this area both domestically within jurisdictions and internationally, given its transnational dimension.
- To identify relevant issues for consideration as to policy and practice in this area domestically and internationally.

Human trafficking was chosen by MONEYVAL as a subject for the joint FATF / MONEYVAL typologies exercise because of the importance of such trafficking as a potential source of proceeds. According to the UNODC, it is the fastest growing criminal business in the world. It was also assumed that many MONEYVAL countries would have significant experience to share in this field.

The *cross-border nature* of human trafficking (and, most likely, of its financial aspects) was another major reason for deciding to work on this topic in an international forum.

Then, it soon appeared necessary to extend the topic to include illegal (organised) migration, which also has some similar implications for countries of origin, transit and destination.

Among the reasons for extending the topic to illegal migration were:

- The need to avoid, for the purposes of our money laundering typologies work, any unnecessary methodological complications arising from the UN definition of human trafficking (see the two protocols to the UN Convention on Transnational Organised Crime)<sup>19</sup>,

---

<sup>19</sup>As indicated in the UN website, “In some respects, trafficking in persons resembles the smuggling of migrants, which is the subject of a further Protocol (Protocol against the Smuggling of Migrants by Land, Sea and Air), but there are several important differences.

- The fact that the distinction between human trafficking and illegal migration is not always obvious to authorities which are not dealing with criminal investigations of such cases, and
- That a global overview may be needed to determine whether a given case is actually one of human trafficking or of illegal migration, whereas such an overview may not be available first hand (e.g., a case can be seen as illegal migration in the transit country and human trafficking in the country of origin or destination).

Indeed, it is noted that in some jurisdictions, the elements of the criminal offences themselves can significantly overlap. Migrant smuggling has also been described as “facilitated illegal immigration”. Countries reporting describe how significant percentages of illegal immigration are now facilitated. Hungary reported that, while in the mid 1990s, 20 to 25% of persons who were helped to leave their home countries were assisted by facilitators, today this proportion exceeds 70%. It is also noted that smuggling fees charged are substantial and increasing. Few clients can raise the entire smuggling fee from their personal assets and fewer still appear to be willing to put that much money at risk by paying in full before obtaining their objective. In these cases, migrants may have to work off debts through servitude in a transit or destination country.

The underlying (“push and pull”) factors are well known. On the one hand, there is a perceived need for cheap labour in certain developed states. On the other hand, many persons in less developed countries, where living standards are poor, wish for a better life in more developed countries. Sometimes, other political considerations in their own countries encourage prospective migrants to pay to leave. They frequently resort to individuals or criminal organisations for assistance in illicitly crossing international borders. Such movements of persons often involve long journeys from the source country, sometimes across several land borders, through transit countries to the ultimate destination, often using vehicles. Equally, illegal immigration may simply involve the purchase of air or sea tickets. Whatever the means of transport, in the majority of cases, most facilitated illegal immigration involves the obtaining of sophisticated forged travel and identification documentation - which can be part of the “service” offered to the candidate migrant. Forged travel documents often will be difficult to detect, especially if the “service” is provided by well organised and professional smugglers.

At the destination the business relationship in facilitated illegal immigration usually ends, and the balance of fees is paid, or has to be worked off as a debt. It is here perhaps that there is a possible overlap with human trafficking: where illegal migrants who seek facilitated passage across international frontiers cannot pay off their debts they can themselves become victims in the same way as those smuggled with a view to prostitution etc.

Human trafficking, as also noted in footnote 1, usually entails the illicit recruitment and transportation of men, women and children across borders with a view to “enslavement” – e.g., sexual servitude in brothels, or other forms of cheap labour. Sophisticated international networks (often spanning

---

The smuggling of migrants, while often undertaken in dangerous or degrading conditions, involves migrants who have consented to the smuggling. Trafficking victims, on the other hand, have either never consented or, if they initially consented, that consent has been rendered meaningless by the coercive, deceptive or abusive actions of the traffickers.

Another major difference is that smuggling ends with the arrival of the migrants at their destination, whereas trafficking involves the ongoing exploitation of the victims in some manner to generate illicit profits for the traffickers. From a practical standpoint, victims of trafficking also tend to be more severely affected and in greater need of protection from re-victimization and other forms of further abuse than are smuggled migrants.

Finally, smuggling is always transnational, whereas trafficking may not be. Trafficking can occur regardless of whether victims are taken to another country or only moved from one place to another within the same country.”

countries of recruitment/origin, transit and destination) are required to ensure a constant turnover of people to service the demand. Classically there are clearly identified “victims” in human trafficking, and often force or other elements of coercion are used. Victims in the destination countries are often “owned”. In many cases, the level of physical and psychological damage inflicted upon the victims is so severe and enduring that it can be impossible to restore them to complete health.

### **Brief History of the Work Carried Out**

Trafficking in human beings and smuggling of migrants is on top of the agendas of a number of international organisations and individual countries. Thus, research is conducted on a regular basis at these levels. At national level, research work is particularly visible in destination and transit countries. Some examples of those publicly available reports dealing with these issues are:

- Annual threat assessments on serious and organised crime of the National Criminal Investigation Services - NCIS (UK) at: [www.ncis.gov.uk](http://www.ncis.gov.uk)
- Annual reports on organised crime and on trafficking in human beings of the *Bundeskriminalamt* (Germany) at: [www.bka.de](http://www.bka.de) (German only)
- The 2002 reports of the Centre for the Study of Democracy (Bulgaria) on Smuggling in Southeast Europe and on Corruption, trafficking and institutional reform at: [www.csd.bg/publications](http://www.csd.bg/publications)
- The 2002 report on Trafficking in Human Beings, Illegal Immigration and Finland of HEUNI at: [www.heuni.fi](http://www.heuni.fi)
- The 2002 report on Trafficking in Human Beings in Southeast Europe produced jointly by UNICEF, UNOHCHR and OSCE/ODHR at <http://www.unhchr.ch/women/trafficking.pdf>
- Annual reports on organised crime of the Council of Europe at [www.coe.int/economiccrime](http://www.coe.int/economiccrime) ; see also the Council of Europe website on trafficking in human beings and the current work on the drafting of a Convention on trafficking in human beings at [www.coe.int/trafficking](http://www.coe.int/trafficking)
- Annual reports on organised crime of EUROPOL at [www.europol.eu.int](http://www.europol.eu.int) , as well as the serious crime overviews: 2003 and 2004 reports on “Trafficking in Human Beings”, on “Trafficking of Human beings: child abuse”, on “Illegal Migration” (extensive versions of the reports are sometimes available to EU member State officials only but abridged versions can be found on the website).
- At the level of the UNDP in Vienna, a (non public) database was set up. It contains data from multiple sources on global trends, cross national routes and the volume of trafficking in persons and smuggling of migrants, as well as data on victims and offenders of trafficking and responses of criminal justice systems to this criminal activity. The analysed data will result in regular reports including results at national, regional and global levels. A first preliminary findings paper has been published at [www.unodc.org/pdf/crime/forum/forum3\\_note1.pdf](http://www.unodc.org/pdf/crime/forum/forum3_note1.pdf). The "Global Crime and Corruption Trends" report, currently under preparation, will also address human trafficking and its links to organised crime, drawing on results from the data collected.

It is estimated that USD 10 billion a year is generated by the facilitation of human trafficking and illegal migration.

However, unlike other serious and organised crime topics, there is very limited knowledge about the methods being used by criminal organisations to launder illegal proceeds related to human trafficking and illegal migration.

## Methodology

The present report is the end result of work carried out by one of the five workshops of the joint FATF / MONEYVAL typologies meeting held in Moscow from 6 to 8 December 2004.

This workshop involved representatives from the following countries: Belgium, Bulgaria, Cyprus, Hong Kong China, Croatia, Denmark, “The Former Yugoslav Republic of Macedonia”, Hungary, Italy, Lithuania, Luxembourg, Malta, Slovak Republic, Slovenia, South Africa, Spain, United Kingdom, United States of America.

The discussions were facilitated by the Slovenian project leader, who also was responsible for preparing a work plan and a questionnaire (see appendix) to guide the workshop discussions. He was assisted in this by a steering group comprising some of the above countries, as well as the MONEYVAL Secretariat. A discussion paper, based on the responses to the questionnaire, was also prepared to guide the workshop discussions. Replies to the questionnaire were provided by 25 FATF and MONEYVAL countries altogether, prior to the typologies meeting.

During the workshop, presentations with concrete cases were made by several countries. At a later stage, the workshop was split in two groups to discuss money laundering aspects in connection with trafficking in human beings on the one hand, and illegal migration/human smuggling on the other. The findings of the workshop were then presented to the typologies meeting plenary on the last day by the project leader.

## FINDINGS

***Finding 1: Investigation: the predicate crimes and associated money laundering are being detected through both the preventive anti-money laundering systems and by law enforcement independently. The reports through the preventive system are usually confined to traditional obliged institutions. The most successful countries target the proceeds in parallel financial investigations, and follow the financial flows.***

Investigations of the predicate offences and associated money laundering can be triggered through both the preventive and the repressive systems. Thus, there are many possible players in the detection of these offences. As for the preventive system, they include: the entities obligated to report suspicions to the FIU and the FIU itself, and the Customs (where a reporting duty for certain amounts of cross border movements of funds exists). The main law enforcement authorities which generate investigations independently are: the border guards, Customs services, Immigration services, Intelligence services domestically and internationally, domestic police units investigating the predicate offences and units of the police responsible for financial investigations. Sometimes, joint teams are created in individual domestic cases.

Partly because of the variety of agencies involved in preventing and combating human trafficking and smuggling of migrants, information sharing between the various authorities which may be involved is an important issue. The creation of information focal points in certain jurisdictions has proved helpful. Belgium and the United States reported the development of centres for information and analysis for human trafficking. In the Belgian example, all parties involved are connected to a secure website, enabling them to feed the site with information and to access all data on it. This was found to enhance domestic cooperation. From the replies to the questionnaire, it was not always clear how the investigations of human trafficking and smuggling are triggered. In some cases it was suspicious transaction reports arising from remittances from individual persons, which attracted the attention of banks and which were reported to the FIU. Belgium indicated that, on 31 December 2003, the number of such files transmitted by the FIU to law enforcement was 262, representing nearly 5% of the total number of files transmitted by them since their establishment in 1993. A rising trend in the number of

these files has been noted over the last few years. In 2003, more than 11% of the files transmitted by the FIU to law enforcement related to this type of crime.

Other cases appear to have been generated by law enforcement domestically or in an international context (by international intelligence networks, on the occasion of a bilateral investigation – see typology 6, for instance). The police and the immigration services especially play an important role in the uncovering of human trafficking and smuggling, and the financial schemes that accompany them.

Special investigative means, in particular interceptions of communications, undercover operations – including the use of “front” shops/businesses – have been found to be useful tools to obtain evidence and information, including evidence and information about the proceeds generated by the criminal activities. Parallel financial investigations targeting proceeds (with the application of temporary measures) are leading to successful money laundering prosecutions and confiscation of proceeds in some jurisdictions, but, as noted below, this is far from universal.

As far as cross-border movements are concerned, the Italian experience has shown that analyses of the origin of funds declared at the border (where such a reporting duty exists) can provide a useful geo-strategic overview. Such analyses have shown unexpectedly large amounts being carried by people from distant countries, compared to Italy’s immediate neighbours. Random checks can then focus on perceived risk groups and facilitate the detection of undeclared monies (e.g., for the period December 1999 to June 2002: Euro 14,5 million was detected in connection with travellers from Hong Kong and from China). Recent cases have shown that Chinese criminal organisations present in Italy are involved in human trafficking.

It is interesting to note that social security and labour administrations (and inspectorates) – although they can be directly involved - have seldom been mentioned as sources of reports or information useful for human trafficking and illegal migration cases. Occasionally, the labour administrations have been useful to cross check data, for instance to confirm suspicions as to the real number of employees working for a business suspected of being directly involved in smuggling of workers/immigrants.

The limited role of the tax administrations was also observed, although they too have been mentioned occasionally as a source of information to cross check data. This was, perhaps, surprising because prostitution and shadow economy labour are areas of concern for these agencies in a number of countries. Health care systems, social workers and humanitarian organisations – likely to be confronted with the kind of distress generated by the exploitation of human beings – have almost never been mentioned in our research as sources of reports and intelligence.

During the discussions, some members pointed to the Brussels Declaration on Preventing and Combating Trafficking in Human Beings, adopted by the European Council in June 2003, which provides a useful starting point for European countries tackling these problems. It addresses issues such as the need for involvement of the civil society and the private sector in the fight against human trafficking, as well as the need to improve cooperation between origin, transit and destination countries. This illustrates, once again, the importance of international cooperation (notably between law enforcement agencies), considering the *cross-border nature* of the crimes.

### ***Finding 2: Profits and prices: information is fragmented***

It remains a challenge to estimate the overall profitability of human trafficking and illegal immigration globally. Indeed such an exercise could only be speculative, and would add little to estimates given in other published documentation.

To establish real figures from which possible extrapolations could be made would involve gathering a whole range of data. As noted above there are numerous factors which determine prices paid. Assessments of profitability derived from detected and documented cases in Slovakia indicated



variations from hundreds of Euros to several hundreds of thousand Euros. In order to assess the overall amount of moneys generated by a single transporting operation, one would need to assemble all the known costs incurred in the origin, transit and destination countries. For example, the only figures which appeared available to the Serbian authorities related to the costs for the transit of Chinese migrants through Serbia, for destination elsewhere.

Both offences generate much of their direct proceeds in cash and most of the direct proceeds are made, one way or another, by “working”.

Information about prices charged is usually gathered by law enforcement intelligence. In some countries, it is believed that costs account for up to 50% of the prices paid. Costs include: bribes paid to facilitate the operation, payments for travel/transit, payments for accommodation/hiding in safe houses en route, special services (e.g., special security cross-border transfers).

### ***Prices for human smuggling/assistance to illegal migration***

The figures available are the *prices* charged in individual countries. They range from about Euro 250 to USD 100,000, the most expensive country to enter being apparently the US, followed by Canada<sup>20</sup> and the Scandinavian<sup>21</sup> countries. The table beneath provides some examples:

Route/country of destination	Average cost
To the USA, depending on route and origin	USD 1,000 – 100,000
From China to Italy	USD 13,000
From South Asia to Spain	Euro 6,000 (12,000 if false ID provided)
From North Africa to Spain	Euro 4,000 (6,000 if false ID provided)
Through Hungary (from Russia to Western Europe)	Euro 800 – 10,000
To / through Cyprus	USD 3,000 – 5,000
From Slovakia to Italy	USD 3,000 – 4,000
For transit through “the Former Yugoslav Republic of Macedonia”	Euro 1,000-1,500
For transit through Serbia and Montenegro	USD 1,000
Through Malta (from Africa to mainland Europe)	USD 800 to 1000
To/through Croatia	Euro 500
From Hungary to Italy	Euro 500
To enter “the Former Yugoslav Republic of Macedonia” from a neighbouring country	Euro 250-300

The factors determining the prices include:

- The nationality and wealth of the prospective migrant.

<sup>20</sup> The Canadian authorities, in a later comment, confirmed that “Smuggling fees charged to reach Canada vary by mode of transportation and by particular market. Anecdotal evidence obtained from smuggled persons suggests that these fees range from USD 20,00 to USD 60,000”

<sup>21</sup> Prices of trafficking services for the route Sofia to Denmark or Norway are about 5,000 to 6,000 USD (source: CSD 2002 report on Corruption, trafficking and institutional reform)

- The risks involved in the journeys. The more secure borders appear to be, the more difficult (and therefore expensive) they will be to penetrate.
- The degree of professionalism of the “service provider”: the Slovakian authorities, for instance, pointed out that, as a rule, well established and well organised criminal groups (usually top organised groups within the criminal hierarchy), with strong internal structures and wide sharing of responsibilities for the migrants, demand higher prices.
- The degree of comfort expected on the journey also had an impact on price, in the Slovakian experience.
- The attractiveness of the country of destination.

### ***Prices for trafficking in human beings***

These prices are more difficult to assess. One of the possible reasons for this could be that this activity is conducted under an even greater “law of silence” (because of the use of threat and violence) than the activities involved in assistance to illegal migration. The price can also depend on the cost of the journey and the perceived “value” to the criminal groups of the victims.

Some countries have, nonetheless, been able to provide some overall figures. For example, Serbia and Montenegro reported that, according to earlier estimates, principal organisers of trafficking in women in their country could earn DEM 500,000 per year. Currently, it is estimated that profits from prostitution in Serbia alone amount to Euro 40 million annually, not including high class prostitution and proceeds from trafficking in women, which are considered to be significantly larger. Cases have also been reported where prostitutes were bought for 2,000 USD and sold after some time to another exploiter/pimp for the same or a higher amount.

Another phenomenon, reported by Italy, is the kidnapping of migrants. This illustrates how an illegal migrant case can turn into a human trafficking case. By relying on connections with Far East criminal organisations, a “batch” of Chinese migrants is “purchased” at an average price of Euro 5,000-6,000 per person. The transfer to Italy usually involves a stop-over in an eastern European country. The group is then handed over to the organisation which is responsible for smuggling the migrants across the Italian borders. Once in Italy, they are (unexpectedly) held captive until someone, either the relatives or their final employers, deposit a ransom for their release. The ransom amounts to over Euro 13,000. Should no one pay, the migrants are sold to another organisation or are enslaved in illegal manufacturing activities.

***Finding 3: There are some parallels between the flows of persons in these cases and the money flows, although the payments for transportation in illegal migration can be split between the countries of origin, transit and destination; the profits from human trafficking are generally invested in the country of destination or origin***

Information provided by the countries indicate that the problem of human trafficking and smuggling translates geographically mainly into a south to north and east to west flow of persons. In Europe we have seen networks trafficking women from some non European Union countries into the European Union, notably the destinations being the larger developed countries in Western Europe. The newer members of the European Union currently remain largely transit countries. Outside Europe, Canada has become a destination and transit country for women trafficked for the purposes of sexual exploitation from China, South Korea, Thailand, Cambodia, the Philippines, Latin America, Russia, and Eastern Europe. Most transiting victims are bound for lucrative markets such as the United States. The money routes are often similar to the human ones.

There are some specificities, depending on the proceeds-generating (predicate) offences being considered.

For *illegal migration/human smuggling*, there is a payment made by the migrant to the criminals. The payment can take place at different moments:

- In advance, in the country of origin (sometimes as a contract on transfer, which can imply a multiplicity of attempts until the transfer succeeds).
- After the transfer, in the destination country.
- Partly in advance and completed at the end (the illegal migrants who cannot pay the whole amount will pay the balance afterwards).
- Step-by-step, notably when payments are also made in the transit countries or for certain services.

The moment of payment can sometimes depend on the ethnic origin of migrants: for instance, it appears that Asian migrants tend to pay at the end, whereas North African migrants pay in advance. It may also happen that a group of migrants has been “stolen” by criminal organisations other than the one which was to receive the shipment. In this event, the migrants are required to pay a second transfer fee before being released.

The experience of various countries shows that there can be a variety of actors with different tasks involved in such criminal activities. The Hungarian authorities, for instance, have identified no less than 7 different functions: recruiters, organisers, consignors, guides, transporters, falsifiers, hosts and hidiers, watchers or guards etc. Occasionally, accomplices within law enforcement agencies (police, border guards etc.) would provide information on the best crossing points and periods for operations, or other forms of support. Various countries agree that many criminal organisations involved in human smuggling/illegal migration tend to have looser, horizontal structures - rather than hierarchical, more organised vertical structures. The consignor does not directly take part in the operations; he/she is in charge of the money movements and it is with him/her that the migrant is in closest contact, even when sums have been paid for different parts of the service (e.g., to the transporter).

For *human trafficking*, and leaving aside those cases which overlap with illegal migration/human smuggling, cash flows mainly take place between criminals (recruiters, transporters, exploiters etc.). The payments can be made in exchange for services similar to those set out above in relation to human smuggling/illegal migration, or for the sale of people from one exploiter to another. Australia underlined that, for the purpose of sexual servitude, in South East Asia girls are usually recruited through more informal and personal networks of extended family, friends and acquaintances, rather than institutional and sophisticated organised crime networks. Passports, visas and travel requirements tend to be paid by the recruiters, who are then remunerated by the “contract owner” based in Australia once the girls have arrived at their place of servitude. Law enforcement information indicates that there are instances of multiple “contract owners” for one person. The brothel owners jointly pay for one person.

The main goal and criminal profit of trafficking, however, remains slave labour (industry, services, prostitution). The criminal proceeds are thus generated throughout a continuous process where the victims are located. These profits are huge and need to be laundered. The direct proceeds of illegal migration offences are usually the payments for the whole trip. By contrast, in human trafficking, the direct proceeds can include not only the payment for the trip but the profits from servitude, which can be difficult to quantify. Ways to evaluate the real criminal profit derived from certain forms of slave labour in the industry (which would incorporate unpaid salaries which otherwise would have been necessary, social contributions, taxes etc.) were not discussed in detail.

Proceeds may or may not need to be transferred abroad. It appeared from the cases discussed that proceeds are either sent back to the country of origin of the victims/criminals, or were invested locally,

where the exploitation takes place. It further appeared that monies are not usually transferred to “safe” countries for the purpose of dissimulation (as with some major proceeds generating offences).

***Finding 4: There are many types of money transfers connected with these cases. They need to be carefully analysed to determine whether they represent evidence of the predicate offences or the laundering of criminal proceeds. Sometimes money transfers can be both. The sums may be capable of confiscation either as proceeds or instrumentalities.***

Because both offences generate much of their direct proceeds in cash and because cash proceeds often need to be sent abroad (where for example the criminal organisation has a recruiter in the country of origin and accomplices in the country of destination), the money transfers can play a crucial role in the hiding of proceeds. It, however, is often difficult to distinguish between those movements of money which, for example, represent simple payments to couriers (and can be evidence of the predicate offence), and the laundering of criminal proceeds through the various stages of classical money laundering (placement, layering, integration).

There are the patterns of particular money transfers or payment methods to persons facilitating human trafficking and illegal immigration, as well as the remittances, described in some of the replies, which are often sent back home to the source countries by or on behalf of persons who have been trafficked for prostitution. All such transfers, if identified, may be indicators of these offences, and evidence of the predicate offences. In some, but not all cases, they may also represent the direct proceeds of criminal offences. In some human trafficking cases, the victims themselves were reported as having been “used” in order to facilitate the movements of profit back to other members of the trafficking network in the country of origin. If not the victim, other intermediaries may be used, for instance to open a bank account for such purposes (see typology 2 below).

Reported cases in Europe show that human trafficking organisations extensively utilise the services of two wire remitters in particular to pay couriers and sometimes to collect fees from source and destination countries, and that identification of the wire remitters can be problematic.

Money remitters were also identified as being used for the laundering of criminal proceeds in both types of predicate offence.

Another money transfer, which, if identified, might lead to the detection of an offence of illegal migration, concerns the monies borrowed by candidate immigrants to demonstrate sufficient funds to support their residence in certain countries. Once the immigrant has been accepted, the money is paid back, often using money remittance services. Such transfers might constitute evidence in an illegal migration case and might be confiscatable as an instrumentality rather than as proceeds. It is noted that the potential importance of such remittances as indicators of crime also could easily be overlooked by law enforcement/obliged entities/supervisory authorities, given that money remittance services were developed to assist migrant workers to send part of their earnings home to relatives.

***Finding 5: Some vehicles – in particular money remittance services - are more frequently used than others, though no new money laundering techniques were identified***

No novel money laundering techniques have been identified which can be uniquely associated with these offences.

From the replies provided, it appears that the criminal profits in these cases also include proceeds which are used immediately for daily living and for the acquisition of consumer goods (including vehicles), while other amounts are ultimately integrated through investment in real estate and businesses.

As with other cash generating criminal offences, a practical question for investigators and prosecutors is when can laundering be charged. It was noted by some countries that reported in this project, that

the legal structure and/or practice in these jurisdictions allowed for the possession, acquisition or use of consumer goods to be considered as laundering offences, while in others, only the accumulation of proceeds and the various movements (layering) and their subsequent introduction into the legitimate economy (integration) constitutes laundering.

It appears that there are some region-specific patterns. Reported cases, mainly in Europe, appear to show profits at the final stage of the laundering process being invested in banking and insurance products and in real estate or businesses. In other areas (e.g., Asia), underground banking systems (Hawala and Hundi) are being used to retain criminal proceeds.

It appeared from the cases presented and the information submitted by our respondents that some techniques are used more often than others.

*Frequently used money laundering techniques (bearing in mind finding 4)*

- Wire remittance services appear to be a very common means for transferring/laundrying proceeds from illegal migration and human trafficking. These services were involved in one way or another in the vast majority of cases described. The following patterns were observed:
  - Smurfing/structuring - sometimes the same persons perform a number of transactions with the same or different service providers over a short period of time.
  - Use of false identification documents or those of illegal migrants or victims of trafficking.
  - A remittance service being used together with an associated economic entity (e.g., travel agencies. In the United States, these are sometimes reported as being used as fronts for migrant smuggling and trafficking, with the proceeds being reinvested as an income of the travel agency - see typology 8 case C below).
  - Clients being accompanied by other persons (the real client).
  - Cash being sent by different senders to the same person abroad.
- Use of other money transfer services (e.g., telegraphic transfers or postal money orders).
- Use of cash/body couriers (often for large sums).
- Use of underground banking structures (including unlicensed money remittance businesses).
- Purchase of real estate, vehicles and other tangible objects, mostly registered under different names.
- Investments in legal cash based business activities (bars, restaurants and the like); in several cases the businesses were of the same ethnicity as the victims of the human trafficking; in a number of cases, victims of human trafficking/migrants were “employed” in these businesses.

*Less frequently used money laundering techniques*

- Use of non-resident bank accounts.
- Purchase of gambling chips in casinos.
- Use of “back to back” loans (the proceeds are used to guarantee a loan and once the latter is granted, it is repaid with the proceeds – see typology 10).
- Loans given to legal persons in cash.

- Monies being sent by different senders to one person of standing in the same ethnic community and he / she then sends large payments abroad.

Indicators related to money laundering associated with human trafficking and illegal migration have not yet been identified in a number of countries and information and experience is still lacking in respect of the proceeds generated by these offences.

The following indicators were, however, noted in the cases reported by some other countries:

*a) Where the financial system is used:*

- Structuring of funds below cash reporting limits, often using international money transmitters, and exchange offices which carry out such functions (remittances often being sent to sensitive jurisdictions). It is pointed out that repetition of such transactions (with the same people as receivers) and the sensitive nature of the countries of destination are often more important than the amounts.
- Use of the same financial institutions and the designation of the same beneficiaries.
- Atypical or uneconomic or unjustified fund transfers to and from jurisdictions.
- Depositing money in small amounts but where the totals are large in a short time.
- Important transfers on accounts, followed immediately (the same day) by important and repeated cash withdrawals.
- The involvement of high risk countries.
- The existence of unrealistic wealth compared to the client's profile.
- The presence of an accompanying person whose role is unclear.
- Use of fictitious documents, and sometimes fictitious companies.

*b) Where the criminal funds have been incorporated into the activity of a legitimate business, the non- or under-reporting of income/non-submission of tax declaration for the entrepreneurial activity is quite a common pattern.*

In certain countries, the analysis of the laundering of proceeds from human trafficking and smuggling of migrants is currently under way and although some patterns have already been identified, it could be that further, important connections might be established between these predicate crimes and certain business activities already identified as vulnerable to, and responsible for money laundering (e.g., in Italy: textile import, leather manufacturing and trading, and restaurants run by Chinese nationals – see under typologies). The money laundering indicators already identified with regard to these businesses are the following:

- Financial turnover of the company which is overlarge compared to the commercial turnover (unprofitable firms).
- Overlarge profit compared to the commercial structure (little staffing, low real commercial activity, no adequate facilities etc.).
- Use of locals to manage an ethnically-based business (Italy pointed to Italians running Chinese businesses to facilitate relations with financial intermediaries).

*c) Indicators identified in the framework of other schemes include:*

- The non reporting of transborder cash movements.
- The registration of goods, purchased with criminal funds, under other names (relatives etc.).

***Finding 6: In many human trafficking/illegal migration cases, criminals launder their own dirty money***

While the use of professional launderers is reported in the United States, Italy and Russia, in many cases it was observed that criminals launder their own proceeds. It was noted that this has implications for those countries which do not recognise “own proceeds” laundering as a category of the money laundering offence (see below).

## **TYPOLOGIES**

***Typology 1: Money Remittances (two money remittance networks in particular and foreign exchange offices providing similar services etc.)***

As noted, the use of money remittance services is a recurring theme so far as the financial aspects of human trafficking and smuggling of migrants is concerned. It appears that these services, which are used by migrant workers to transfer part of their earnings to their families abroad, and are also used by illegal migrants to pay their fee/debt and also for the criminals involved to launder proceeds. Various reasons for the use of these services were given. The most common ones were: the simple fact that remittance networks around the world are very developed and provide fast and less expensive transfers; the ease with which insufficient or, in some cases counterfeit identification can be used; the lack of limitation on the number of times such services can be used in any one day; and the lack of proper oversight of many such agencies, including in some countries the lack of clear data or information as to the number and types of entities providing these types of services.

### **Case Example 1**

In all cases dealt with by the Slovenian FIU, the suspects used a particular money remittance service network for their money transfers. The fact that the suspects were the recipients and at the same time the remitters of money in the transactions concerned caused problems for law enforcement. It was not clear whether these transactions were part of the perpetration of the predicate criminal offence of illegal migration, or whether they were to be considered as money laundering. Notwithstanding, the FIU found out that the money, which the citizens (refugees) and Slovene citizens (organisers) received from abroad, did not derive from payments for legally performed business activities, because there were no such businesses registered, which could result in legitimate earnings. In addition to the exchange of the amounts from foreign currency into Slovene *tolars*, which is a characteristic of the first stage of money laundering, and immediate remittance of the dirty money abroad, it was possible to infer that a criminal offence of money laundering was committed. This was based on the fact that the suspects used one of the most expensive systems for their remittance abroad. The organisers had to pay very high fees to the banks for the executed money orders through a particular money remittance network, which for asylum holders are considered to be economically illogical transactions. Another fact which raised suspicion was that the Slovene citizens (the organisers) though receiving the money through the particular money remittance network had not submitted their income tax statements to the Tax Authority.

### **Case Example 2**

During the period of July 2001 – September 2003, two sisters received remittances for a total amount of Euro 950,000 on accounts held in Bulgarian banks, and also through agencies affiliated to a particular money remittance network. These remittances were made by different persons based in Syria, Lebanon and France. Some of these remittances were ordered by Bulgarians. Information provided to the FIU by the Bulgarian law enforcement bodies revealed that these sisters were engaged in organising prostitution, and human trafficking and that they possessed large amounts of money, several cars and drivers. The problems for law enforcement were the lack of full identification of the ordering customers, and the fact that the sums were structured in small amounts, ranging from Euro 500 to Euro 6,000. Once the funds arrived on the accounts, they were drawn off immediately in cash with the justification that they were destined to relatives of the ordering customers. The case continues to be under investigation.

A typology involving exchange offices is set out under typology 3.

### ***Typology 2: The Use of Intermediaries (or “straw men”)***

Intermediaries (or “straw men”) are used to perform different kinds of transactions, whether in the banking system or in relation to transfers using wire remittance services. They appear to be used typically as a screen between criminals and financial operators, or for smurfing in order to avoid the reporting threshold.

### **Case Example 3**

One of the reported files concerned an Asian student residing in Belgium who had opened an account with a Belgian bank. Shortly afterwards a Belgian restaurant owner of Asian origin was given power of attorney on the account. During one year the account exclusively showed international payments from Central Asia featuring the same clients. The funds were first withdrawn in cash, first by the Asian student and later by the restaurant owner. According to information obtained by the Belgian FIU, the student had a temporary student visa so he was not allowed to perform any professional activity in Belgium. Police intelligence revealed that the restaurant owner was known for accommodating Asian nationals residing illegally in Belgium. The student, who did not have any official income, clearly acted as an intermediary to open the bank account for the restaurant owner, who also performed cash withdrawals as he had the power of attorney for the account. The international transfers were apparently destined to him. The file is currently under police investigation.

### ***Typology 3: Cash Couriers***

Cash couriers are often used for facilitating payments and moving money back to source countries in these types of offences. In general, they seem to be used for the movement of larger amounts. The role of the courier may be limited to a short period (for instance the time needed to perform a transaction – see case below involving exchange offices). The courier may also be closely connected with the criminal group. The use of body couriers is referred to in typology 8, case A.

### **Case Example 4**

In several files Ecuadorian and Dominican individuals performed transfers through international payment systems in Belgium. For some months they repeatedly went to the same exchange offices, sometimes several times a day. The beneficiaries of these payments, on average some 500 EUR, were individuals in Ecuador and Dominican Republic. Given that the individuals involved did not have any professional activity in Belgium or abroad these transactions did not have an economic justification. Moreover, the individuals were not domiciled at the address that they had stated and this address also featured in another file that had been transmitted by the FIU to law enforcement for exploitation of prostitution and/or trafficking in human beings. The Belgian FIU already knew various Ecuadorian individuals from other reported files dealing with this type of offence, as did the police. These files are currently under police investigation.



#### ***Typology 4: Use of Victims to Perform Transactions***

In the case of trafficking in human beings, it is not uncommon that the victims themselves are used to perform transactions under their own names or using other ID documents. The technique is used for the purpose of smurfing or to hide the real purpose of the transaction/the identity of the criminals.

##### **Case Example 5**

A person performed several times in the same week telegraphic transfers to country A. This person signed the transfers even when they were made under different names, since women were brought in by the person to open accounts using passports and identification documents from country A. The listed occupation of the customers was "receptionist", all in the same location.

#### ***Typology 5: Participation of a Second Person***

Several cases have been described, where a second person is involved in the performance of the transaction, mostly at the same time. The role of the second person is usually unclear but often, he or she seems to be in some kind of supervisory position (handing over money, giving instructions etc.). Below are three cases, which have been reported by Australia as possibly connected to human trafficking for sexual servitude, but not with a structuring scheme.

##### **Case Example 6**

A woman performed regular and multiple transactions at the same location, although not a customer of the banking institution. Telegraphic transfers for amounts around AUD 9,000 were obtained, and a second woman was used to authorise the transfer (by signature). The second woman appeared to be heavily reliant on advice and followed the instructions of the first woman.

##### **Case Example 7**

A person conducting transactions queried requirements for completion of documents, and obtaining of relevant information (including identification documents and contact details). A woman not conducting the transaction actually handed over money and left before the transaction was completed.

##### **Case Example 8**

A customer purchased telegraphic transfers to country A at a rate of 10 to 15 per month. A second person actually completed the transactions on behalf of the customer. In the majority of instances, the funds were described as "gifts".

#### ***Typology 6: Atypical Fund Transfers***

Below is an example of a major case which was identified in one country on the basis of suspicious transactions reported to the FIU. At the same time, the suspect was under investigation by another law enforcement agency in a second country. The size of the proceeds identified and ultimately confiscated appears to be the result of concentrated investigative work performed by agencies in different jurisdictions, good international cooperation on evidence gathering and asset tracing, and by painstaking monitoring of the suspect's activities.

### **Case Example 9**

A major alien smuggling and money laundering case in the Netherlands began with suspicious transaction reports concerning transactions at a local Hong Kong, China bank in which large amounts of money were deposited into accounts and immediately followed by outward remittances into a personal account in the Netherlands. Following the STRs (in 1999), the FIU launched an investigation into the account of Z., from which an address in the Netherlands was established. The Hong Kong, China FIU contacted the Netherlands National Police Agency for background enquiries and was told that the Agency had already started an investigation into Z.'s syndicate involving the smuggling of aliens. Z. was a kingpin in a dismantled alien smuggling organisation in the Netherlands. She coordinated with her accomplices for the purpose of smuggling mainland Chinese through Russia, Ukraine, Turkey and Slovakia into Western Europe. The final destinations were Canada, USA and Mexico.

The Hong Kong, China FIU identified five accounts held by Z., with a total amount of USD 283,000. The information was passed to overseas counterpart agencies. Throughout the period, the FIU continued to monitor the cash flows and the updated balance amounted to over 2 million Euro. To avoid suspicions, Z. appeared to use several bank accounts in various countries in her own name or in the name of facilitators to hide and launder the illegal proceeds. Funds were wire transferred to foreign accounts. The investigation by the Hong Kong, China FIU also revealed that Z. had also triggered 8 STRs for purchasing casino chips with both Dutch and foreign currencies (cash) in a state run casino. Z. was arrested in the Netherlands in June 2000 and convicted in October 2003. She was sentenced to 3 years and 6 months imprisonment. In January 2004, a Dutch court made a confiscation order for 8.7 million Euro, representing unlawful gains. Overseas police agencies also arrested several persons abroad and restrained assets, including real estate and accounts situated in foreign countries.

### ***Typology 7: Use of Underground Banking***

As is well known, underground banking operations are difficult to detect and trace because of their nature. The system implies the existence of a well organised network of correspondents and a high level of internal discipline and trust. The system is often found to be used by particular ethnic communities.

### **Case Example 10**

Immigration and Customs Enforcement (ICE) agents found that by posing as a smuggling organisation, they would have been able to charge a USD 35,000 transportation fee to smuggle each National from the People's Republic of China, located in Thailand, to New York. The criminal organisation often charges these individuals upwards of USD 85,000. The criminal organisation would receive payment for the smuggling before arrival of the Chinese nationals and pay the agents posing as the smuggling organisation. The remaining profit would then be kept in a system of underground banks, thus making the tracing of the profits extremely difficult. The profits would then be sent via wire transfer to Bangkok, Thailand or Hong Kong, China under a false name.

### ***Typology 8: Use of Businesses***

Businesses are associated in various ways with human trafficking and smuggling of migrant schemes. They can be used as facilitating or as money laundering devices, and sometimes as both. In other cases, they are fronts, with no or little activity corresponding to the one for which they are officially registered.

Well-documented cases on the use of businesses often reveal a variety of patterns concerning the transfer of funds, their accumulation, their conversion and investment.

It is difficult to identify common denominator as to the types of businesses used in these types of case. Often, the businesses are directly involved in cross border activity (travel agencies, money remitters etc.). But this is not always the case, and cash intensive business concerns regularly feature in the reported cases. It is thought that some of the profits from these offences is ploughed back into these businesses.

### **Case Example 11 – A restaurant**

Through investigative efforts it was revealed that a Chinese restaurant and two other Asian restaurants located in New Mexico were engaged in multiple violations of federal and state law. The violations included money laundering, harbouring illegal aliens, inducing illegal aliens to come to the United States, conspiracy, and multiple state charges related to labour law.

This investigation showed that, after being smuggled into the United States, the undocumented migrants would all live in the same house provided by their employers and work at their employers' restaurant six days a week for twelve hours a day, earning a substandard wage. This wage was used to repay smuggling debts that were incurred in both China and the United States. Some of the smuggled aliens borrowed money from a loan shark in China and would send their wages, via wire transfer, to China in order to repay the loan. The other smuggled aliens would use their wages to repay the owner of the restaurant, since he had paid the smuggling fees for the aliens. These fees ranged from USD 40,000 - 60,000. The US Immigration and Customs Enforcement (ICE) agents conducted surveillance and notified the Department of Labour of the investigation. By comparing the reports filed with the Department of Labour and the notes taken during surveillance ICE agents noticed that the businesses were only reporting 40% of their employees.

ICE executed 10 simultaneous search warrants. During the execution of the warrants ICE agents found 28 undocumented aliens. Additionally ICE discovered accounting ledgers, which identified approximately USD 2,000,000 in unreported proceeds. ICE agents found that the proceeds were being sent to China via money wire, mail, and body couriers. ICE seized two bank accounts worth USD 50,000 and 28,000 respectively. The Asset Identification and Removal Group is attempting to identify other real properties and assets owned by the group.

### **Case Example 12 – A money transmitting business**

The US Immigration and Customs Enforcement (ICE) offices within the Arizona corridor are investigating a criminal enterprise responsible for smuggling undocumented aliens (UDA's) into the United States and transferring of the illegal proceeds from the smuggling operation via money transmitters. A common practice that alien smuggling groups utilize in the Arizona corridor is to secure a small down payment from the smuggled migrants before they leave Mexico. Prior to crossing the border, the migrants must provide the smuggler a name and contact number for a relative or prospective employer in the United States who will guarantee the remainder of the smuggling fee and air fare to their final destination in the United States. After crossing the border the smuggled migrants are temporally staged in Phoenix or Tucson. From there the smugglers contact the guarantor who then sends, by wire, the remaining smuggling fee.

In this particular conspiracy, ICE agents learned that the alien smuggling family operated their own unlicensed money transmitting business to further conceal their illegal activities. The investigation is focusing on violations of alien smuggling, conspiracy to commit alien smuggling, and money laundering.

On April 19, 2003, special agents assigned to an Asset Identification and Removal Group seized an un-liquidated investment account belonging to the family. The un-liquidated investment account was valued at USD 219,000.

### **Case Example 13 – Travel agencies**

The investigation was initiated as part of a wide ranging initiative targeting human smuggling organisations operating in and around the Los Angeles International Airport. Through intelligence acquired during this initiative and extensive financial research, Immigration and Customs Enforcement (ICE) agents initiated a human smuggling/financial investigation into criminal smuggling organisations. These organisations own and operate travel agencies which are used as fronts to facilitate the movement of smuggled migrants from the southwest border to Los Angeles, California and on to various locations throughout the United States. These travel agencies provide staging areas, plane tickets and fraudulent identification for migrants being smuggled by the organisation.

The criminal organisations generate huge profits from their smuggling operations, which are laundered (including investment in the travel agency). For the period January 2003 through July 2004, ICE has identified 13,857 transactions through a particular money remittance network, totalling more than USD 27,000,000.

On November 4, 2004, ICE agents and CBP/Border Patrol executed six Federal search warrants within the Los Angeles area. Five of the search warrants were executed at travel agencies identified as having facilitated human smuggling and money laundering activities. A sixth warrant was served at a residence belonging to a targeted individual who has been linked to the criminal organisation. In addition to the search warrants, twenty-six bank accounts belonging to the targets of the investigation were frozen.

### **Case Example 14 – Landscaping companies**

A human smuggling and trafficking investigation revealed that a criminal organisation was responsible for smuggling Ecuadorian nationals into the United States. Once in the United States the undocumented aliens were forced to live in communal housing supplied by the smugglers. The aliens were also forced to work for landscaping companies chosen by the smugglers. As the aliens were paid for their work the smuggling organisation would take their checks and deposit them into an account owned by the smuggling organisation.

The organisation would then subtract money due to the aliens from their checks for housing, at an overpriced rate, and smuggling fees. The organisation would only return approximately 20% of the money to the aliens. The organisation then used the money to buy real estate in the United States and in Mexico. On occasion the smuggling organisation would send money to Mexico via one money remittance network in particular. The organisation also deposited checks directly into legitimate bank accounts set up in Mexico.

### **Case Example 15 – A law firm and fraudulent asylum requests**

In the New York area a legitimate law firm aided Chinese smugglers by using their law firm to fraudulently create asylum requests for use at CIS. In a period of time, over 1,000 Nationals of the People's Republic of China were smuggled into the United States. The law firm would charge between USD 40,000 and 50,000 per asylum request. Further, the law firm also filed false income tax returns and paid their employees in cash thereby avoiding all withholdings. Approximately USD 5 million was seized constituting the proceeds of the smuggling scheme. The proceeds were represented in both real property and currency.

### ***Typology 9: Investment in Real Estate***

Investment in real estate is another frequently reported method of converting proceeds from human trafficking and smuggling of migrants. Although the case beneath does not constitute an example of money laundering detected on the occasion of the purchase of real estate (the investigation was triggered by the reporting of transactions by financial institutions), it shows how relatives can be used in such a context, as intermediaries.

### Case Example 16

The Slovenian FIU has worked on a case which involved a Slovenian citizen, who was the leading member of an organised criminal association dealing with smuggling of illegal refugees, mostly Turkish, Albanian, Macedonian and Iranian citizens, to the West. In the years 1998 to 2003, this Slovenian citizen received 81 money orders from 14 different individuals from the USA, 'the former Yugoslav Republic of Macedonia', Italy and Germany for a total amount of 40,000,000 Slovene *tolars*. In connection with this transaction, the FIU had reason to believe that the money derived from the organisation of illegal migration or from the participation of the suspect in the group for the organisation of illegal migration. The biggest share of money was remitted to Slovenia from the USA in the amount of 31,000,000 Slovene *tolars* or 77% of all money orders in the amount of 40,000,000 Slovene *tolars*. The main portion of this money remained in Slovenia and was thought to be used for investment into real estate and was also distributed among other members of the criminal association. In the year 2000 the suspect's wife, who has not filed an income tax statement for that year, used 14,000,000 Slovene *tolars* to buy real estate. The FIU also found out that both the suspect and his wife had made transactions representing several times their official income (as filed in their income tax statements during the years 1998 to 2003). The suspect was finally convicted in 2003, in connection with the amount of 40,000,000 Slovene *tolars*, for organisation of illegal migration. The case has shown the following patterns:

- very high fees were paid for the money transfers which could have been executed at much lower costs; such economically illogical transactions are - as a rule, thought to be connected with money laundering;
- the monies spent by the suspect's wife to buy real estate in the amount of 14,000,000 Slovene *tolars*, did not originate from her own income, but was handed to her by her husband, who received it for organising illegal migration. In the real estate purchase contract, the buyer is the suspect's wife, with the purpose of concealing the source and the real beneficiary of the dirty money.

### ***Typology 10: "Back-to-back" Loans***

So-called "back to back" loans are not, so far as has been established in this research, a frequently used money laundering technique in relation to the offences studied. The case below, which is an illustration of this technique, is reported here for the sake of completeness and for its comparative novelty as a money laundering technique.

### Case Example 17

In the year 2000, the Slovenian FIU forwarded to the Criminal Police Directorate a suspicious transaction report connected with the organised perpetration of illegal migration. The FIU had found that the main organiser laundered his proceeds by using the banking system. Even though the suspect had not filed any income tax statements to the Tax Authority since 1995, the FIU found more than DEM 1,400,000 of money orders received in different currencies and from which a suspicion was raised that they derived from the smuggling of immigrants.

To hide the source of the money, the suspect used a money laundering technique known as a "back to back loan". In the year 1999, the suspect took a loan from a Slovene bank, for an amount of DEM 200,000 with a repayment term of one year. The loan was secured in a way that he restricted the use of his illegally gained money for a year in the form of a term deposit<sup>22</sup> in the amount of DEM 215,000 at the same bank. The suspect concluded his loan agreement without any real sound economic reasons; his term deposit was much bigger than the actual loan; the interest rate for the term deposit was 2.94%, and the interest for the loan was 5.8%, which caused additional loss to the suspect. In the early stage of his loan arrangement the suspect regularly repaid the loan, but at the end of one year when his term deposit became a normal demand deposit, he repaid the main part of his outstanding loan liabilities. Even though some interest accrued on his term deposit, he still suffered a loss in the amount of 1,200,000 Slovene *tolars*. With an economically illogical transaction, the suspect managed to launder DEM 200,000 of dirty money.

<sup>22</sup>A "term deposit" is a deposit where the money cannot be used by the customer for a certain period of time, for which the customer usually receives a higher interest rate than for a normal demand deposit.

## CONCLUSIONS

We are conscious that in the time available, our research has only begun to scratch the surface of these issues. Nonetheless, we can draw some tentative conclusions:

While we have not detected any very significant differences in the typologies of money laundering in respect of offences of human trafficking and illegal migration, there are differences in the money flows associated with these offences. These need careful analysis and investigation back to the country of origin if the laundering offences are always to be successfully detected in respect of these predicates. In the course of analysing these money flows, it is necessary to identify and separate out which are payments/fees or other sums which may be evidence of the substantive offences, as opposed to money flows which represent the laundering of criminal proceeds. As noted earlier, both sums may be confiscatable in due course either as instrumentalities or as proceeds.

Though the STR reporting system generates some inquiries, trafficking in human beings and illegal migration remains primarily a law enforcement issue. The background of those country experts who participated in the workshop supports this.

It was underlined that the exchange of information and cooperation between authorities (including trans-/internationally due to the *cross border nature* of the crimes considered) is very important to ascertain the complex nature of trafficking and smuggling schemes. Likewise, raising awareness of the importance of financial investigation as part of the investigation of the crime remains crucial. As indicated earlier, not all countries have as yet information on the laundering techniques used in this field, although our research shows that, to a large extent, they are similar to those used in relation to other cash generating predicate offences, for instance drug trafficking.

It was clear from our discussions that there is a general need to enhance awareness – at least at local level - about the nature of trafficking in human beings and smuggling of migrants. Local police may not always realise the implications of cases they are handling. It was noted that local police sometimes process cases of prostitution or living off immoral earnings without considering whether the offences they are dealing with are also part of a larger human trafficking organisation.

It was also underlined that the investigation of these serious crimes needs to be supported by the use of special investigative means. Further, it was noted, as indicated earlier, that the financial investigation (targeting proceeds) needs to be conducted in parallel with the main investigation of the predicate offence in order to:

- Trace the monies with a view to seizure and confiscation;
- Help identify the criminal networks and the kingpins so that not only those lower down the command structures of such networks are targeted; and – *most importantly*
- Help substantiate a case of human trafficking and smuggling of migrants since the evidence of payments/financial benefits is a prerequisite for obtaining a conviction in such cases.

Unfortunately, the importance of such investigations is not yet universally acknowledged. In some countries, law enforcement agencies routinely conduct financial investigations into the financial aspects of organised human trafficking and illegal migration. However, in some Central and Eastern European countries, where confiscation of proceeds, as widely interpreted in the international instruments, is still not in place traffickers appear able to retain most of their profits with impunity. The time available did not allow our project to investigate whether, when there are convictions for human trafficking/illegal migration, reverse onus provisions are being applied regarding the lawful origin of alleged proceeds. Neither was there time to explore other successful non-criminal repressive strategies – e.g., taxation, non-criminal asset forfeiture. Another important issue that might be discussed further in the future concerns what exactly can be forfeited/confiscated as instrumentalities,

bearing in mind the particularities of the crimes considered (e.g., parts of a legal business which has been used to facilitate the entry/stay of illegal immigrants, means of transport used, etc.).

Turning to actual investigations and prosecutions, we noted that money laundering cases can actually be prosecuted where illegal migration or human trafficking are underlying predicate offences to money laundering. A round table of the participants revealed, encouragingly, that money laundering cases, on the basis of these predicates, had either been successfully prosecuted or were being brought in the following jurisdictions: Belgium; Bulgaria; Hungary; Luxemburg; Slovakia; Slovenia; Italy; United Kingdom; United States; Hong Kong, China; and Russia. That said, it is acknowledged that money laundering in relation to smuggling of migrants and human trafficking is not easy to detect and prosecute. Reasons for this include:

- The fact that payments are almost exclusively made in cash.
- Payments are often made outside the countries where the smuggling and trafficking crimes are likely to be detected (transit and destination countries).
- Amounts paid are often small (because of individual payments or fragmentation to circumvent the reporting threshold).
- Transfers are done through means which are difficult to control: underground banking, money transfer services such as those offered through certain money remittance networks, body carriers etc.
- Lack of criminalisation of self-laundering. Among the countries represented in the workshop, there was only one state where this applied and legislation was being amended to cover this.
- Smugglers and traffickers adapt their working methods to avoid detection.

The issue of the cooperation of victims with investigations and prosecutions in these cases was not discussed in depth. However, it was noted that some investigations were triggered by “escaped” victims. Most countries treat victims as valuable intelligence rather than as potential witnesses. In most countries, it is considered that victims of trafficking are usually unwilling to testify or provide information because of fears of retaliation against them or their relatives. Most countries also appear to lack adequate incentives, protection and psychological support measures for victims such as to encourage their active use in actual cases.

The issue of money transfer services (such as those offered by certain money remittance networks) appears to be particularly crucial in the context of combating money laundering of proceeds from human trafficking and (organised) illegal migration. Tighter regulations of these services need to be seriously considered by those countries particularly affected by these offences. It is especially important that the authorities have an overview of who can or does provide such services and who supervises the sectors concerned. The United States in particular had taken successful defensive measures in connection with money transmission services<sup>23</sup>.

---

<sup>23</sup> According to the experience of the United States, damming warrants are a useful tool. Damming warrants allow for the blocking of funds wired to an individual described in the warrant for a specific period of time. When the smuggler targeted in the warrant attempts to collect the funds, the Non-Bank Money Transmitters (NBMT) refers the smuggler to a customer service number, which is monitored and staffed by ICE Agents. Those agents will then determine if the funds are criminal or legitimate proceeds. If the funds are determined to be criminal proceeds, the recipient is notified that the funds were seized by law enforcement. If the transaction is found to be legitimate, the funds will be released. The subjects of damming warrants are members of criminal organisations. The parameters include inbound amounts in the range and increments of USD 1,500, correlating to fees associated with smuggling an alien from Mexico into the United States. By filtering and analyzing

The immediate implementation of FATF Special Recommendation VI on alternative remittance and Special Recommendation VII on wire transfers, both of which also cover money laundering, needs to be addressed by countries implicated in human trafficking and illegal migration. The major issues in this context are:

- The variable identification requirements ranging from a customer's ID check to the absence of identification (in some cases, only the code was used to ascertain the legitimate recipient).
- A number of them operate illegally, and are not subject to adequate supervision, or no supervision at all (this could be the case of money remittance services offered by businesses which are not traditionally obligated entities under money laundering legislation – e.g., travel agencies).
- When the service is connected with another form of legal business, it offers a powerful tool for both transferring and laundering proceeds via integration in the business' activity.
- The introduction of the single currency in Europe has resulted in foreign exchange operators diversifying their services and providing money transfer services leading to a proliferation of operators in this area; the multiplication of such services appears to have led to increased competition among them and to some greater laxity as regards customer identification.

It appeared from our work, that the use of cash couriers (particularly bulk carriers) is another crucial issue to be addressed in coherent national policies aimed at combating these crimes. In this context, the immediate implementation of special recommendation IX on cash couriers (which also applies to money laundering) should be urgently considered by those countries which are affected by these offences.

If countries are to make real progress against human trafficking and illegal migration, the removal of the profit from these crimes, through dissuasive confiscation orders, appears to be important in the development of national strategies. This supposes, to a large extent, that the proceeds are secured at an early stage of the (financial) investigation through temporary measures. In most jurisdictions, dissuasive confiscation orders turn on the recognition of the relevant offence as especially serious.

In this context, it is considered that jurisdictions should recognise that human trafficking and smuggling of migrants are serious offences which should be capable of attracting significant confiscation orders after conviction. Because of the difficulties in assessing the amount of proceeds generated by the offences being considered – this is particularly true for human trafficking and the forced labour which goes with it – measures could be considered at the national level, to the extent that they are consistent with the principles of domestic law, to require that in respect of these serious offences, after conviction, an offender demonstrates the origin of proceeds or property said to be liable to confiscation.

### **ISSUES FOR CONSIDERATION**

Though there is clearly much more research that could be undertaken on the subject, on a number of the issues raised in the discussions (and touched on in this report), the working group felt that no further studies needed to be undertaken by it, at this stage, in the specific context of typologies.

The issues for consideration formulated by the working group therefore flow from the conclusions set out above. They apply to countries generally, but are of particular relevance to those (origin, transit and destination) countries which are known to be affected by these crimes in all their different stages.

---

transactions, ICE has been able to associate transactions correlating to "buy-out" fees from sponsors, destined for California-based money couriers representing several human smuggling organisations.



The first two considerations relate to the urgent need for implementation of Special Recommendations VI, VII and IX. Though they were introduced in the context of terrorist financing, they also explicitly cover money laundering, and the working group considered that greater awareness-raising on these aspects in all countries was required, especially in respect of financial aspects of human trafficking and illegal migration.

- **Rapid implementation of Special Recommendation VI on alternative remittance and Special Recommendation VII on wire transfers in the context of money laundering (and in particular the predicate offences of human trafficking and illegal migration).** Given the importance of money remittance services in these offences, and the risks involved for countries affected by these crimes, states should consider ways in which controls over money remitters could be tightened. In particular, countries should have a clear overview of all agencies offering these services and consider the feasibility of closer direct supervision of them in order to ensure that Special Recommendations VI and VII are fully observed.
- **Rapid implementation of the new Special Recommendation IX on cash couriers in the context of money laundering.** Special attention should be given to this by countries affected by trafficking in human beings and illegal migration.

The following two considerations are identified in the light of other concerns raised within the project team:

- **As many criminals launder their own proceeds in these offences, the incrimination of self laundering in those countries involved in trafficking in human beings and illegal migration (where self laundering is not currently criminalised) should be actively considered.**
- **In order better to target kingpins in human trafficking and illegal migration in those countries particularly involved in these offences, consideration could be given to measures which require offenders, upon conviction for these offences, to demonstrate the origin of alleged proceeds or other property liable to confiscation to the extent that such a requirement is consistent with the principles of its domestic law.**

**Questionnaire Used for the Preparation of  
Workshop on Money Laundering Methods Associated with  
Human Being Trafficking and Illegal Migration**

1. Has your jurisdiction detected instances of organised trafficking in human beings / illegal migration? If so, what were the main characteristics of *financial operations* associated with such cases (for example, jurisdictions involved, funds paid by migrants, profits derived by traffickers, etc.)? Please provide case examples if possible.
2. To what extent has your jurisdiction conducted investigations into the *financial aspects* of organised human being trafficking and illegal immigration? If such investigations have occurred, what money laundering techniques were detected? What were the obstacles to conducting such investigations? Was it possible to confiscate the proceeds involved? If confiscation was not possible, what were the impediments to taking such action?
3. What patterns have you identified in the use of particular money transfer or payment methods as related to facilitating human being trafficking or providing illegal immigration “services”?
4. What indicators have you observed in relation to money laundering associated with human being trafficking and illegal migration?

What law enforcement agencies or other government authorities are directly involved in detecting and investigating cases of human being trafficking and illegal immigration? What obstacles exist to sharing intelligence or information among these authorities?

## CHAPTER IV

### **MONEY LAUNDERING & TERRORIST FINANCING TRENDS AND INDICATORS: INITIAL PERSPECTIVES**

Attempting to describe current and emerging money laundering trends has been one of the principal goals of the FATF typologies effort since the beginnings of the Task Force in the first years of the 1990s. The early emphasis on cases studies and more recent focus on a thematic approach in examining typologies helped the FATF to build up a significant expertise in the methods used for money laundering. This emphasis on the methods – the “how-to” – of money laundering and terrorist financing has however meant less emphasis on identifying new or potential ML/TF trends in an accurate and consistent manner. While the importance of studying ML/TF methods and techniques cannot be overstated – such studies provide decision makers and operational experts with the material toward which to target policies and strategies for combating financial crime – the “how-to” of ML/TF is only part of the picture.

Understanding the evolution and prevalence over time of particular ML/TF methods — the current and emerging trends — provides the rest of the picture. The study of known or perceived trends enables the development and refinement of indicators that law enforcement and supervisory authorities and especially the private sector can use to help detect specific ML/TF activity. Identifying trends ensures that, in the longer term, the relevant ML/TF methods are themselves examined in a systematic manner and understood and acted on with reference to their context. It is this extra context that also allows the identification of further links between apparently different ML/TF methods. The experience gained through past FATF typologies work has shown that individual topics (or now projects) often identify similar or overlapping ML/TF methods. In this year’s exercise, we can cite as an example alternative remittance systems that, besides being the subject of a specific project also appeared as a factor in some human being trafficking operations, another of this year’s topics. The typologies process should ensure that value is added by linking together these common methods or techniques and make sure our understanding is complete. It is through looking at such activity over time that emerging methods or trends may be identified and potential new areas of vulnerability can be addressed.

The FATF decided to place additional emphasis within its overall typologies effort to identify and describe ML/TF trends at the international level and on a systematic basis. A dedicated project team would carry out this work, which would be based on ML/TF activity detected by national AML/CFT authorities and international organisations. Initially, the project would have as one of its objectives to develop basic indicators related to identified trends. As the initiative matures, the project will be able to start judging the extent to which ML/TF methods and techniques occur and ultimately the importance of particular trends over time. The results of this work could then possibly provide policy makers at national and international levels with additional useful information for prioritising the development of relevant AML/CFT measures.

The Methods and Trends Project Team began its work in 2004 by attempting to develop an inventory of known ML/TF methods and techniques. The basic sources creating this inventory were to include already existing FATF typologies material (including annual typologies reports and written submissions provided by countries during the yearly typologies exercises), finished typologies reports prepared by national and international authorities, national indicator lists developed to aid financial institutions in detecting and reporting ML/TF activities, etc. The use of a broad range of sources was intended to ensure that the methods inventoried would not only include ML/TF activity detected through AML/CFT reporting systems. Upon completion of the inventory, the Methods and Trends Project Team would turn to development of a “methodology” that could provide a system for further analysing these techniques.

Very quickly it became clear that the Project Team needed first to build a common analytical framework in order to create an inventory of ML/TF methods. Such a framework was necessary given the diversity of potential sources of information and differing national approaches to analysis of ML/TF phenomena. The Team thus used the workshop held during joint meeting of ML/TF experts in Moscow on 6-8 December 2005 to focus its efforts on agreeing basic concepts and initial common approaches to the analysis of ML/TF activities.

### Defining basic concepts

The Moscow workshop provided the opportunity to define key terms and concepts relating to analysis of ML/TF activities. Participants in the workshop provided most of the input on these definitions; however, it was also clear that participants were agreeing to “working definitions” that would likely be modified and further refined as the work of the Project Team progresses. From these working definitions, a first and very preliminary analytical approach for ML/TF methods and trends would develop, which in turn would be subject to further modification.

In the first group of terms, the workshop / project team concentrated on concepts relating to methods and trends.

- *Method*: In the ML/TF context, a *method* is a particular procedure for carrying out ML or TF activity. It was felt useful to consider further distinctions in the concept of ML/TF method:
- *Technique*: A ML or TF *technique* is a particular action or way that the ML or TF activity is carried out. *Techniques* in the ML/TF context could include, for example, depositing funds into a bank account, transmission of funds by international wire transfer, exchanging funds in one currency for another, purchasing a cashier’s cheque, over- and under-invoicing as part of an import/export transaction.
- *Mechanism*: A ML or TF *mechanism* is a system or thing that carries out part of the ML or TF process. Examples of ML or TF *mechanisms* might include a financial institution, a money remitter, an Internet casino, a legal entity or arrangement (used as a cover for illegal activity or established for the purpose of hiding ownership or control), etc.
- *Instrument*: A ML or TF *instrument* is an object of value (or representing value) that is somehow used in the ML or TF process. Examples of ML/TF *instruments* include cash funds, cheques, travellers’ cheques, letters of credit, precious stones, real estate, securities, etc.

There is a certain amount of overlap between these last three concepts. For example, the action of depositing funds into a bank account relates to all three concepts: (1) depositing funds is a *technique*, (2) the financial institution managing the account is a *mechanism* and (3) the funds deposited are an *instrument*. It should be noted as well that, for the most part, the examples provided for each of these concepts may not in and of themselves illegal activities.<sup>24</sup> Indeed, it is only when these *techniques*, *mechanisms* and *instruments* are put together to form a ML or TF operation that they may become illegal.

- *Scheme*: A ML or TF *scheme* is the particular ML/TF process that combines various methods (*techniques*, *mechanisms* and *instruments*) into a unique operation. In some instances, such *schemes* are described as *cases*, since an individual investigation or case may uncover a unique scheme. However, using the latter term tends to confuse the concept with investigative case;

---

<sup>24</sup>Some examples of techniques, mechanisms and instruments that could be considered inherently illegal include structuring or smurfing to avoid reporting requirements or bribing a bank employee not to undertake usual AML obligations (*techniques*), use of an unlicensed money remitter where such use is illegal (*mechanism*) and third-party (endorsed) cheques used as means of payment when such use is illegal (*instrument*).

often *schemes* are not detected through investigations alone, and investigations can uncover more than one ML/TF scheme.

- *Typology*: When a series of ML or TF schemes appear to be constructed in a similar fashion or using the same or similar methods, then similar scheme can be classified as a *typology*. It is from the study of ML/TF typologies then that experts can detect the weaknesses that will allow appropriate counter-measures to be developed. Furthermore, a typology, when well-understood, will provide some indication of particular weak points in already existing AML/CFT measures.

### **Defining a *Trend***

It is also important to differentiate clearly between ML/TF *trends* and from ML/TF *methods* and *typologies*. While a *method* or *typology* still refers to unique processes at a particular point or period in time, a *trend* could be considered the evolution of a *method* or *typology* over time. For this reason, in trying to identify and describe ML/TF trends, experts must take into account the temporal aspect (frequency and repetition) and geographic aspect (pervasiveness), as well as the transformation over time of individual methods and typologies.

In practically all areas, defining and then describing a trend is often difficult. In the ML/TF area, there are particular difficulties in trying to identify trends because of the illegal or clandestine nature of such activity. ML/TF activity cannot be observed through easily available information or statistics. To determine a trend, the analyst must rely on what are often indirect indicators. Some examples of information that can be used includes:

- “Intelligence” provided by law enforcement agencies, FIUs and other competent authorities
- Law enforcement investigations
- Criminal prosecutions / convictions / attachments and confiscation orders

The difficulties in using these sources of information to identify or confirm a ML/TF trend is that it does not provide a complete picture of the situation. For example, the number of prosecutions or convictions in a particular location may indicate a high (or low) concentration of ML activity. However, high numbers of prosecutions – taken out of context – could represent a single large-scale case with a number of persons involved in the same operation rather than a high concentration of activity overall. A small number of convictions – again, taken out of context – could mean not that there is a low concentration of ML activity but that there are perhaps other factors that limit the numbers of prosecutions under the ML offence (for example, the predicate or ancillary ML offence is easier to prove).

### **First step on developing an analytical approach: Determining categories / classifications**

After creating a series of working definitions for relevant basic concepts, the Moscow workshop turned to laying the groundwork for a common approach to typologies analysis generally and to the identification of ML/TF trends in particular. One of the basic elements of any analysis is the process of classification. In the case of ML/TF, some of the concepts defined above – *technique*, *mechanism*, *instrument* and *typology* – can already be used for classifying the various activities described in ML/TF case examples. Besides these categories, however, there are a number of others ways in which ML/TF activity can be classified. For example:

- *By ML/TF stage*: For money laundering, these stages include *placement*, *layering* and *integration*. For terrorist financing, the stages include *collection*, *transmission/dissimulation* and *use*. Examples of techniques at the placement stage might include conversion of one currency for another or structuring of cash deposits. An example of methods relevant to the layering and/or transmission stages might include the use of wire transfers or money remittance systems.

- *By predicate or other related offence:* Certain ML activity may be more closely related to specific predicate offences. For example, in some jurisdictions, structuring or smurfing was traditionally associated with narcotics trafficking. The ML activity associated with certain types of large-scale frauds may be particularly associated with the use of shell companies or banks.
- *By country or region:* Some types of ML/TF activity may be associated with specific countries or regions. For example, the nature and degree of misuse of alternative remittance systems is linked to some countries or regions more than others.
- *By financial or other sector involved:* Specific ML/TF methods are associated with certain sectors of the economy. Structuring or smurfing is generally associated with the banking sector, for example.
- *By development stage of the financial market:* The ML/TF methods that might be used in a highly developed financial sector will differ from those used in a cash-based economy, for example.
- *By weak point or vulnerability in the AML/CFT system:* Bureaux de change might be exploited for ML/TF purposes in a particular jurisdiction because they fall outside of that jurisdiction's regulatory regime. Trusts or other legal arrangements are often used in schemes that attempt to take advantage of differences between jurisdictions that have or do not have them.

None of these ways of classifying ML/TF methods could be considered individually as an analytical method; rather, categorising such activity in these ways can serve as the first step in identifying common elements that could in turn help in the detection of patterns or eventually in the development of relevant indicators. As an initial step in building on these basic analytical processes, the Moscow workshop proposed that a few potential methods / trends would be looked at informally using the simple methods of categorisation indicated above. This would serve to test the utility of classifying and, it is hoped, help provide additional analytical procedures that could also be useful in examining ML/TF subjects.

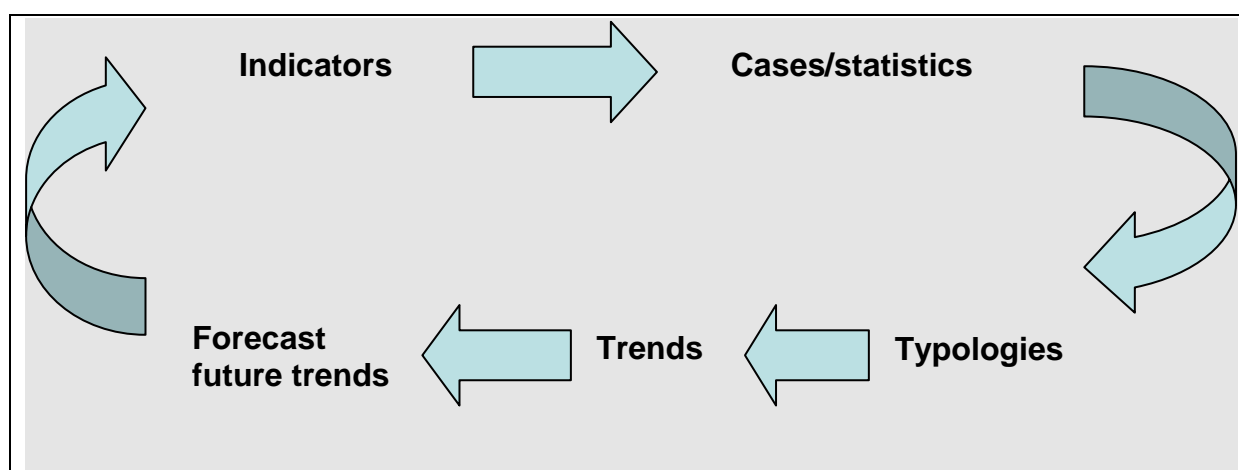
## **ML/TF Indicators**

Looking forward to ways that the project team on methods and trends could eventually develop ML/TF indicators, the Moscow workshop focussed again on defining basic concepts. The term *indicator* itself initially posed some problem, as there is sometimes confusion between a ML/TF indicator and a ML/TF method. While it is sometimes true that the methods defined earlier in this chapter could indicate ML or TF activity, they are not synonymous. For example, exchanging one currency for another is not by itself and indicator of ML. By the same token, indicators are not all necessarily ML/TF methods.

The concept of indicator also presents a few other problems. For example, specific indicators might point the way toward a particular ML/TF methods or typologies; however, it is from the study of these methods and typologies that indicators are ultimately derived. Indicators can thus have different roles depending on who is working with them.

When developed from concrete examples, indicators help in detecting ML/TF activity. As such they are a necessary tool for financial institutions, other financial intermediaries and gatekeepers who are on the front line in confronting activities that may or may not be suspicious (and thus may or may not be related in some way to money laundering, terrorist financing or some other financial crime). For the private sector, valid ML/TF indicators are therefore essential in establishing and "calibrating" mechanisms that help to identify suspicious or unusual transactions which must then be reported to a financial intelligence unit.

For law enforcement and other investigative authorities, ML/TF indicators can also play a role. Indicators viewed along with other information may help such authorities to detect specific types of criminal offences or may otherwise help in orienting a particular ML/TF investigation. If we take into account that indicators can be derived from analysis of concrete cases, it becomes apparent that indicators are part of a continuous process that can start and finish with indicators. The Moscow workshop discussed this process – usually described in more general terms as the “intelligence cycle” – and noted that it is particularly useful for explaining how ML/TF indicators can start the process and at the same time be one of the ultimate products.



*Figure 1: The “Intelligence Cycle” adapted to ML/TF analysis Source: FATF*

## Conclusion and Next Steps

The study of ML/TF trends in an accurate and systematic manner is becoming ever more essential in order to acquire a fuller understanding of the vulnerabilities of the financial system to exploitation by criminals and terrorists. To acquire this “whole picture” of ML/TF, it is necessary to go beyond the “how-to” of this activity and attempt to determine the larger context in which such activity occurs – the current and emerging ML/TF trends. The FATF has with the establishment of its project on ML/TF methods and trends taken the first steps in developing analytical processes that will lead to the identification of credible and relevant ML/TF trends. The resulting processes, which will take time to develop fully, should also be useful for the analytical component of research undertaken as part of other typologies projects. This work should also result in the development of both generic and specific ML/TF indicators that could be used by the private sector (financial institutions and other intermediaries), law enforcement and other investigative authorities.

From the start, this work is viewed as a long-term initiative. The project is intended to develop processes that will necessarily be tested and then improve as experience increases and as the FATF acquires more information on ML/TF methods from a broader range of sources. Working more closely, for example, with the various FATF-style regional bodies, the Egmont Group and other international partners is likely to prove a valuable source of information as well as providing a key forum for dialogue on emerging trends. The methods and trends project could also play a role in initial development of certain typologies topics before they are assigned to individual project groups.