FATF

FATF REPORT

THE ROLE OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS IN MONEY LAUNDERING AND TERRORIST FINANCING

October 2013

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

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

www.fatf-gafi.org

TABLE OF CONTENTS

ACRONYMS

AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
CDD	Customer Due Diligence
CFT	Combatting the financing of terrorism
DNFBP	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HOSSP	Hawala and Other Similar Service Provider
MLA	Mutual Legal Assistance
MSB	Money Service Business
MSOs	Money Service Operators
MVTS	Money or Value Transfer Services
STR	Suspicious Transaction Report

EXECUTIVE SUMMARY

Twelve years after September 11th and the adoption of Special Recommendation VI on Alternative Remittance Systems, two often competing and conflicting views on *hawala* still stand. Many countries and communities, as well as the development community, view them as essential providers of financial services to the unbanked in countries with limited financial access. In significant numbers of jurisdictions and sometimes in the same jurisdiction, law enforcement views them as one of the leading channels for terrorist financing and money laundering.

Against this background, this typology seeks to demystify *hawala* and similar service providers. It seeks to provide a facts-based review of the extent of their vulnerability, as of today, to money laundering and terrorist financing. To this end, the typology project team sought input from members of the FATF and FATF-style regional bodies. The team received feed-back from 33 countries to a survey it had developed.

The term *hawala* is used in a number of jurisdictions and is associated with a money transfer mechanism that operated extensively in South Asia many centuries ago, and which still exists there, as well in the Middle East, and in Africa. In others countries, it has several different connotations in particular illegal money transmitter and in others, the term *hawala* is neither used nor understood, however, the service of remitting money may be covered by the country's legislative framework.

Hawala in fact is not a universal term. Still, there appears to be a universal recognition of the existence of *hawala* or *hawala*-like providers across jurisdictions, in so far as they present unique characteristics, focused on their settlement mechanisms. Recognizing this, this typology uses a broader term than *hawala* and instead focuses on "*hawala* and other similar service providers" or HOSSPs.

HOSSPs, for the purpose of the typology, are defined as money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. Some HOSSPs have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *underground banking*. While they often use banking channels to settle between receiving and pay-out agents, what makes them distinct from other money transmitters is their use of non-bank settlement methods, including settlement via trade and cash, as well as prolonged settlement time. There is also a general agreement as to what they are not: global money transfer networks (including agents) operated by large multinational money transmitters and money transfers carried out through new payment methods including mobile money remittance services. This description is based on *services* provided by them and *not their legal status*.

HOSSPs are used in some jurisdictions by legitimate customers for reasons of geography, culture, and lack of banking access. They are also used by individuals and entities seeking to evade currency controls, tax obligations, and sanctions. HOSSPs generally are cash-in and cash out businesses that primarily send personal remittances of low value. They generally operate in areas with a high percentage of expatriate workers and are visible to members of that community. They often run businesses other than money transfer, particularly currency exchange.

This typology reviews three major types of HOSSPs: pure traditional (legitimate) ones; hybrid traditional (often unwitting) ones; and criminal (complicit) ones. Distinct ML/FT risks apply to each. Pure traditional HOSSPs tend to be popular because of familial, regional or tribal affiliation and inadequate access to regulated financial services for senders/recipients in origin/receiver countries. Hybrid traditional HOSSPs also serve legitimate customers, but at the same time are used, wittingly or not, for illegitimate purposes to transfer funds cross-border. Criminal HOSSPs, on the other hand, are set up or expanded to service criminals.

Surveyed countries gave a number of reasons for the continued existence of HOSSPs, including their competitive pricing, faster money transmission, cultural preference, lack of banking access, low confidence in the banking system, as well as deliberate transfer or concealment of criminal proceeds and evasion of currency controls, sanctions, and taxes. At the same time, the typology highlights that many of the assumptions on HOSSPs are outdated. For instance, they, in some jurisdictions, offer services well beyond money transmission. More universally, they often have detailed records; are not necessarily based upon trust; often are highly visible to the community they serve; and are not always high risk. Further, they ultimately often settle through banks, meaning that banks that have been provided with high risk indicators by their authorities are positioned to identify suspicious activities and notify their authorities accordingly.

The typology explains the different settlement mechanisms used by HOSSPs, including simple reverse transactions, triangular settlement, settlement through value, and the use of cash couriers. It provides country-specific examples, as well outlines their communication techniques that in some cases permit the instant availability of funds. It finds that most countries cannot provide estimates on the scale of unregulated HOSSPs or their relative threat.

As always the case when criminals own or control financial intermediaries, criminal HOSSPs deserve particular attention. Although a limited number of case studies were provided to the project team, there are several reasons why HOSSPs continue to pose a money laundering and terrorist financing vulnerability. These include a lack of supervisory will or resources; settlement across multiple jurisdictions through value or cash outside of the banking system in some cases; the use of businesses that are not regulated financial institutions; the use of net settlement and the commingling of licit and illicit proceeds. While the settlement through value or trade that masks the individual fund transfers is a source of vulnerability, the most significant reason for concern is lack of supervisory resources and commitment to effective regulation.

Out of the cases gathered for this typology, a picture emerges of common elements used by *criminal* HOSSPs, including control by a professional third party money launderer called a controller or money broker, depending upon the jurisdiction. Based upon existing case studies, it appears that HOSSPs can also be abused or used for import and export fraud, to launder drug proceeds, and to evade sanctions.

Similarly, the typology's case studies provide examples of terrorists still using HOSSPs to move funds twelve years after 9/11. They are used for reasons of familiarity, culture, extensive international reach, speed of transfers, and often lax supervision or lack of political will. The latter factors make it more likely that these institutions may lack robust AML/CFT controls, making them attractive to criminals and terrorist financiers.

A slight majority of surveyed countries bar HOSSPs from operating legally. Those that allow them to operate legally, provided they license/register with the relevant authorities and comply with relevant AML/CFT and other laws, largely believe that legalization of HOSSPs helped expand remittances through legal channels. However, in most jurisdictions that allow HOSSPs to operate legally, relatively few HOSSPs have actually registered or become licensed, with a few notable exceptions.

Effective supervision of HOSSPs is one of the primary challenges facing regulators and their governments. Most countries do not appear to have separate examiner teams for HOSSPs. While most have criminal, civil, and, to a lesser extent, administrative sanctions available for violations of AML/CFT obligations, many countries do not appear to have used these sanctions. Few countries require that money transmitters, including legal HOSSPs, should only partner with money transmitters in pay-out countries that are legally licensed or registered. The absence of requirements on foreign counterparties may be a critical vulnerability posed by money transmitters, including HOSSPs and further consideration of the application of Recommendation 13 in the context of money transmitters offering cross-border may be beneficial. Similarly, the absence of more than a handful of case studies involving international cooperation suggests that further discussion is warranted on how law enforcement or other competent authorities can better obtain the tools and expertise needed to tackle HOSSPs involved in money laundering or terrorist financing.

In the first decade after 9/11, the globe has been largely ineffective in supervising HOSSPs. The international community can address the resulting vulnerability by bringing the HOSSPs under a risk-based AML/CFT regulatory and supervisory framework that is effectively implemented. FATF could take these findings into account when it considers the policy implications of this report.

Note: The findings highlighted in this report should also be useful to other streams of work at the FATF, within national governments and for other stakeholders, for example in relation to the implementation of the FATF Standards.

CHAPTER 1: SCOPE OF THE PROJECT

The scope of the project is a discussion of typology and role of *hawala* and other similar service providers (HOSSPs) in money laundering and terrorist financing. HOSSPs are a subset of money or value transfer services (MVTS).

MVTS are defined by Financial Action Task Force (FATF) as financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods.

One key lesson from the survey questionnaire prepared by the typology project team and distributed to members of FATF and FSRBs and discussed at the typology workshop held in Dakar, Senegal in 2012[1] is that there is no common definition to the term *hawala*, which is interpreted in varied ways, having different meanings across jurisdictions. Some HOSSPs have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *underground banking*.

The term *hawala* is traditionally associated with a money transfer mechanism that operated extensively in South Asia many centuries ago and had strong links along traditional trade routes in Middle East and parts of East Africa. It operated as a closed system within corridors linked by family, tribe or ethnicity. In recent times, the term *hawala* has often been used as a "proxy" to describe a wider range of financial service providers, beyond these traditional and geographically tied systems.

In other countries, the term *hawala* is actually not used at all. However, there is a general recognition of the existence of *hawala* or *hawala-like* providers in many jurisdictions and of the type of methods they use and services they provide. There is also a general agreement as to what they are not: global money transfer networks (including agents) operated by large multinational money transmitters and money transfers carried out through new payment methods including mobile money remittance services.

Based on experience across countries, HOSSPs provide both legitimate and illegitimate services. They are money transfer service providers that are legal in certain countries if registered or licensed and illegal in others. In other countries, HOSSPs are referred only within the context of underground or criminal money transfer services.

For the purpose of this typology, HOSSPs are defined as money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time.

[1] The 11-member project team prepared a 47 question questionnaire, which was circulated to the FATF membership and to the FSRBS in September 2012. The APG sent an abbreviated version of the questionnaire to its members. Received questionnaire results were discussed at a typology workshop in Dakar, Senegal in November 2012.

While HOSSPs often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other settlement methods, including trade, cash, and long-term net settlement. Against this background, it is important to highlight that the definition of "*hawala* and other similar service providers" is based on the services provided by them and is irrespective of their legal status.

As described below, why HOSSPs exist and their services are utilized reflects a rather diverse set of reasons, often linked to country-specific circumstances. These include reasons of history, geography, culture, lack of banking access, currency controls, tax evasion and sanctions circumvention which create a demand and a market, or lead to the emergence of the provision of services described in this report.

This Chapter will explain the attributes of *hawala* and other similar service providers, how HOSSPs operate, what services are provided by them, who uses their services and what technology is used to transmit customer and transaction related information. It includes a discussion on the different formats of *hawala* and other similar service providers operations and the scale and nature of the "*hawala* and other similar" markets around the world.

1.1 ATTRIBUTES OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

H*awala* and other similar service providers share many attributes with other money transmitters. Like many other money transmitters, HOSSPs generally:

a. Are cash-in and cash-out businesses that primarily send personal remittances of low value. This does not preclude them from sending high value business transfers.

b. Operate in areas with high percentages of expatriate workers (in particular in originating countries), often in competition with other money transmitters.

c. Offer legitimate financial services to migrants sending remittances; however, they can also be used (or abused) for illegitimate purposes to move illegal/illicit money across the borders.

d. Operate within a community, are visible and accessible to their customers, are able to know their customers and maintain accurate records sufficient to ensure they complete transactions whilst preserving their profit

e. Run other businesses in addition to money transfer.

f. Belong to networks of similar operators in other countries.

g. Communicate only limited information on the customer and beneficiary as far as individual transactions are concerned. This communication is limited to what is needed to complete the transaction. This information generally includes the beneficiary name, contact number and may also include a transaction reference number (code number/words to identify recipients), in order to ensure that the delivery is made to the right person in an efficient manner.

HOSSPs tend to use specific and distinct settlement tools: They settle through trade, cash courier or net settlement, often without any direct wire transfer between the originator and beneficiary.

However, they may also send wire transfers aggregating funds received through individual remitters through the international banking system. In addition, they sometimes reconcile/settle through third party payments, which may lead to long settlement durations.

1.2 TYPES OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS CATEGORIZED BY LEGITIMATE AND ILLICIT USE

For the purposes of this typology, there are three major types of *hawala* and other similar service providers that operate across the globe as categorized by legitimate and illicit use – to which distinct ML/FT risks apply:

- **Pure traditional** (legitimate) *hawala* and other similar service providers;
- **Hybrid traditional** (sometimes unwitting) *hawala* and other similar service providers and
- **Criminal** (complicit) *hawala* and other similar service providers

PURE TRADITIONAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

In South Asia and Middle East, the word *hawala* is commonly used to refer to "Pure Traditional *Hawala*", a centuries-old money transmission system which was often used for trade-finance. These systems have operated for centuries in an unregulated environment and are still present in some countries for trade-finance and personal remittances, sometimes under a regulatory umbrella, but more typically not. Pure Traditional *Hawala* and other similar service providers are also extensively used to send low-value remittances on behalf of individuals, for example, migrant workers – extending outside their historical geographical area as populations migrate and trade routes develop. For instance, *hawala* are a common provider for remittances to migrant workers in the United Arab Emirates, where a significant portion of the working class population is composed of expatriates. Pure Traditional *Hawala* and other similar service providers tend to be popular among migrants because of familial, regional or tribal affiliation and inadequate access to regulated financial services for senders/recipients in origin/ receiver countries. These service providers may primarily function to provide legitimate and efficient remittance/trade finance services to customers sending low value transactions. If sufficiently regulated and supervised, these providers, due to the low value of their average transactions, may present a low or lower money laundering and terrorist financing vulnerability. Minimal supervision in certain jurisdictions, however, may amplify the risk for misuse.

HYBRID TRADITIONAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Hybrid Traditional *Hawala* and other similar service providers or designated non-financial institutions or designated non-financial businesses and professions (DNFBPs) in the provision of legitimate services but at the same time they may also be used, wittingly or are also used, wittingly or not, for illegitimate purposes such as transmission of illicit money across the borders. These networks are not primarily set up to move illicit money but may be involved in illegal activities such as movement of money generated from tax evasion, to evade currency controls and to avoid sanctions, etc. These service providers utilize similar methods as traditional HOSSPs and are not a

part of a criminal network. They develop where there is an un-serviced demand for remittances; they may interact with other HOSSPs to complete transactions.

CRIMINAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

In some countries, there is concern that HOSSPs systems are increasingly being set up or expanded to service criminals. Providers who set up such systems are described in this report as "Criminal HOSSPs". Such systems are driven by illegitimate money flows and are often controlled by criminals or criminal groups. They therefore represent a high criminal money laundering and terrorist financing risk. A third party professional money launderer often runs the financial network. These criminal networks also enable other offences including tax fraud, currency offences and corruption. Criminal *Hawala* and other similar service providers are often a part of well-developed criminal networks that have been developed specifically to enable illegitimate activities. Initially these channels may be developed as networks to satisfy local/personal remittance needs by Traditional or Hybrid *Hawala* and other similar service providers. As the network grows into a strong transfer corridor, it becomes attractive to criminals and evolves into a criminal transfer corridor. These criminal networks are characterized by high value transactions between legal and natural persons that do not necessarily share the same cultural or geographic background. They are often used to send payments to countries with developed and regulated banking systems.

1.3 COMMON CHARACTERISTICS OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

This sub-section describes the common characteristics of "*Hawala* and Other Similar Service Providers" based on survey[2] results, previous FATF work on alternate remittance services, literature review and country presentations at *hawala* typology workshop. The descriptions are also influenced by the lack of a common definition or understanding of what HOSSPs are. All the characteristics may not always be present in all the countries of operations. In other words, only some of these characteristics may be present in some countries.

Generally *hawala* and other similar service providers include:

a. Illegal or unlicensed/unregistered money transmitters. More than half of the respondents confirmed that HOSSPs are generally either unregulated or illegal in their country. In most of the countries, *hawala* and other similar service providers have not traditionally been subject to any regulatory oversight. However, recent efforts have resulted in the shifting of *hawala* and other similar service providers into the regulated financial sector in several countries. In 50% of the countries that responded to the question, *hawala* and other similar service providers are now regulated. In some countries, the process of regulation is in its very early stage.

[2] Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, 22 countries provided an answer to this question and three countries could not because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

b. Alternative remittance providers that transfers funds outside of banks or other regulated financial institutions. All except one of the surveyed countries that responded to the question agreed to this, and this characteristic is the only one that is common in most of the surveyed countries.

c. Money transmitters that use net settlement with payout agents actually transferring no funds. In net settlement, there are no funds transferred for each and every transaction that takes place between *hawala* and other similar service providers. For these individual transactions, *hawaladar* (a money transmitter that provides *hawala* services) and similar service providers use their local cash pool to pay the beneficiary. After a set period of time (example after a month) only the net amount owed between the two *hawaladars* and other similar service providers is settled. About 80% of the surveyed countries concur that net settlement without transfer of funds is the most common settlement process used in their country by *hawala* and other similar service providers.

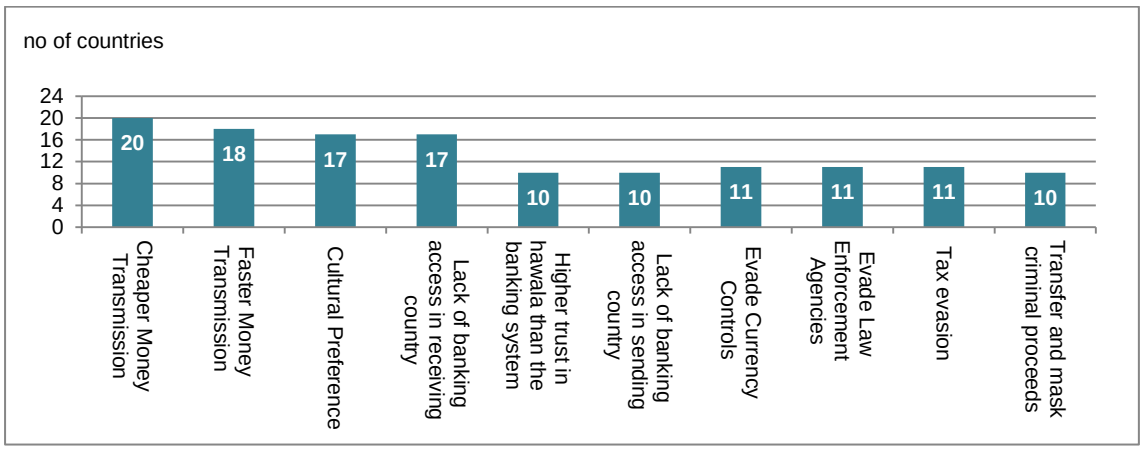
d. Money transmitters that settle through equivalent value instead of monetary instruments. Settlement through value may take place through trade transactions, such as merchandise or other commodities. At times, *hawaladar* and other similar service providers that owe debt to corresponding providers settle accounts by fulfilling commercial obligations of such corresponding providers such as paying a debt or invoice of same value that they owe. This approach is used in 68%of the countries that responded to the question.

e. Money transmitters that often only serve specific diaspora communities. About 32% of the countries believed that *hawala* and other similar systems serviced only specific communities. Traditionally, *hawala* and other similar channels were described as groups or networks that were based on familial, regional, or tribal affiliation. In recent times, *hawala* and other similar service providers have started servicing wider networks, but this is still an emerging trend.

1.4 REASONS *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS EXIST

This section highlights the main reasons for existence of *hawala* and other similar service providers in various countries. The survey sought information on what needs *hawala* and other similar service providers fulfil in the surveyed countries. Figure 1.1 below highlights the main reasons put forward and their frequency. As it can be observed, there are significant differences in the responses received, highlighting a noticeable disparity across countries, reflecting themselves the different characteristics of *hawala* and other similar service providers. Some characteristics are more prevalent in some countries than others. The responses indicated that some of the answers are not based on specific real-life examples, but more on perceptions of the roles and characteristics of HOSSPs.

Figure 1.1 **Reasons for Existence of *Hawala* and Other Similar Service Providers – Survey Result**



Source: F*ATF project questionnaire.*

Note: Only FATF member countries responded to this question. Out of 25 FATF member countries that responded 22 countries provided an answer to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

The most common reasons cited were:

a. **Cheaper Money Transmission:** *hawala* and other similar service providers usually charge 25-50% of the equivalent bank charge depending on destination of transfer, according to the responses of some countries. Depending upon the jurisdiction, customers generally obtain better exchange rates from HOSSPs than from the banks because they operate with very low overheads.

b. **Faster Money Transmission:** *hawala* and other similar service providers may have a vast network of counterparties located in specific countries. Money transmission can be completed in few hours or at the most in one or two days. In the same locations, banks can often take a few days or even longer in certain jurisdictions, to send an international wire transfer and money transmission networks may be unable or limited in their ability to compete. One of the reasons for quick transmission of funds under HOSSPs is that operators do not transfer cash for every client transaction, often resort to net settlement as do many other types of MVTS.

c. **Cultural Preference:** HOSSPs have existed for a long time in some areas of Central Asia, South Asia and Middle East, even long before the modern banking started operating. So it can be a cultural tradition for the people in these areas to transfer money through traditional *hawala* and other similar service providers. In many developed countries, such channels are primarily used by migrants because of ease of rapport building and access between *hawaladars* and other similar service providers and their customers, who share similar customs, lifestyle and language.

d. **Lack of Banking Access in Remittance Receiving and Sending Country:** Many remittance receiving countries have underdeveloped financial systems. In such

countries, *hawala* and other similar service providers have the ability to deliver money to distant locations where regulated channels do not exist. Countries like Nepal, Pakistan or some countries in North Africa and the Middle East are good examples of such situation. HOSSPs are also often the only channel through which funds can be transmitted in certain conflict regions like in parts of Somalia and parts of Afghanistan[3]. These remittance transfers are the safest, easiest and cheapest way to transfer funds in these countries.

In addition, on the remittance sending country side, where banking access is more developed, *hawala* and other similar service providers are often used by illegal foreign migrants residing in developed countries. Their illegal immigration status precludes these clients to access banks and other regulated financial services providers – leaving only limited cost-effective alternatives like unregulated service providers to send remittances to their families. It is worth emphasizing though that legal resident and migrants also extensively use these service providers for the other reasons stated in this section.

e. **Higher Confidence in *Hawala* and other similar service providers than in the banking system:** This is true in countries where there is a cultural lack of confidence towards banks – in particular in countries where customers have in the past lost their deposits when bank failures occurred. The limited understanding or familiarity with traditional financial services due to lack of financial literacy may be another reason explaining this lack of confidence towards regulated financial institutions. Finally, language barriers are likely to be a significant hurdle for immigrant populations.

f. **Evade Currency controls and international sanctions:** Responses to the survey highlight how, in some specific circumstances, *hawala* and other similar service providers seem to have been used to circumvent restrictions applying to international transactions – for instance exchange controls or international sanctions. These responses and examples show how *hawala* and other similar channels are used to bypass currency controls or international sanctions that increase money laundering and terrorist financing risks.

g. **Evade Taxes:** Responses note *hawala* and other similar service providers are used to evade taxes - as the tax authority have access to records kept in banks, but usually do not have the same tools for HOSSPs and other similar service providers – or do not even try to trace transactions in such circumstances. The use by commercial businesses of unregulated networks (instead of official financial service providers) may signal the underlying intention of concealing the funds being transferred for tax evasion purposes or to avoid sanctions.

h. **Transfer or Conceal Criminal Proceeds:** Responses note that criminals are perceived to prefer to use HOSSPs to transfer funds because commitment to CDD procedures performed by some *hawaladars* are not believed to be as rigorous and

[3] A 2005 World Bank study estimated that 80 to 90 per cent of Afghanistan's economic activity at that time was facilitated by *hawala*.

deep as those of banks and other regulated financial institutions, and are less likely to be accessible to the authorities. Therefore where holders of illicit funds have access to HOSSPs and the operators are willing to serve them, it is thought easier to transfer criminal money through these channels. In addition, tracing the money flow by the competent authorities may be made more challenging because, even when records are kept they can be falsified (ranging from counterfeit or hijacked customer identities to complete sets of entirely fictitious business records), making them, less easily followed by law enforcement.

This summary highlights that *hawala* and other similar service providers offer services for legitimate purposes, but can also be abused – or set up for criminal purposes. The level of regulation of HOSSPs at both ends of a remittance (and their actual implementation of AML/CFT requirements) has a link to their level of risk.

1.5 OUTDATED ASSUMPTIONS

Some surveyed countries also noted that some of widely repeated characteristics of pure traditional *hawala* do not necessarily match the reality in all the countries, particularly in Western Europe and North America. These were referred to as "***Hawala* Myths**".

a. **An ancient and static system:** Even pure traditional *hawala* is actually an ever evolving one. Country experiences suggest that entities within licit network adapt their structure and methods to ensure remittance corridors are serviced efficiently. Each end of a remittance reflects the rules, regulations and context that they operate in. In many countries, an operation described as *hawala* looks and acts the same as a MSB in another country.

b. **Remittance system only, it also offers other financial services:** In its heartland, "pure traditional *hawala*" are not pure remittance systems. Apart from sending remittances, they also usually offer other financial services such as currency exchange, and in some jurisdictions, short term lending, trade guarantees, and safe keeping of funds. In some countries, they may operate as pawn shops, travel agencies and mobile phone shops.

c. **Paperless system:** Many *hawala* investigations have revealed that *hawaladars* and similar service providers actually keep detailed records. They maintain manual accounts, ledgers, computerized records or a combination of these. The businesses of some *hawaladars* are based on small margins of profit, and recording and tracking deposits, payments and transfers is important to their good reputation and efficiency; alternatively HOSSPs that service the criminal market need to keep detailed records in order to keep track of transactions completed through complex settlement methods such as third party payments and trade transactions.

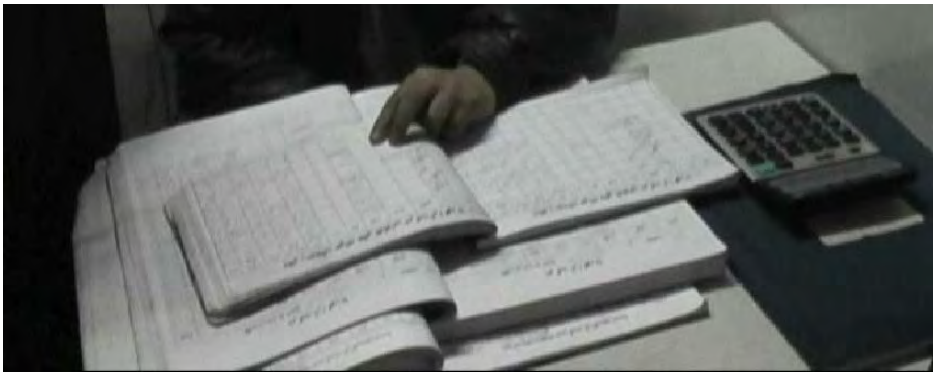


Image 1. **Hawala ledgers from Hawala Bazaar in Kabul, Afghanistan**

d. **Always Cheaper:** "*hawala* and other similar service providers'" transactions may be cheap but only within defined and specific corridors. Their competiveness is highest where customers need to send money to areas where traditional banking systems and large money transmitter's chains find it difficult, expensive or a high risk to operate. When such conditions are not met, the cost of sending funds through *hawala* and other similar service providers may actually not be that competitive.

e. **Trust based system of money transmission:** *hawala* are often defined as a trust-based system of money transmission. Rather than trust, *hawaladars* and other similar service providers actually rely on reputation for effective delivery. The customer chooses a *hawaladar* or other similar service provider because of their reputation for performance and this reputation is quickly lost when performance slips. *Hawaladar* and other similar service providers are also often relatively respected individuals within their community and success of their business is performance based.

f. **Underground:** In many countries, *hawaladars* and other similar service providers are actually highly visible within the community they serve and may even advertise their services openly (even when they are not a regulated or licensed or registered business).

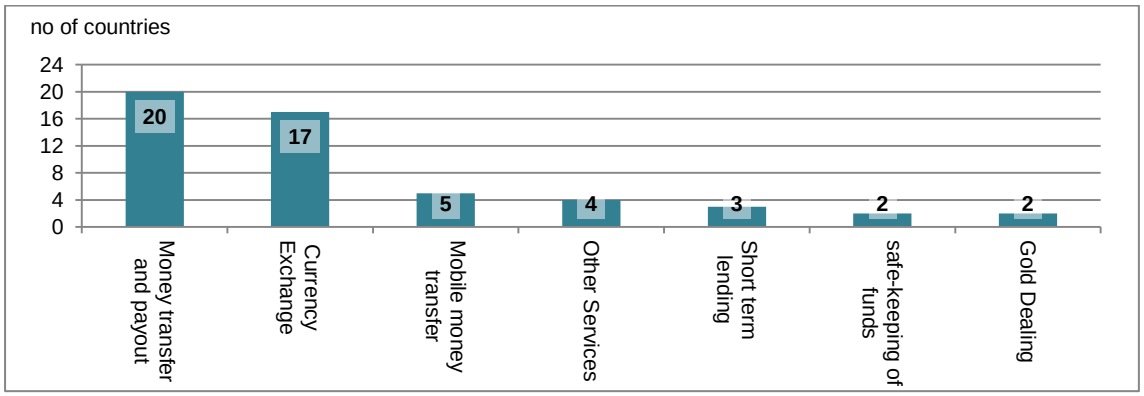
g. **High Risk always:** Depending on the type of *hawala* or other similar service provider and on the kind of services provided, the risk profile may actually differ significantly. The risk profile of the *hawala* and other similar services providers is dependent on its customer's risk profile, among others. *Hawala* transactions can be a lower risk if, for example, the service is provided by a regulated entity or entails low value transactions on behalf of low risk individuals.

1.6 SERVICES PROVIDED BY *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

The survey results as shown in Figure 1.2 summarize the feed-back on the types of services predominantly provided by *hawala* and other similar service providers. The two most common financial services provided are: 1) money transfer and pay-out and 2) currency exchange. Besides these services, *hawala* and other similar service providers may offer other services such as safe-

keeping of funds for the clients, short-term lending, mobile money transfers etc. although these are not as common.

Figure 1.2 **Financial Services provided by *Hawala* and Other Similar Service Providers**

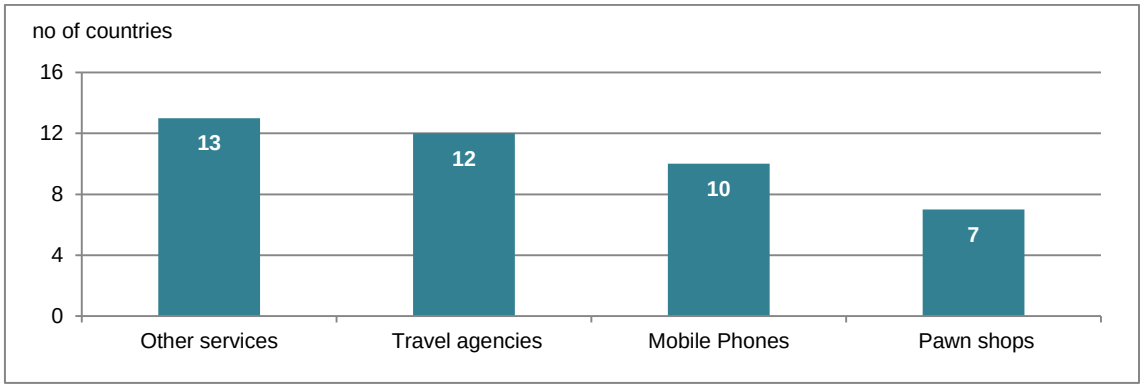


Source: FATF project questionnaire.

Note: Only FATF member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, 1 country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Apart from financial services, in many of the surveyed countries, *hawala* and other similar service providers also operate other business (see Figure 1.3). Typical side-line retail business includes travel agencies, pawn shops, selling mobile phones, SIM cards and mobile top-up cards. Many of them also operate as travel agents. In some cases they also operate as community specific grocers. Grocery stores are a typical venue for *hawaladars* and other similar services providers to conduct their remittance business. Many of them also provide import –export business – which creates an enabling environment for value settlement – in particular over-under invoicing when remitting funds to other geographic locations. Some *hawala* and other similar service providers also operate out of neighbourhood businesses, such as nail salons, beauty salons, flower shops etc. Such businesses not only generate more business for the service providers, but also provide a veil without being easily identified by regulators and law enforcement agencies. By running an additional business such as a travel or ticket agency or freight forwarding, criminal HOSSPs can derive an additional benefit that provides them with a ready supply of customer identity documents, which can be 'hijacked' and used to generate false customer records which are used to mask the receipt of criminally derived cash.

Figure 1.3 **Businesses Operated by *Hawala* and Other Similar Service Providers**



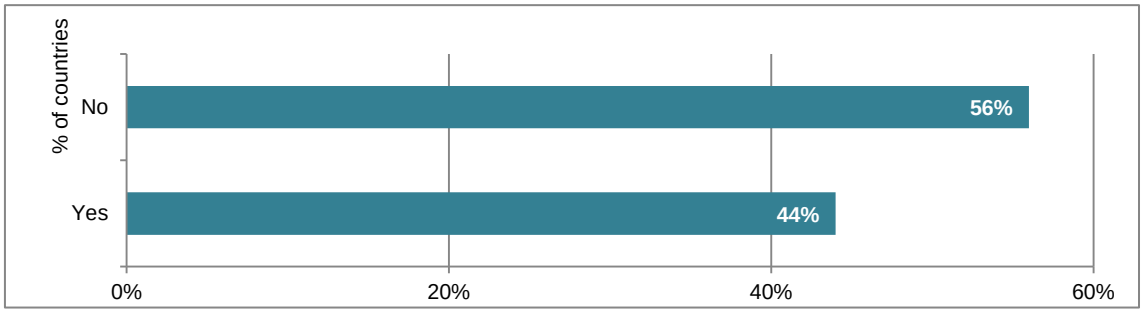
Source: FATF project questionnaire.

Note: Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, only 16 countries provided an answer to this question, 6 countries did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and Other Similar Service Providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

1.7 PROVIDING SERVICES TO UNBANKED

In a large minority of countries, HOSSPs are believed to provide services to the unbanked. Twenty five[4] surveyed countries answered the question whether HOSSPs provide legitimate financial service to the unbanked and under-banked in their country. Of those surveyed, 44% of the countries answered positively as shown in Figure 1.4. In the majority of the surveyed countries where HOSSPs are legal, they are considered to play an important role in providing financial services to the unbanked population, facilitate migrant remittances that support development, with the majority of the transactions being for overseas legitimate family support.

Figure 1.4 **Do HOSSPs Provide Legitimate Financial Service to the Unbanked?**



Source: FATF project questionnaire.

[4] Both FATF and APG member countries responded to this question. Out of 25 FATF member countries that responded 19 countries provided an answer to this question, 3 countries did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. Out of 8 APG member countries that responded 6 countries provided an answer to this question, 1 country did not respond to this question and 1 country could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country.

1.8 SETTLEMENT MECHANISMS USED BY *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

As noted above, settlement in the context of *hawala* and other similar service providers generally takes place through net settlement, with recourse to value settlement. The use of net settlement by HOSSPs is not unique, but a technique also often used by banks and other money transmitters. The use of value to settle is unique. Some however also use actual transfer of funds for the settlement purpose. Most of the regulated *hawala* and other similar service providers use regulated channels, such as the banking system, to settle if their respective ledger does not balance after certain time period.

In this context, the most frequent methods of settlement used by *hawala* and other similar service providers include:

a. Simple "reverse *hawala*": a remittance or payment going in the opposite direction. For example, an individual customer wants to send money from US to India. The service provider in the US will ask his counterpart in India to make a payment to the beneficiary in India. For this transaction, there is no transfer of funds between the two service providers, and the service provider in India will use his local cash pool to make the payments. To settle the accounts, sometime in the future the US service provider will make a payment to a beneficiary in US on behalf of a customer of the service provider in India. Over a period of time, the overall net amount of transactions may balance. When this does not occur, notably if the aggregate remittance flows are highly asymmetrical among countries, net settlement then takes place – often through wire transfers through the banking system.

b. "Triangular" settlement with networks of service providers. *Hawaladars* and other similar service providers may operate within a network that is spread across many jurisdictions. They use cross-provider balances on each other and correspondents to settle their respective accounts. In the above example, the service providers in the US and India both operate within the same broader network. After the initial transaction, the US service provider owes the Indian one. At the same time, the service provider in India has a customer who wants to send money to Somalia. If the service provider in India doesn't have any counterpart in Somalia, he would seek assistance from his counterpart in the US to identify a counterpart service provider in Somalia who owes debt to the US one. Once the Somalia service provider pays the beneficiary on behalf of the Indian one, all accounts are settled.

c. Value settlement through trade transactions, including through over or under invoicing. This type of arrangement is a common practice in Afghanistan, Iran, Pakistan and Somalia. In this case, operators use a surplus of cash or banked money to fund trade payments at the request of a business which in turn pays the individual recipients in the remittance destination region. International controllers or money brokers involved in criminal HOSSPs often settle by conducting completely separate trade transactions with criminally derived cash in their control.

d. Settlement through cash transport – notably cash couriers, including cross border.

Box 1.1 **Country Examples of Settlement procedures given by survey respondents**

Belgium: In some cases money remitters (HOSSPs) used the banking system to transfer bulk funds received from different clients to the bank account of hawaladars in Dubai. From there on, the money is send to the beneficiaries' in East-African countries using settlement through value or mobile payment systems. In other cases, money was directly transferred from Belgium to Pakistan using settlement through value, licensed money remitters and the regular banking system.

Sweden: Money is generally not moved physically or electronically at the time of the individual (usually rather small) payment order. Each month or at agreed point in time there is a settlement or clearance of transactions between the Swedish agent and the foreign agent. The difference is sent from the Swedish agent to the foreign (local) agent in one big lump sum through a Swedish bank to the bank account of the agent overseas. Settlement may also take place with merchandise or other commodities. In recent years it has also become more frequent that individuals (with or without their own business) make their own bank accounts available to international payment transfers.

Chinese Taipei: "Underground Money shops" (the Chinese term for HOSSPs) settle transactions either by direct remittances, cross-border transportation of precious metals, cash or mingling remittance transfer with trade accounts. In some recent cases, settlements were done through Western Union Remittance System and China Union Pay Cards as well.

Italy: Evidence from STRs in Italy suggest that HOSSPs may collect remittances from their customers (usually belonging to their own diaspora communities) and perform bulk transfers to the country of origin by making use of official channels, either by depositing the funds on his/her own bank account and making a wire transfer to his/her correspondent in the beneficiary country or by placing an order at a licensed money remittance transmitter. The use of prepaid cards in the remittance collection phase is also being observed.

Germany: Illegal HOSSPs often use relatives in foreign countries for the pay-out. Sometimes they travel to the foreign country themselves regularly to pay out the money. Another way is they use registered service providers, but act in their own name instead of the name of the customer. In some rare cases, authorized agents conduct money remittance business on their own behalf in an illegal way by using the software given by the principal remittance service provider.

Source: Country investigations, FATF project questionnaire.

1.9 TECHNOLOGIES AND COMMUNICATION TOOLS USED BY *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

The techniques and tools used by *hawaladars* and other similar service providers require effective communication mechanisms, as they cannot rely on the IT communication services of international funds transfers' providers.

Effective communication is also one key competitive advantage of these services providers, as clients value the immediate availability of funds. Telephone, fax and e-mails to communicate transmission messages to other services providers across the borders are therefore essential. Recently, authorities have been observing the use of advanced internet technologies by *hawala* and

other similar agents and suspect they are exclusively using protected online services to conduct their activities and maintain their accounts, leaving no manual accounts. Some of these authorities suspect that these services and websites are being hosted from servers located in Dubai[5]. The same authorities also consider that such agents also operate through banks located in Dubai for net settlement of their transactions, leaving no trail after being processed through these banks.[6]

1.10 SCALE OF UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

The scale of unregulated *hawalas* is unknown and is impossible to generalize. Most countries have difficulties reaching credible estimates of the size of unregulated *hawala* and other similar service providers. Variations are understood to be significant from one country to the other, as are the structure of the *hawala* and other similar services markets. In some countries, traditional *hawala* and other similar services providers are believed to be more prominent while in others, illegal/criminal operators reportedly represent the highest market share. The situation is further complicated as in many countries regulated money transfer agents are reportedly used to conduct illegal *hawala* and other similar services transactions separately and covertly in addition to their regulated activities. Such market structures make it even more difficult to estimate the amount of illegal HOSSPs in a country.

Out of the 21[7] countries that responded to the question on the size of illegal *hawala* and other similar service providers in their jurisdiction, only 8 countries attempted to provide some information on the scale of unregulated *hawala* and other similar services operations in their country. The remaining 13 countries acknowledged the existence of unregulated *hawala* and other similar service providers but could not provide any estimate. The estimated number of unregulated *hawala* and other similar services provided by countries ranged from 25 to several hundred. Countries pointed out that these estimates most likely underestimate the real number of unregulated operators. Some countries provided a rough estimate of the market share of unregulated *hawala* and other similar service providers in total remittance market, ranging from 10% to 50%. These estimates are largely based on investigations, are anecdotal, and may not be representative.

Against such difficulties to reach even reasonable estimates, regulating, supervising and monitoring unregulated *hawala* and other similar service providers proves very challenging.

Several reasons can be identified to explain the challenge in providing reasonable estimates, including: (1) Very small number of ML/TF investigations involving *hawala* and other similar service providers; (2) Very limited number of operations by public authorities to detect unregulated *hawala* and other similar service providers; (3) Strong variations and diversity in the structure of

5 Netherlands Authorities.

6 *Ibid.*

7 Only FATF member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, one country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

the *hawala* and other similar service providers markets; and (4) The absence in most countries of coordinated policy and operational coordination to identify unregulated *hawala* and other similar service providers.

1.11 LACK OF SUPERVISION EXACERBATES MONEY LAUNDERING AND TERRORIST FINANCING VULNERABILITY

One of the key findings of this survey is that how best to regulate and supervise *hawala* and other similar service providers remains one of the key challenges authorities face in many countries today and that a lack of supervisory resources for MVTS is a global problem. As with other sectors, the less regulated and supervised the *hawala* and other similar service providers market is, the greater the money laundering and terrorist financing vulnerability. Completely unregulated operators are particularly vulnerable to Money Laundering/Terrorist Financing risks because they permit funds to be sent with little or no CDD requirements, allowing a money launderer or terrorist financier to freely send funds with limited risk of being identified. The information collected from the questionnaire shows that with no requirement to comply with core AML/CFT obligations, most of the unregulated *hawala* and other similar service providers maintain records in a format that are not easily accessible to law enforcement authorities. Similarly, the findings highlight how limited supervisory capacity for the MVTS sector in most countries only exacerbates this problem. FATF could take these findings into account when it considers the policy implications of this report.

On the other hand, unregulated *hawala* and similar services provide legitimate and efficient remittance services to lower risk customers who pose lower ML/TF risk. Their services are particularly relevant where access to the regulated financial sector is difficult or prohibitively expensive.

The multi-dimensional nature of unregulated *hawala* and other similar service providers makes regulating the sector a complex issue, all the more so given the significant resources constraints facing supervisors of the MVTS sector. Understanding the dynamics of unregulated *hawala* and other similar service providers in the framework of broader financial system is important before designing a monitoring/regulatory/supervisory regime for the sector. One of the concerns expressed by the development community is whether over-regulating *hawala* and other similar service providers could result in such providers becoming completely underground and as a result, more vulnerable to ML/TF risks. Hard evidence, however, is difficult to come by to document this concern. As countries are imposing stricter AML obligations such as CDD in the regulated financial sector - including remittance and money transfer businesses, it is possible that unregulated sector might become more attractive for money laundering activities. Therefore it becomes of paramount importance for countries to balance these two facets of the sector in order to most effectively mitigate ML/TF risks.

While much attention has been paid to *hawala* and other similar service providers over the last ten years, the complexity, diversity, varying drivers and variety of the *hawala* and other similar service providers, particularly in countries where the regulated financial sector is far from having reached maturity, continues to make the set up and enforcement of effective regulatory and supervisory frameworks a challenge in many countries.

CHAPTER 2: MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH HAWALA AND OTHER SIMILAR SERVICE PROVIDERS

2.1 VULNERABILITY TO MONEY LAUNDERING AND TERRORIST FINANCING

As is always the case when criminals own or control financial intermediaries, criminal HOSSPs deserve particular attention. Although a limited number of case studies were provided to the project team, there are several reasons why HOSSPs continue to pose a money laundering and terrorist financing vulnerability. These include a lack of supervisory will or resources; settlement across multiple jurisdictions through value or cash outside of the banking system in some instances; the use of businesses whose primary focus may not be regulated as financial institutions; the use of net settlement or cover payments, not serial payments, to settle through the banking system that makes it difficult to track individual transfers; the commingling of criminal and illicit proceeds; and the masking of illicit proceed transfer that appears to be trade. None of these factors are unique to HOSSPs. The most significant reasons for concern are two-fold and jurisdiction-specific: lack of supervisory resources and settlement through value or cash that makes HOSSPs transactions particularly difficult for law enforcement to follow the money.

High threat HOSSPs networks often rely on the fact that the full size of the network is not visible in any individual country and that national registers of registered or licensed money transmitters are either not accessible or are difficult to find.

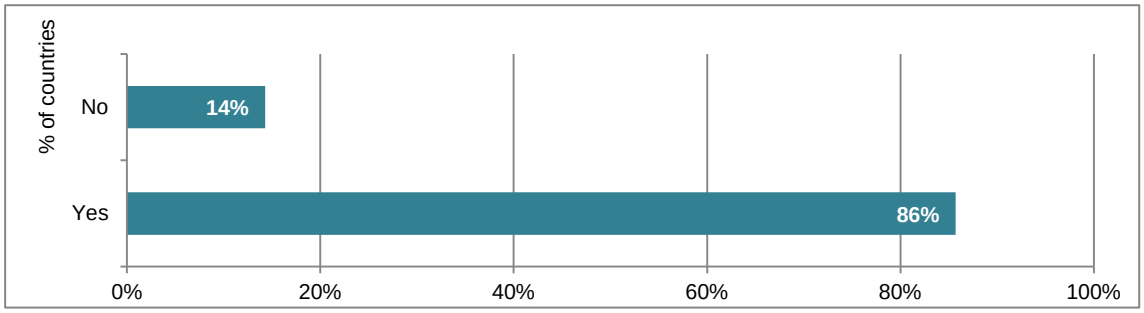
Most countries view HOSSPs as highly vulnerable to money laundering. Despite a limited number of cases provided to the project team, twenty eight[8] surveyed countries answered the question whether HOSSPs are regarded as high risk for criminal money laundering in their country. Of those, 86% of the surveyed countries stated that HOSSPs are vulnerable to ML risks as shown in Figure 2.1. All 4 countries that said no to the question clearly stated that HOSSPs are not commonly used in their countries because of the existence of highly efficient and convenient banking and remittance services.

Among the countries that answered positively to the question, very few responding countries clearly mentioned that there have been convictions of illegal HOSSPs for money laundering crimes. Some countries explicitly stated that they do not have the data to support the contention that HOSSPs are highly vulnerable, but base this conclusion on financial intelligence investigations/reports. A few countries raised concerns that increased customer due diligence and compliance processes in place at other types of financial institutions may make unregulated HOSSPs more attractive for money laundering. For these countries, HOSSPs are seen as vulnerable because they avoid attention from authorities including law enforcement authorities,

8 Both FATF and APG member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, 1 country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. Out of 8 APG member countries that responded 7 countries provided an answer to this question and 1 country could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country.

evade restrictions on foreign exchange controls and leave a minimal paper trail for law enforcement agencies to follow in comparison to banks or other money transmitters.

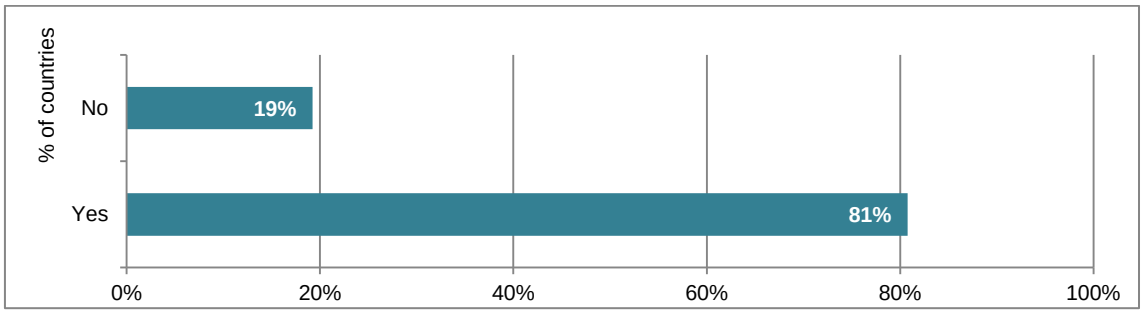
Figure 2.1 **Are HOSSPs vulnerable to money laundering risk?**



Source: FATF project questionnaire.

Most countries also view HOSSPs as highly vulnerable to terrorist financing. Twenty six[9] surveyed countries answered the question whether HOSSPs are regarded as high risk for terrorist financing (TF) in their country. 81% of the surveyed countries agreed that HOSSPs are vulnerable to TF risks as shown in Figure 2.2. All 5 countries that said no to the question clearly stated that HOSSPs are not commonly used in their countries because of the existence of highly efficient and convenient banking and remittance services.

Figure 2.2 **Are HOSSPs vulnerable to terrorist financing risk?**



Source: FATF project questionnaire.

Among the countries that answered positively to the question, only a few countries like India mentioned that there have been quite a few cases where the funds from abroad by the terrorist organizations were received in the country through HOSSPs. Many countries consider HOSSPs as high vulnerability for TF but have very few domestic cases to support the statement.

[9] Both FATF and APG member countries responded to this question. Out of 25 FATF member countries that responded 21 countries provided an answer to this question, 1 country did not respond to this question and 3 countries could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country. Out of 8 APG member countries that responded 5 countries provided an answer to this question, 2 countries did not respond to this question and 1 country could not provide an answer to this question because "*hawala* and other similar service providers" do not exist in their country.

2.2 CRIMINAL HOSSPS

A distinct form of criminal remittance network has been reported as operating internationally and servicing the needs of criminal organizations. These criminal HOSSPs appear to exist predominately to serve the criminal needs. In Europe and Australia, they are focussed on the collection of cash and transfer of value across borders, whilst in India or Pakistan they may be focussed on capital flight, exchange control violations or tax fraud.

2.3 WHAT MAKES CRIMINAL HOSSPS DISTINCT

Criminal HOSSPs primarily exist to facilitate the movement and/or laundering of criminal proceeds generated by drug trafficking, smuggling and fraud. Their existence is primarily driven by the demand from criminal customers to dispose of cash on their behalf and pay the equivalent value to the criminal group on demand elsewhere in the world. To achieve this criminal HOSSP networks use cash pools and reciprocal settlements by servicing remittances for other HOSSP groups. Individual criminal HOSSPs groups co-operate to form unregulated networks with surplus cash or individual electronic remittances are shared to complete the remittances demanded by different markets.

2.4 CRIMINAL HOSSPS METHODOLOGY FOR CRIMINAL PROCEEDS TRANSFERS

Law enforcement case studies indicate that criminal HOSSPs generally involve at least four individuals for the placement stage of criminal proceeds. These are:

- **Controller or Money Broker** – a trusted individual normally who arranges for the collection of street money (e.g., drug proceeds) and arranges for the delivery of an equivalent value to its ultimate destination (e.g., to businesses controlled by a drug cartel).
- **Collector** – instructed by the Controller to collect money from criminals and dispose it upon the controller's instructions.
- **Co-ordinator** – an intermediary who manages parts of the money laundering process for one or more Controller.
- **Transmitter** – receives and dispatches the money to the control of the Controller.

Role of the Controller: The Controller (also called a money broker in some jurisdictions) is the key to success of the system. The criminal customer tells the controller who will hand over the money and where the value is to be paid. Acting as a third party money launderer, the Controller serves multiple criminal organizations in multiple countries. The Controllers back office needs to keep records of the money he collects, controls and disburses. The Controller will normally be responsible for the money from the time it is collected until the value is successfully delivered as instructed. He may bear the cost of funds that are lost or are not effectively transferred.

Role of the Collector: The Collector is the Controller's trusted representative operating on instructions sent to him by the Controller, or his back office, by text message, email, and

Blackberry messenger or by other means. He faces the highest risk of arrest, because he has to meet the criminals to collect the cash. The Collector contacts the criminals and arranges to collect the cash at a discrete place or in circumstances where such activity, even if overt, does not attract attention. Over time the criminal and Collector may contact each other directly to arrange the pick-ups, but the collector will be told how much money he is responsible for and will dispose it on the instructions of the controller. The Controller will receive instructions from the criminal group directly or by such means which ensures the information is accurately received and understood.

2.5. COMPLETING THE CRIMINAL PROCEEDS TRANSFERS

Once the cash is counted, and any shortages accounted for, the Controller completes the criminal transaction by arranging for the equivalent value to be made available to the criminal group in the chosen destination, either by an electronic payment from a business controlled by an associate or through another handover of cash. Where the transaction is completed with a cash handover, the Controller arranges for this to be done by a Collector working for him or through another controller who co-operates with him. A token may also be used for this handover from a Collector to a criminal customer, but the process will start with a Collector nominating a bank note to be used, and conclude with the bank note being passed to the Collector.

2.5.1 AUTHENTICATING THE HANDOVER – USE OF A TOKEN

A regular feature of criminal cash handovers is the use of the unique serial number on a banknote to act as a means of identification and a rudimentary receipt for the handover. A Collector starts the process by identifying banknotes in his possession to be used as "tokens" in future transactions. He gives his Controller the serial number, and the controller then passes this on to the criminal customers holding the cash to be laundered. The criminal group ensures that the courier delivering the cash to the meeting knows what banknote will be presented to him. The collector shows the banknote and usually passes it over when he has received the cash. The criminal cash courier then takes the token away with him to show his bosses he has passed the money to the right person.

Box 2.1 **Use of Tokens in UK**

Communication between Controller & Collector to arrange Token number

		Send me any token no ugnt	06/01/2012 12:16:01 UTC (Device)	06/01/2012 12:15:57 (Network)	06/01/2012 12:15:57 (Network) 06/01/2012 12:16:01 UTC (Device)	Read	Inbox	
		LC26126666	06/01/2012 12:17:11 UTC (Device)		06/01/2012 12:17:11 UTC (Device)	Sent	Sentbox	

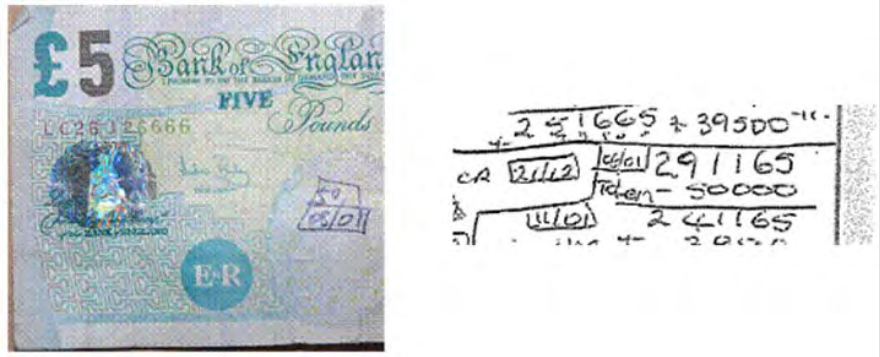
continued on following page

continued from previous page

Collector arranging handover with criminal customer and reporting to Controller

Simone west hounslow		Tw5 0Lf new HESTON road 122	08/01/2012 14:56:36 UTC (Device)	08/01/2012 14:56:34 (Network)	08/01/2012 14:56:34 (Network) 08/01/2012 14:56:36 UTC (Device)	Read	Inbox
		Have u recieved 50pin	08/01/2012 15:14:28 UTC (Device)	08/01/2012 15:14:26 (Network)	08/01/2012 15:14:26 (Network) 08/01/2012 15:14:28 UTC (Device)	Read	Inbox
		Nope gonna go pick up dis evening from same person in west london like last time	08/01/2012 15:17:11 UTC (Device)		08/01/2012 15:17:11 UTC (Device)	Sent	Sentbox
		Ok once u get plz let me know guys waiting for ks this side	08/01/2012 15:18:58 UTC (Device)	08/01/2012 15:18:53 (Network)	08/01/2012 15:18:53 (Network) 08/01/2012 15:18:58 UTC (Device)	Read	Inbox

Token seized from criminal courier marked with the amount collected and recorded in her drugs ledger



Step by step explanation – Use of tokens by criminal HOSSPs in UK

1. The first text message above is from a Controller to a Collector requesting the Collector sends a token number for use in a handover of criminal cash.
2. In the second text, the Collector sends the serial number of a Bank of England GBP 5 note to the Controller for use as a token; the Controller would then forward this token number, with the Collector's mobile telephone number, to the criminal customer.
3. In the third text, the Collector sends the criminal customer's courier the details of where to meet to conduct the handover – a UK postcode and address (probably for entering into a satellite navigation device).
4. In the fourth text, the Controller asks the Collector if the handover has taken place – the words '50pin' refer to the collection of GBP 50 000.
5. In the fifth text, the Collector confirms that the handover will take place later that evening from a criminal courier she has met before.
6. In the sixth text, the Controller asks for confirmation when the handover has taken place as his customers need the money elsewhere and he needs to make the equivalent value available to them as soon as possible.
7. The banknote shown has the same serial number as the token number in the second text and is annotated with the amount collected and the date (50 08/01 – note dates on text messages). In this case the Collector has retained the token, possibly because the criminal courier and collector already knew each other (see above).The extract from the ledger (completed by the collector) shows the Collector's record of the transaction.

Source: United Kingdom.

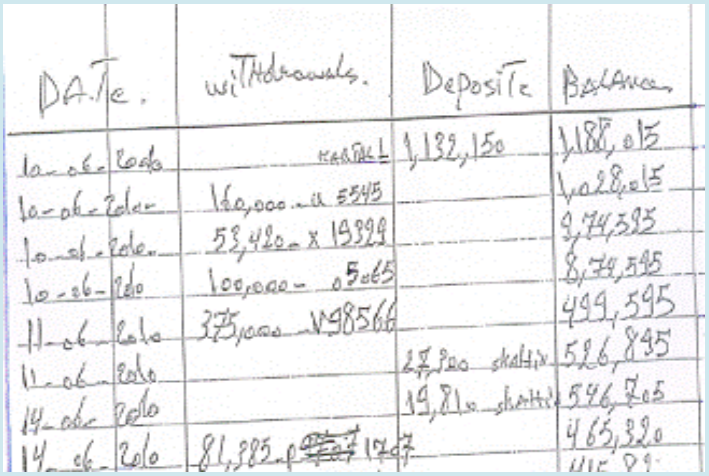
Box 2.2 **Use of Tokens in the Netherlands**

Another example of use of tokens can be seen in the following extract from a Dutch investigation. While the case example below is a real one, note the mobile phone numbers are fictitious. The real numbers have been replaced with randomly generated phone numbers.

Information that is sent through payment chain for conducting illegal transfer

- HOSSPs broker sends a SMS-message:
- 236430126 (mobile phone number)
- 163665 (amount to be transferred USD 163 665)
- X4569 (Token, identification number)
- The HOSSPs broker calls the mobile phone and delivers the money.

Example of a token. Part of a banknote is used as identification for a transfer.



DATE.	WITHDRAWALS.	DEPOSITE	BALANCE
10-06-2010		1,132,150	1,188,015
10-06-2010	160,000 - 5545		1,028,015
10-06-2010	53,420 - x 19999		974,595
10-06-2010	100,000 - 05665		874,595
11-06-2010	375,000 V98566		499,595
11-06-2010		27,200 skatti	526,895
14-06-2010		19,810 skatti	546,705
14-06-2010	81,385 - [illegible]		465,320

Record from a Dutch Collector showing a Token number (*e.g.,* V98566) being used for each "withdrawal" or handover.

Source: Netherlands.

2.5.2 CRIMINAL HOSSPS CONTROLLER TRANSFER METHODS

The Controller takes responsibility for the cash once the Collector has made the handover. The Controller may charge a fee based on the percentage of the money and/or manipulate the exchange rate used to make a profit. The cash value becomes his as he uses value held in separate cash pools to complete the criminal transaction. Controllers have used the following identified methods to dispose of the cash:

a. Using local complicit money service businesses to bank and transmit the money to third parties or into accounts run by the Controller;

b. Passing the cash to other "customers" of the Controller to complete separate inward remittances which can be legitimate but are most profitable when they complete a different criminal transfer;

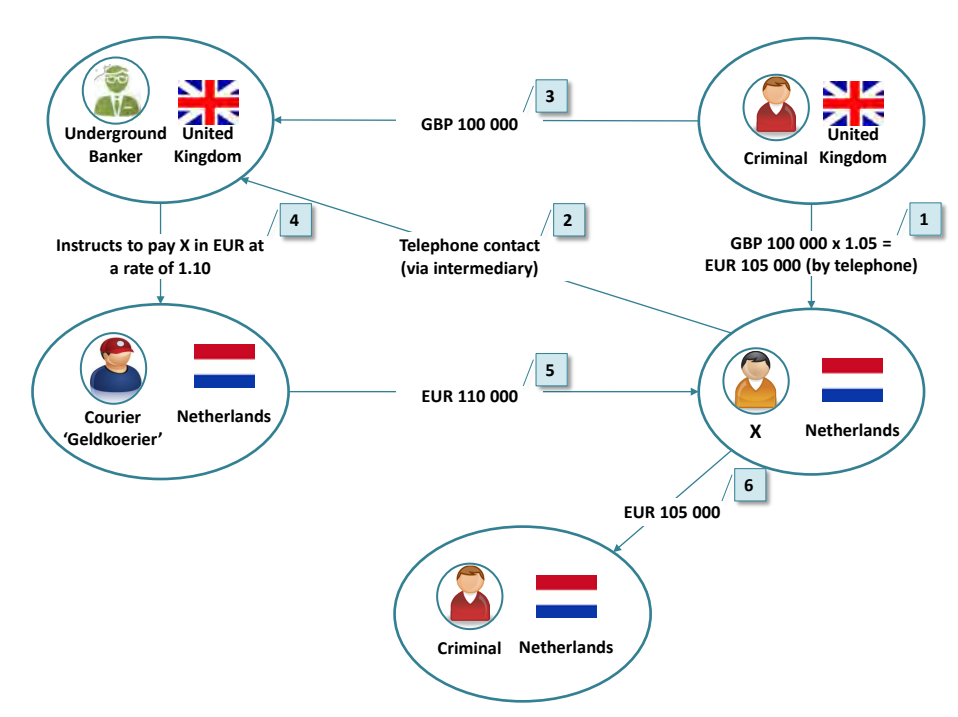
c. Paying the cash into bank accounts on behalf of the Controller to complete separate inward remittances (cuckoo smurfing); and

d. The physical movement of the cash (cash smuggling) by courier or in freight for sale or disposal at a safer location.

None of these techniques are necessarily unique to Criminal HOSSPs.

Box 2.3 **Illegal Currency Trade**

The following example from the Netherlands shows how the Criminal HOSSPs network profit from criminal proceeds transfer.



The picture above shows the working of the underground banking currency traders. The procedure of illegal currency trade is as follows (boxed numbers in above figure correspond to

transaction).

1. Underground broker/criminal HOSSPs broker X resides in the Netherlands and makes a phone call to a criminal or an intermediary in UK who has GBP 100 000 and wants to pay Euros to a criminal contact in the Netherlands. X buys the GBP 100 000 and offers an exchange rate of 1.05. This rate is lower than the official exchange rate. Either the criminal accepts or negotiates the rate with the underground broker.
2. X makes a phone call to a criminal HOSSPs broker in UK. In this phone call X offers GBP 100 000 at an exchange rate of 1.1 to EUR. This rate is higher than the official exchange rate. The broker in UK agrees to pay higher exchange rate probably because he can probably sell pounds later for better exchange rate.
3. The GBP 100 000 is physically transferred in UK from the criminal in UK to the underground broker in UK.
4. The underground broker in UK calls a contact in Netherlands (in picture 'Geldkoerier Nederland') and directs him to pay EUR 110 000 (GBP 100 000 x 1.1) to X.
5. The contact *Geldkoerier Nederland* in Netherlands brings EUR 110 000 physically to X.
6. X pays EUR 105 000 to a criminal in Netherlands. X makes a profit of EUR 5 000 on this specific criminal currency trade and there is no physical money transfer across the border. Such transactions can be easily undertaken without paper trail.

Source: Netherlands.

2.6 MONEY LAUNDERING VULNERABILITY OF HOSSPS

2.6.1 USE OF THIRD PARTY PAYMENTS TO TRANSFER CRIMINAL PROCEEDS

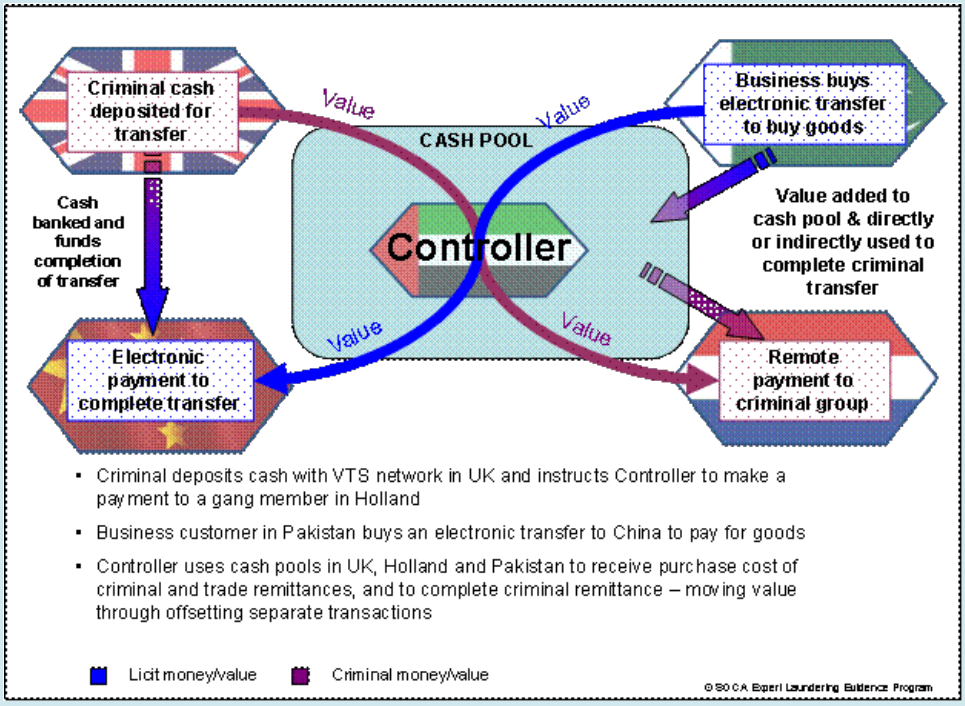
A common technique used by criminal HOSSPs is to use third party payments to transmit funds as well as to commit export and import fraud. Controllers build up large cash pools in countries where they service drug traffickers and other cash based criminals. To move the value of this cash, they directly or indirectly offer remittance services to other markets which have a demand for electronic remittances. They can do this by undercutting bank costs and exchange rates and use their cash pool to complete licit remittances, but they are also uniquely placed to service other criminal remittance corridors serving customers undertaking tax fraud, import fraud, export fraud or breaching exchange controls.

The Controller sends limited information to their transmitter, just enough information to complete a bank electronic transfer request. This will typically comprises of the beneficiary account Name, account number, SWIFT code and amount. In a country where the banks or regulators are vigilant the transmitter has often been observed creating false invoices to provide a false provenance for the transfer made.

This process is known as third party payment or invoice settlement, and has commonly been used by criminal HOSSPs, because it is an efficient way of moving excess values from a cash pool and HOSSPs get paid to do so.

Box 2.4 **The Use of Trade to Transfer Criminal Proceeds**

The example below is a typical third party payment settlement.



Controllers have a lucrative second market in servicing businesses and individuals who want to move value to breach local rules or to facilitate fraud. This may occur in countries where the amount of outward remittances in foreign currency is restricted or where exchange control or restricted access to foreign currency creates delay or high exchange costs. However access to a Controllers cash pools can also facilitate fraud.

Source: United Kingdom.

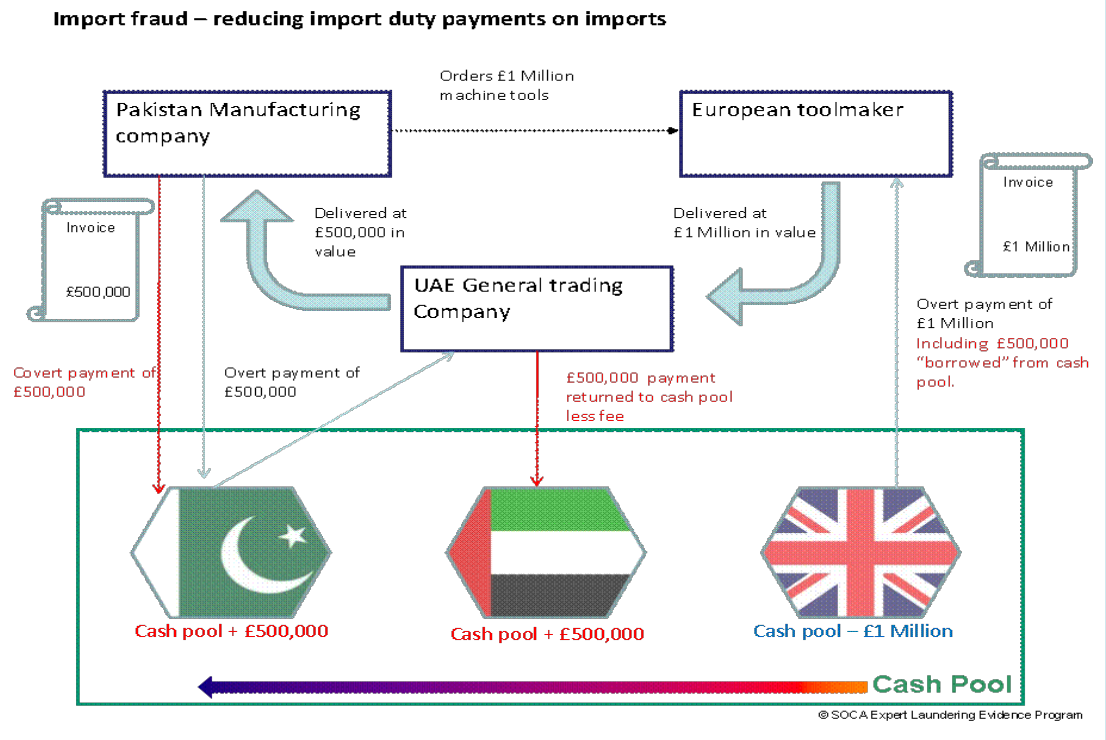
Box 2.5 **Import Fraud through third party payment**

In this example a Controller makes a third party payment to facilitate an import fraud. The example provided involves the United Arab Emirates and Pakistan:

- A Pakistan manufacturing company seeks to buy a new machine costing GBP 1 000 000.
- It identifies a European supplier and places a provisional order.
- To avoid import tax it uses a UAE general trading company as an intermediary. The UAE Company invoices them for the same equipment at GBP 500 000 in value, and an overt payment is made through an MSB associated to the cash pool. This provides all the documents required to validate the import of the machinery at a reduced value.
- At the same time the Pakistani manufacturer arranges for the full GBP 1 000 000 payment to be made through the cash pool in the UK. The goods are delivered to the UAE intermediary for onwards shipment to China.
- The UAE Company has a surplus of GBP 500 000 which it returns to or leaves in the cash pool

in UAE. The Pakistani manufacturing company also has a debt to the cash pool of GBP 500 000 (the balance of the true value of the imported goods) which it settles with a covert payment to the cash pool.

- The net result is that the UK cash pool is reduced by GBP 1 000 000 whilst the Pakistan & UAE cash pool increase by GBP 500 000 each.



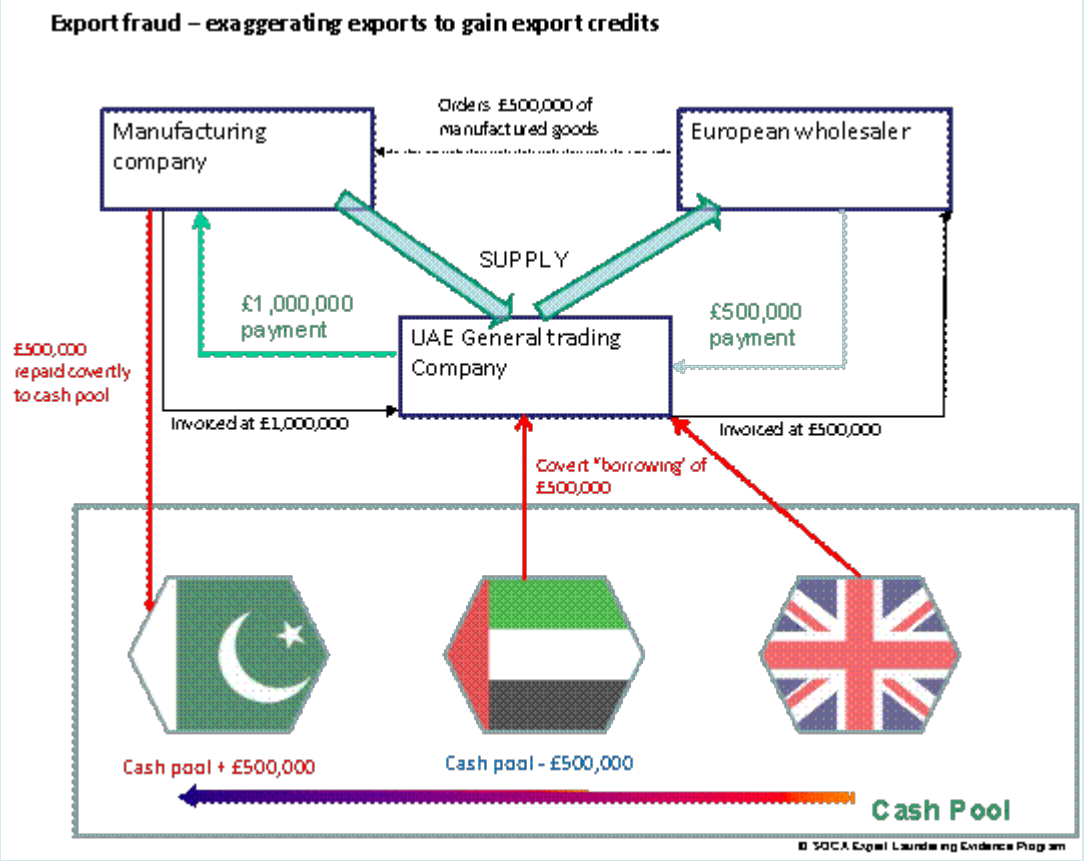
Source: United Kingdom.

Box 2.6 **Export fraud through third party payment**

- Case studies indicate that HOSSPs are used to facilitate export fraud. Export fraud can work in many ways, but the principal is the same – to overvalue export goods to benefit from export credits or tax rebates. This example uses Pakistan, where exporters can benefit from export rebates, GST rebates (equivalent of UK VAT), as well as beneficial access to credit.
- A European wholesaler orders GBP 500 000 of manufactured goods from a Pakistani manufacturing company.
- The Pakistani company arranges to supply the goods through a UAE company. This company invoices the buyer at a true value of GBP 500 000, receives payment and supplies the goods.
- At the same the Pakistani manufacturer raises an invoice for the same goods to the UAE Company but for a false value of GBP 1 000 000. The UAE Company "borrows" GBP 500 000 from the cash pool, combines this with the licit payment from the buyer and pays the full value of the false GBP 1 000 000 invoice.
- The Pakistani company returns GBP 500 000 to the cash pool in Pakistan to settle the amount borrowed in UAE plus any fees. The Pakistani company benefits from increased tax

rebates and access to credit.

- The net effect of the fraud is to move GBP 500 000 in value from the UAE to Pakistani cash pool.



Source: United Kingdom.

2.6.2 USE OF TRADE BY CRIMINAL HOSSPS TO LAUNDER DRUG PROCEEDS

Ample evidence underscores the use of criminal HOSSPs to launder drug proceeds. The use of trade by criminal money brokers has been identified by law enforcement as a common technique to facilitate the movement of drug proceeds generated in one jurisdiction to drug cartels outside of the jurisdiction. The net settlement technique called the "black market peso exchange" system is a common criminal HOSSPs method used in the United States and elsewhere by drug cartels.

Developed in the 1990s, Colombian and Mexican drug cartels export drugs to the United States, where they are sold for US dollars. The drug cartel enters into a contract with a peso broker (the controller), who uses a US-based agent to buy the US dollars from the drug sales. Once the US dollars are received, the peso broker deposits the equivalent in pesos into the drug cartels' account in Colombia or Mexico. To obtain the pesos, the peso broker buys the pesos from Colombian or Mexican-based exporters, who need to purchase goods in dollars in the United States or abroad. The broker then arranges for the importers to obtain the dollars in the United States to purchase goods for export to the importers' home country.

Box 2.7 **Criminal HOSSPs Use of Trade to Launder Drug Proceeds**

Case 1: Toy Company Used to Launder Proceeds

A Los Angeles-based toy company named Angel Toy Company manufactured plush toys like teddy bears. In March 2011, all three defendants pleaded guilty to conspiracy to structure currency transactions. In court documents, all three defendants admitted that, from 2000 through July 2010, there was an agreement that cash deposits into ATC's bank accounts had to be under USD 10 000 in order to avoid financial reporting requirements, specifically the filing of a Currency Transaction Report. The owners of Angel Toys received cash deposits, which were drug proceeds, into their banks accounts. The money was returned to drug traffickers when actual goods – in the case of the company, stuffed animals such as Teddy bears – are exported to the foreign countries and sold to generate local "clean" money.

The investigation revealed two primary ways in which ATC received and structured cash: in some cases, people affiliated with drug traffickers simply dropped cash at ATC's offices in downtown Los Angeles; the second method involved cash deposits made directly into an ATC bank account, sometimes by individuals located as far away as New York. During one four-year period, the investigation tracked more than USD 8 million in cash deposit into ATC accounts, and not a single transaction was for more than USD 10 000, according to court documents. The owners of Angel Toys were sentenced to more than three years in prison.

Source: United States.

Case 2: Use of Underground Money Shops and Local Banks to Launder Drug Proceeds

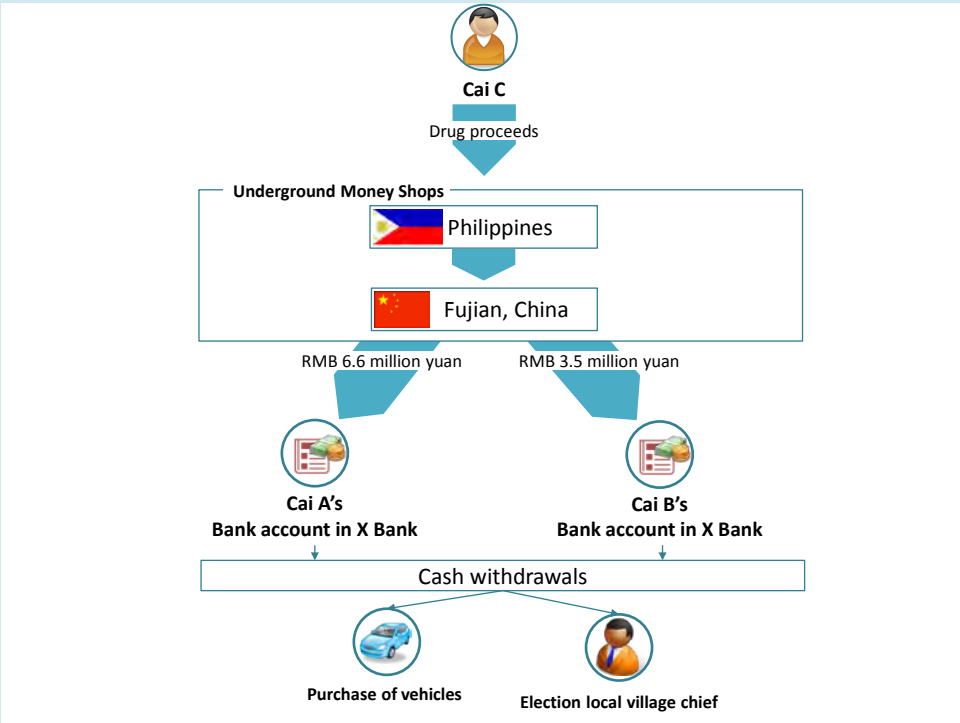
On May 9, 2005, fifteen defendants involved in '5.12' transnational drug trafficking case, which was jointly investigated by the Chinese and Malaysian police, were convicted of drug manufacturing and trafficking and money laundering by the Intermediate People's Court of Quanzhou, Fujian. Found guilty of money laundering, Cai A was sentenced to three years' imprisonment and a fine of RMB 330 000 yuan, and Cai B was sentenced to two and a half years' imprisonment and a fine of RMB 175 000 yuan.

From August 2002 to April 2004, the drug dealer Cai C had transferred the drug proceeds from underground money shops in Philippines to their counterparts in China. Abetted by Cai C, his relatives Cai A and Cai B respectively opened accounts with their own names in the local banks and deposited the illicit money in these accounts. The total amount of illicit money deposited in Cai B's accounts was about RMB 3.5 million yuan while that deposited in Cai A's account was about RMB 6.6 million yuan. Afterwards, most of the illicit money had been used for the purchase of vehicles and the election of local village chief.

The main process of money laundering activities in this case can be divided into the following steps:

1. Cai Ci transferred drug proceeds from underground money shops in Philippines to their counterparts in Quanzhou, Jinjiang and Shishi in China;
2. Underground money shops in Quanzhou, Jinjiang and Shishi deposited these funds in Cai A and Cai B's bank accounts;
3. Cai A and Cai B withdrew cash to purchase vehicles and so forth ordered by Cai Ci.

The flow of funds is depicted as follows:



Source: China.

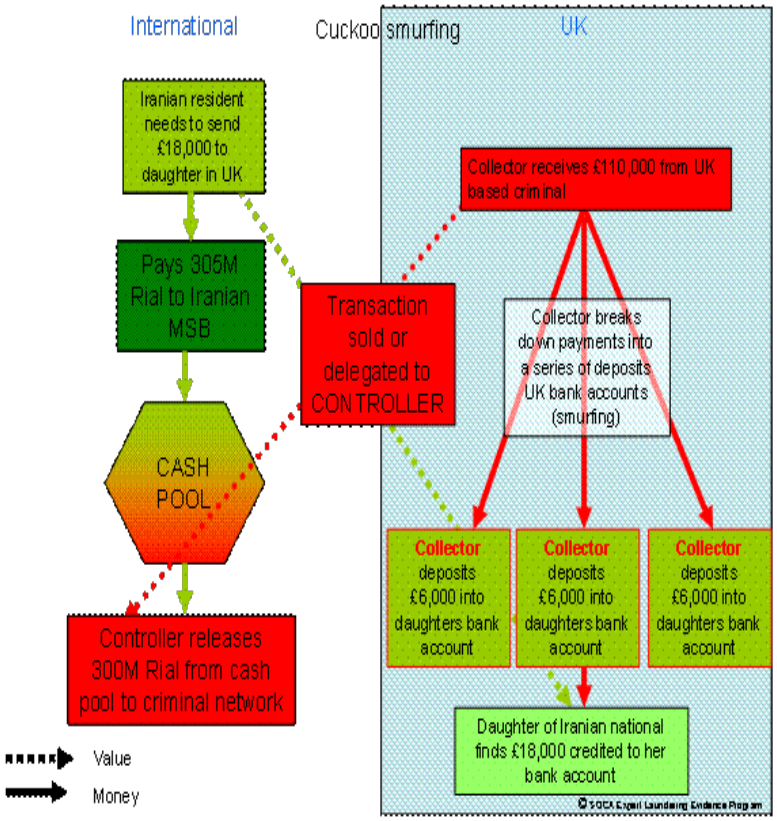
2.6.3 USE OF CRIMINAL HOSSPS TO EVADE SANCTIONS

Criminal HOSSPs are used to evade sanctions and to allow the transfer of funds into and out of sanctioned jurisdictions because these entities offer an alternative to banks and other regulated financial institutions that will no longer process transactions on behalf of sanctioned entities. Criminal HOSSPs are used instead because they can mask the identity of the ultimate originator from the banks or money transmitters that wire the funds on behalf of the HOSSPs. As illustrated below, one common technique is cuckoo smurfing. It occurs where the destination account is in the same country as surplus of criminal cash.

In the example in Figure 2.3, the Controller has a relationship with a *saraf* or money exchanger in Iran. A customer approaches the *saraf* to make a transfer of GBP 18 000 to the bank account of their daughter in UK. The Controller has a surplus of cash from a collection made from a Criminal group in UK and instructs their Collector to use part of this cash to make a series of small deposits into account number given by the family in Iran. The Iranian sender and recipient have no control over how the remittance is completed. The Collector chooses to "smurf" or structure the deposits to limit the likelihood of his role be identified by the receiving bank.

For the Controller this technique has the advantage of avoiding the costs and risk of running any overt business and also the bank charges are met by the person receiving the inward remittances. This technique has been the subject of large scale prosecutions in UK and Australia, with individual groups of Collectors responsible for cuckoo smurfing deposits into business and personal bank accounts in excess of GBP 100 million.

Figure 2.3 **Cuckoo Smurfing by Criminal HOSSPs**



Source: United Kingdom.

Box 2.8 **Sanctions Evasion by Criminal HOSSPs**

Iran Sanctions Evasion by Criminal HOSSPs: Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) agents arrest Manhattan management consultant on charges of criminally violating the Iran Trade Embargo. ICE agents, acting as part of a New York-based Task Force, arrested Mahmoud Reza Banki on January 7, 2009. The investigation was conducted jointly by ICE and the U.S. Treasury's Office of Foreign Assets Control. According to the indictment, BANKI provided money transmitting services to residents of Iran by operating a *hawala* in which BANKI received wire transfers in a personal bank account he maintained at Bank of America in Manhattan totalling about USD 4.7 million from companies and individuals located in the following countries: Saudi Arabia, Kuwait, Latvia, Slovenia, Russia, Sweden, the Philippines, the United States, and other countries.

Generally, BANKI did not know the wire originators personally. He received the funds with the understanding that an equivalent amount of Iranian currency would, in turn, be disbursed to intended recipients residing in Iran. Banki informed an Iran-based co-conspirator, when funds had been received and the co-conspirator then disbursed the funds in Iran, less any fees. Banki, according to the indictment, used specific funds transferred into his Bank of America account to make joint investments in the United States with the Iran-based co-conspirator. Among other things, Banki used the funds to purchase a USD 2.4 million Manhattan condominium; to invest in securities for his own benefit and that of the co-conspirator; and to make payments on his credit card accounts, including about USD 55 000 in one month alone in the summer of 2007.

Banki was charged with violating the International Emergency Economic Powers Act (IEEPA), together with Executive Orders and U.S. Department of Treasury regulations; conducting an unlicensed money transmitting business; and conspiracy to commit those crimes. Banki was found guilty on June 4, 2010, of one count of conspiracy to violate IEEPA and to operate unlicensed money transmitting business; one substantive count of violating IEEPA; one substantive count of operating an unlicensed money transmitting business; and two counts of making false statements to a Federal agency. In response to a special verdict form, the jury found that BANKI was an aider and abettor with respect to the substantive IEEPA and unlicensed money transmitting counts. BANKI was also ordered to forfeit USD 3 314 047, which represents the sum of money involved in the offenses and the proceeds derived there from. In October 2011, the United States Court of Appeals reversed the lower court's decision that al-Banki had acted as unregistered money transmitter on technical grounds, but did not challenge the facts of the case.

Source: United States.

2.7 TERRORIST FINANCING AND HOSSPS

More than a decade after the promulgation of Special Recommendation VI, terrorists continue to use HOSSPs to transmit funds. Terrorist exploitation of money transmitters is a function of geography, culture and financial access. In many countries of greatest concern, HOSSPs traditionally were a legitimate and accepted type of remitters and the primary vehicle for fund transfers, both legitimate and illicit. Limited banking access and high degrees of corruption and tax evasion in some of these jurisdictions continues to lead legitimate customers and criminals alike to use networks of unregistered HOSSPs.

There are several reasons why HOSSPs continue to pose a terrorist financing vulnerability, including: a lack of supervisory will or resources; settlement across multiple jurisdictions through value or cash outside of the banking system in some cases; the use of businesses that are not regulated financial institutions; the use of net settlement and the commingling of licit and illicit proceeds. While the settlement through value or trade that masks the individual fund transfers is a source of vulnerability, the most significant reason for concern is lack of supervisory resources and commitment to effective regulation. Inadequate efforts of outreach to the unregulated sector to pull them into the regulated sphere in some countries plus limited or no enforcement actions against unregistered entities also minimizes the incentives for unregulated entities to subject themselves to regulation and supervision, making them more vulnerable to terrorist abuse.

Box 2.9 **Terrorist Abuse of HOSSPs – United States Cases**

Case Example 1: Terrorist Abuse of HOSSPs - Hamza Case

In April 2008, Money remitter sentenced to over 9 years for money laundering conspiracy and concealing terrorist financing Saifullah Anjum Ranjha, a Pakistani national residing in Washington, D.C. and Maryland, was sentenced to 110 months in prison for conspiring to launder money and for concealing terrorist financing in addition to being ordered to forfeit USD 2 208 000 worth of assets. This was an Immigration and Customs Enforcement (ICE)-led

investigation. According to his guilty plea, Ranjha operated a money remitter business in the District of Columbia known as Hamza, Inc. A cooperating witness, acting at the direction of law enforcement, held himself out to Ranjha and his associates to be involved in large scale international drug trafficking, international smuggling of counterfeit cigarettes and weapons. He also represented that he was providing assistance and financing to members of al Qaeda and its affiliated organizations and their operatives. From October 2003 to September 19, 2007, the cooperating witness gave Ranjha and his associates a total of USD 2 208 000 in government funds in order to transfer the monies abroad through a hawala. The cooperating witness represented that the monies were the proceeds of, and related to, his purported illegal activities and Ranjha laundered these funds believing they were to be used to support those activities. Ranjha was the primary point of contact for the cooperating witness and received the bulk of the monies from the cooperating witness, for a total of 21 hawala transactions in amounts ranging from USD 13 000 to USD 300 000. Most of the monies were turned over to Ranjha in locations in Maryland. On a few occasions the cooperating witness met Ranjha and other co-conspirators at Hamza, Inc. to provide monies for a particular hawala transfers. Ranjha arranged with his associates for the equivalent amount of monies, minus commissions, to be delivered to the cooperating witness, his third party designee, or a designated bank account in Canada, England, Spain, Pakistan, Japan and Australia. Ranjha kept a commission of approximately five per cent of the amount of currency sought to be transferred on each occasion. Other conspirators involved in a particular transaction retained an additional commission of between three to five per cent of the transaction amount. All the funds transferred abroad were picked up by cooperating individuals and returned to the Government.

Case Example 2: Terrorist Abuse of HOSSPs - Times Square Bomber case

On August 18, 2011, Mohammad Younis pled guilty in Manhattan federal court to operating an unlicensed money transfer business between the United States and Pakistan. One of the money transfers was used to fund the May 1, 2010, attempted car bombing in New York City's Times Square by Faisal Shahzad who is serving a life sentence in federal prison.

From January to May 2010, Younis provided money transmitting services to individuals in the New York City area by assisting in the operation of a hawala. On April 10, 2010, Younis engaged in two separate hawala transactions with customers who travelled from Connecticut and New Jersey to meet with him in Long Island. In each of the transactions, Younis provided thousands of dollars in cash to the individuals at the direction of a co-conspirator in Pakistan, but without knowledge of how the customers were planning to use the funds. At no time did Younis have the license to operate a money transmitting business from either state or federal authorities.

One of the individuals to whom Younis provided money was Shahzad, who, on June 21, 2010, pled guilty to a ten-count indictment charging him with crimes relating to his attempt to detonate a car bomb in Times Square on May 1, 2010. During the course of his plea allocution, Shahzad acknowledged receiving a cash payment in April 2010 in the United States to fund his preparations for the May 1, 2010, attempted bombing. According to Shahzad, the April cash payment was arranged in Pakistan by associates of the Tehrik-e-Taliban, the militant extremist group based in Pakistan that trained him to make and use explosive devices.

On September 15, 2010, Younis was arrested by the FBI and other agents of the New York Joint Terrorism Task Force.

Younis 45, of Long Island, New York, pled guilty to one count of conducting an unlicensed

money transmitting business.

Case Example 3: Terrorist Abuse of HOSSPs - Carnival Ice Cream Case

Abad and his nephew Aref Elfgeeh ran a money-transfer operation at Abad's Carnival French Ice Cream (or "Carnival") shop in Brooklyn, New York. Abad was arrested in January 2003; an arrest warrant was issued for Aref, who was arrested in December of that year. Carnival French Ice Cream maintained an account at J.P. Morgan Chase Bank ("Chase"), as well as account statements from 12 "feeder" accounts at Chase and other banks. Bank statements showed large totals of money deposited into the Carnival account in small amounts as transfers from 12 feeder accounts, and large sums of money wired out of the Carnival account to accounts in 25 other countries, including Yemen where one of the recipients was a known member of Al Qaeda that used the Abads business to transmit funds to him. In a one-month period during the fall of 2000, more than USD 245 000 was deposited into the Carnival account and more than USD 268 000 was wired out. Between 1996 and 2003, the total amount deposited into the Carnival account was USD 22 190 642.21, and the total amount withdrawn was USD 21 995 556.54. Abad was charged with operating an unlicensed money transmission business.

The money arrived in the feeder accounts by various means, including check deposits, cash deposits, and wire transfers. Then, money went from the feeder accounts to the Carnival account in generally one of two ways. Most often there were checks written from one of the 12 feeder accounts, payable to the order of Carnival French Ice Cream account and then it was deposited into the Carnival French Ice Cream account. On some occasions the feeder accounts would wire money over to the Carnival French Ice Cream account. There were hundreds of checks from the feeder accounts made out to the Carnival account. One of the feeder accounts was a Chase bank account opened in the name of Prospect Deli that was opened by Aref and listed the home address and telephone number of Abad. The Prospect Deli was a business a few blocks away from the Carnival French Ice Cream shop; the Prospect Deli was in operation only from 1996 to 1998, but activity in the Prospect Deli bank account continued until 2002. For example, bank records showed that in 2001 approximately $850,000 was deposited into the Prospect Deli account and about USD 823 000 was transferred out to the Carnival account. Aref was sentenced principally to 51 months' imprisonment, followed by a three-year term of supervised release, and was ordered to pay a USD 500 000 fine and to forfeit USD 22 435 467. Abad was sentence principally to 188 months' imprisonment to be followed by a three-year term of supervised release, and was ordered to pay a USD 1 250 000 fine and to forfeit USD 22 435 467.

Source: United States.

Box 2.10 **Terrorist Abuse of HOSSPs – Indian Cases**

Case Example 1: Terrorist Abuse of HOSSPs

In a case of hawala money transfer to terrorists of the proscribed terrorist organization "X" in India, two hawala operators along with two receivers of hawala money for the terrorists were apprehended in the year 2011 and an amount of approximately INR 2 000 000 (USD 32 000) was recovered from them. They revealed that the hawala money was provided by the organization leaders based in country "Y" and routed through another country "Z" where another over ground worker of the terrorist organization is based. The modus operandi is that the terrorist leader in country "Y" collects terror funds in that country and sends it to another terrorist agent in country "Z" who contacts hawala operators who operate freely in that country. Apparently hawala is not illegal in country "Z". The hawala operator in country "Z" then gives a number on a currency note to the agent along with the telephone number of the person who would deliver the money in India. The agent then informs the same to the terrorist leader at "Y". The terrorist leader at "Y" then contacts the over-ground worker of the proscribed terrorist organisation at Delhi and gives the telephone number of the hawala agent and the number of the currency note. This over-ground worker then contacts the hawala operator at the given number and then collects the money at the decided location after giving the number of the currency note. The over-ground worker does not get to know the identity of the hawala operator as he delivers the money wearing a scooter helmet.

Note: The terrorist agent does not have to pay any commission at the receiving end.

Case Example 2: Terrorist Abuse of HOSSPs

In another case of Terrorist financing, a sum of INR 10 000 000 (USD 160 000) was intercepted in a State A in India which was meant to be delivered to a terrorist gang X. Investigation revealed that a number of earlier consignments had earlier been delivered to the terrorist gang earlier. It was revealed that development funds of a particular area in that State was defalcated and then sent to location P in that State. From location P, it was sent to location Q in another State B with the help of hundi operators operating between State A and State B. The hundi operators are told that the money belongs to a very influential person at state A. The hundi operators do not object conducting the transaction hearing the name of this influential person and deliver the money at state B to the person authorized by the agent of the terrorist gang. The money is delivered after deducting a commission of 1 per cent from the total money which is transferred. At State B, the hawala money is then changed from INR to Dollars in an unregulated exchange market and then transferred to another country E where arms and ammunition are purchased by the terrorist gang leaders based there. These arms and ammunition are then transferred across the borders and then delivered to the terrorist gang operating in State A for carrying our terrorist activities. In this case a total of 15 accused were arrested and charge sheeted and the trial is being held. The arrested members include terrorists, contractors, agents and government servants.

Source: India.

CHAPTER 3: REGULATORY AND SUPERVISORY RESPONSES TO MITIGATE ML/TF RISKS

The findings highlighted in this chapter should also be useful to other streams of work at the FATF, within national governments and for other stakeholders, for example in relation to the implementation of the FATF Standards.

3.1 A REGULATORY/SUPERVISORY RESPONSE INFLUENCED BY THE LEGAL STATUS OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS (HOSSPS)

This section focuses on the legal status of HOSSPs in the surveyed countries. The findings of the survey confirm that countries have taken different approaches to the regulation of *hawala* and other similar service providers, with a slight majority of countries treating *hawalas* and other similar service providers as illegal.

Among the 33[10] surveyed countries, 18 countries treat *hawala* and other similar service providers as illegal while 15 countries consider them legal if registered or licensed. Interestingly, most developed countries allow licensing or registration of HOSSPs, while developing countries do not. Within the developed countries respondents, only six out of 17 countries define *hawala* and other similar service providers as "illegal" and the remaining eleven have legalised *hawala* and other similar activity if service providers are either registered or licensed. On the other hand, 12 out of 16 developing countries respondents define *hawala* and other similar activity as "illegal" and only 4 countries allow them to operate legally if licensed or registered (See Table 3.1.). One of the reasons put forward by developing countries to consider *hawala* and other similar service providers as "illegal" is their capacity constraints.

Table 3.1 **Legal Status of *Hawala* and Other Similar Service Providers**

	Status of *hawala* and other similar service providers		
	Illegal	**Legal**	**Total**
Number of Countries	**18**	**15**	**33**
of which Developed Country	6	11	17
of which Developing Country	12	4	16

Source: FATF project questionnaire.

At the same time, caution needs to be exercised when analysing the survey results. As explained in Chapter 1, countries have varying definitions of what *hawala* means. In the 18 countries where

[10] 25 FATF and eight APG member countries provided answer to the question on legal status of *hawala* and other similar service providers in their country. Please note that three FATF member countries responded to this question where *hawala* and other similar service providers do not exist as a money transmission channel but *hawala* and other similar service providers is either legal or illegal under an existing law.

hawala and other similar service providers are illegal, two rather different approaches can be identified:

- Countries that do not allow *hawala* or other similar service providers to operate because *hawala* in these countries is synonymous to "illegal" operations. However, providers of the same kind of services can legally operate if licensed or registered but under a different name such as money service providers, or payment institution, or money remitters and therefore not included in the definition used in this report
- Countries where only traditional financial institutions – such as banks -are allowed to provide money remittance services. In such countries, *hawala* and other similar service providers are simply supposed to be non-existent.

3.2 IMPACT OF THE LEGALISATION OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS ON THE FORMALISATION OF THE REMITTANCE MARKET?

To gauge the impact of the legalisation of *hawala* and other similar service providers, the surveyed countries were asked whether legalizing *hawala* and other similar service providers has helped in formalizing the remittance market successfully in their country. 80%[11] of the surveyed countries where *hawala* and other similar service providers are legal answered positively to this question, confirming that licensing or registration requirements have led to an expansion of the regulated remittance market (Figure 3.1). However, this seems contradicted by the numbers of registered/licensed *hawala* and other similar service providers provided in the questionnaire responses by the countries where *hawala* is legalised. The number of domestic principal licensed/registered *hawala* and other similar service providers in seven[12] countries reporting numbers ranged from four to 26. In one country, the number of businesses registering as unregulated value transfer services (informal value transfer services or IVTS), a broader category than HOSSPs, was over 1 000. This country uses the term IVTS to refer to any system, mechanism, or network of people that receives money for the purposes of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form.

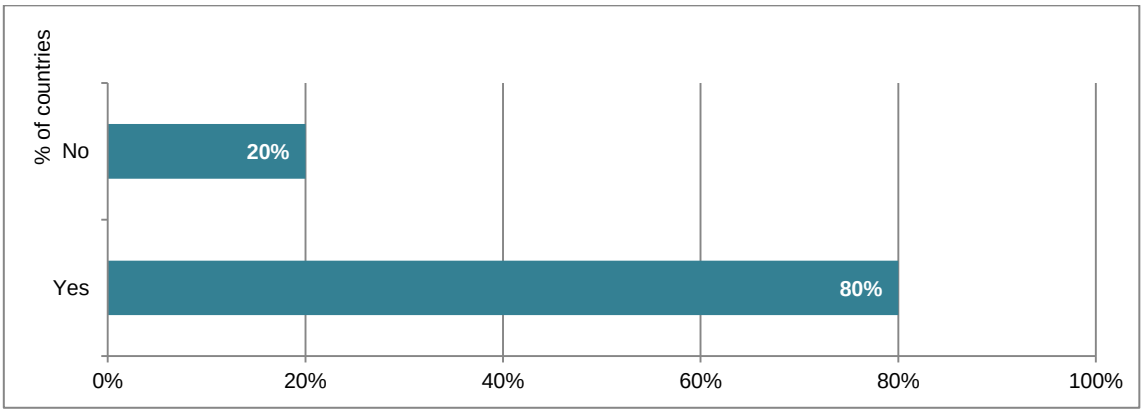
In general, the numbers of regulated HOSSPs are still very few—making it very likely that unregulated *hawala* and other similar service providers are in effect continuing their business in these countries. In most of the countries where *hawala* and other similar service providers have been legalised, they operate as licensed Money Service Operators (MSOs) and are required to

11 15 surveyed countries have legalised *hawala* and other similar service providers. Out of 15, 10 countries responded to the question. 4 countries where HOSSPs are legal did not respond to the question and one country could not respond because *hawala* does not exist as a money transmission channel in that country though *hawala* and other similar service providers is legal under an existing law.

12 Out of the 15 surveyed countries that legalised *hawala* and other similar service providers, eleven countries have provided information about licensed or registered domestic *hawala* and other similar service providers. But only seven countries could provide exact number of licensed/registered *hawala* and other similar service providers operating in their country.

conduct customer due diligence (CDD), keep records and implement other AML/CFT obligations set out in law - which contributes to mitigating ML/TF risks.

Figure 3.1 **Did Legalisation of Hawala and Other Similar Service Providers Help Formalise the Remittance Market?**



Source: FATF project questionnaire.

3.3 LESSONS LEARNED REGARDING THE LICENSING /REGISTRATION REQUIREMENTS FOR REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Building on the survey results, this section presents the licensing/registration requirements for regulated *hawala* and other similar service providers and their agents/branches.

3.3.1 SURVEY RESULTS: LICENSING/REGISTRATION REQUIREMENTS FOR REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Under a registration regime, the service provider has to identify its business to the authorities and provide certain information (as may be requested by the authorities). Authorities usually attach few or no conditions to the ability of the service provider to provide its services under the registration regime, making the market entry easier. Although there are varying practices of registration requirements, registration regime tend not to require AML/CFT compliance systems prior to registration unlike licensing system, and the initial application fee for registration is also lower than that for obtaining a license. A licensing regime provides more front-end screening by authorities and requirements to meet certain criteria. Regulatory authority grants the licensee the permission to engage in certain activities subject to specified terms and conditions. Such terms and conditions may define purpose, time-period, territory, compliance requirements, and operational instructions among others.

The survey results as shown in Table 3.2 illustrate that registration and licensing regimes are almost equally used in countries where *hawala* and other similar service providers have been legalised. The licensing approach is slightly more common with a total of seven countries adopting it compared to five countries which adopted a registration regime. Two countries— Republic of Guinea, and Sweden—have dual system depending on the size and type of service providers. For example in Sweden, a legal or natural person who is involved in commercial money remittance is

obliged to be either licensed (as a payment institution) or registered (as a registered payment service provider). The turnover of business is one among other factors that determines whether registration is sufficient or not. Similarly in the UK, a dual system is in place by which the service provider needs to obtain a license from the Financial Conduct Authority as an authorized payment institution or a payment service provider, but at the same time, also needs to register with the Customs and Tax authority for AML/CFT purpose.

Table 3.2 **Licensing/Registration Requirement for *Hawala* and Other Similar Service providers**

	Licensing	Registration	Dual
Developed Country	6	3	2
Developing Country	1	2	1
Total	7	5	3

Source: FATF project questionnaire.

3.3.2 SURVEY RESULTS: LICENSING/REGISTRATION REQUIREMENTS FOR AGENTS OR BRANCHES OF *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

In the majority of the countries where *hawala* and other similar service providers are legal, they usually can operate through branches or agents, which allow them to reach out to remote areas and expand their business. Survey results illustrate that in the case of agents, registration is by far the preferred approach, while in the case of branches, registration, licensing, as well as dual systems are used.

In the case of branches, one of the reasons why licensing or dual systems are used more often than in case of agents is that these are service providers which usually deliver only financial services (Table 3.3). By contrast, agents tend to provide remittance or other financial services as ancillary services to other businesses, such as operating supermarket, gas station, grocery stores, etc.

Table 2.3 **Licensing/Registration Requirements for Agents/Branches of Hawala and Other Similar Service Providers**

	Branches	Agents
Only Licensing	2	1
Only Registration	5	7
Dual System	1	0

Source: FATF project questionnaire.

3.3.3 REGULATING MARKET ENTRY FOR *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS: LICENSE OR REGISTRATION REQUIREMENT? [13]

Several factors determine the choice between a licensing regime and a registration regime—which in themselves have different impact on the ease/control of market access and the resources required for regulatory/supervisory oversight. This choice is also likely to have a bearing on the incentives for businesses between staying informal or entering the regulated economy.

Registration regimes require fewer conditions to be fulfilled at the time of entry thus making it easier to enter the market. Licensing regimes are most often more involved processes with more demanding conditions. They also usually require front-end screening of the applicants by the authorities. As a result, registration processes are expected to be faster and less resource consuming, while more supervisory capacities are expected to be necessary for licensing regimes. All things being equal, the less stringent up-stream conditions under registration regimes are expected to call for more on-going supervision and surveillance—particularly if the market is composed of a large number of smaller players.

Another important factor is how the registration/licensing regimes comparatively affect the incentives for expanding remittances through regulated channels. Survey results do not point to any clear cut benefit from one system compared to the other. It is however expected that the lower the barriers at entry and application fees, the easier it would be for market participants (notably the smaller ones) to enter the regulated market.

Both registration and licensing regimes create a framework for supervisors to exercise control over who can act as a principal service provider or an agent and to ensure compliance with AML/CFT obligations. Licensing requirements are expected to be more comprehensive and rigorous; they are also more expensive, which increases compliance costs for both the authorities and the service providers – irrespective of ML/TF risks.

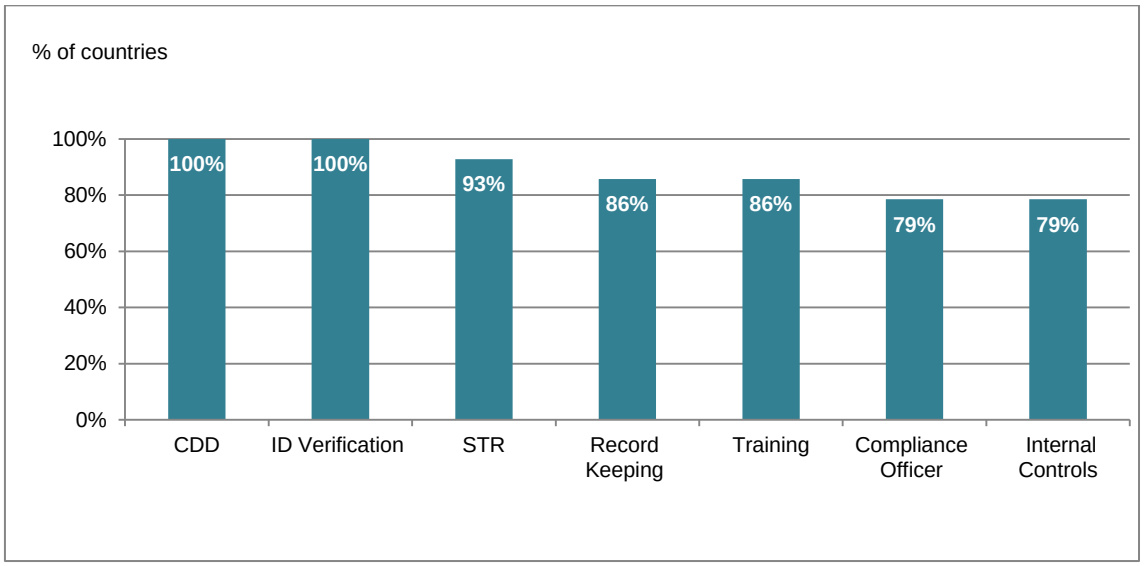
3.4 AML/CFT OBLIGATIONS OF REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Where legal, money service businesses and *hawala* and other similar service providers are usually treated the same way and subject to the same regulations as far as AML/CFT obligations are concerned. Out of 15 countries where *hawala* and other similar service providers are legal, 14 countries provided data on AML/CFT obligations of regulated *hawala* and other similar service providers in their countries. Survey results as shown in Figure 3.2 indicates that 75-100% of these countries impose Customer Due Diligence (CDD), Identify (ID) verification, Suspicious Transaction Reporting (STR), Recordkeeping, Training, Compliance Officers, and Internal Controls Requirements. In particular, all these countries require compliance with CDD requirements. All except one country require STR reporting. All except two countries require training of staff on AML/CFT regulations and record keeping for a minimum of five years. Only three of these countries

[13] Discussion in this sub-section relies on information provided in the World Bank report "Making Remittances Work: Balancing Financial Integrity and Inclusion" (soon to be published). Authors: E. Todoroki, W.Noor, K.Celik and A. Kulathunga.

do not require the appointment of a compliance officer and development and implementation of an internal control program.

Figure 3.2 **AML/CFT Obligations of *Hawala* and Other Similar Service Providers (percentage of countries)**



Source: FATF project questionnaire.

3.5 SUPERVISION AND ENFORCEMENT RELATED TO *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Effective supervision of HOSSPs is one of the primary challenges facing regulators. This section discusses the survey results on the supervision of *hawala* and other similar service providers, sanctions applicable to regulated *hawala* and other similar service providers for failure to implement AML/CFT obligations and requirement on foreign counterparties with respect to money transfers.

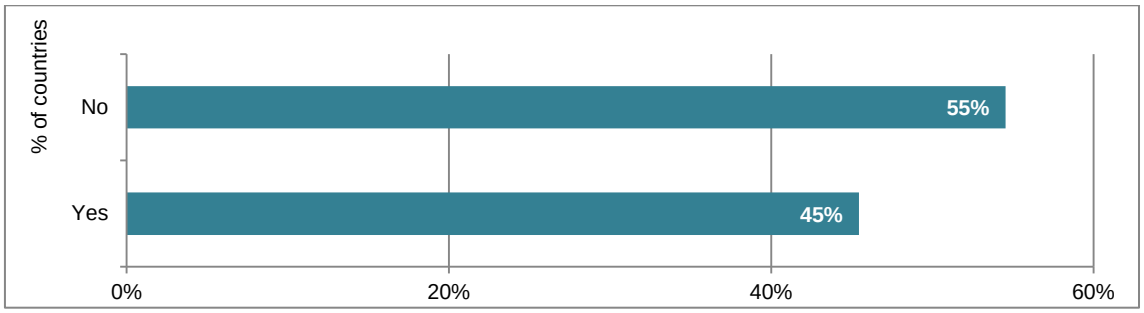
3.5.1 SUPERVISION OF REGULATED HAWALA AND OTHER SIMILAR SERVICE PROVIDERS

Five countries responded that they have a separate examination approach and teams for regulated *hawala* and other similar service providers while six[14] countries did not have such a separate approach, as shown in Figure 3.3. It is not clear whether the separate examination team is only for *hawala* and other similar service providers or it is for general remittance companies, money service providers, or payment institutions, among others.

In the case of Australia, within the FIU, there is a centralised team that focuses on remittance service providers.

[14] Only 11 out of 15 surveyed countries where *hawala* and other similar service providers are legal provided the information.

Figure 3.3 **Separate Team to Examine Regulated *Hawala* and Other Similar Service Providers (percentage of countries)**



Source: FATF project questionnaire.

3.5.2 SURVEY RESULTS: REGULATORY AND SUPERVISORY AUTHORITIES

In developing countries, the Central Bank is most of the time the supervisory authority for HOSSPs, while there is more diversity in the case of developed countries. Except for one country, the same agency is responsible both for regulation and supervision of the legal *hawala* and other similar service providers. Though the sample size is small, there are essentially four different institutional arrangements for the regulation and supervision of legal HOSSPs:

1. Central Bank
2. Financial Supervisory Authority (FSA)
3. Financial Intelligence Unit (FIU)
4. Others like Excise and Customs department, Department of Internal Affairs

Having the central Bank as the regulator and supervisor is the most common model in developing countries, as the Central Bank is the default supervisor for the whole financial market in addition to being one of the most established state agencies in these countries.[15]

The most common regulator and supervisor in developed countries is the Financial Supervisory Authority. In the case of Germany, Norway and Sweden, this authority is the sole regulator and supervisor for the legal HOSSPs. In the UK, the FCA (Financial Conduct Authority) regulates and supervises in cooperation with another authority, "H M Revenue and Customs".

In several countries, the FIU has been designated as the AML/CFT regulator and supervisor of legal *hawala* and other similar service providers – for instance Canada and United States. In the U.S., the FIU has delegated examination of HOSSPs to their tax authority. In Australia, all the AML/CFT supervision including those of *hawala* and other similar service providers is undertaken by the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian FIU.

All these various arrangements are outlined in Table 3.4.

15 See Todoroki, Noor, Celik, Kulathunga (2013).

Table 3.4 **AML/CFT Regulatory and Supervisory Authorities in Surveyed Countries**

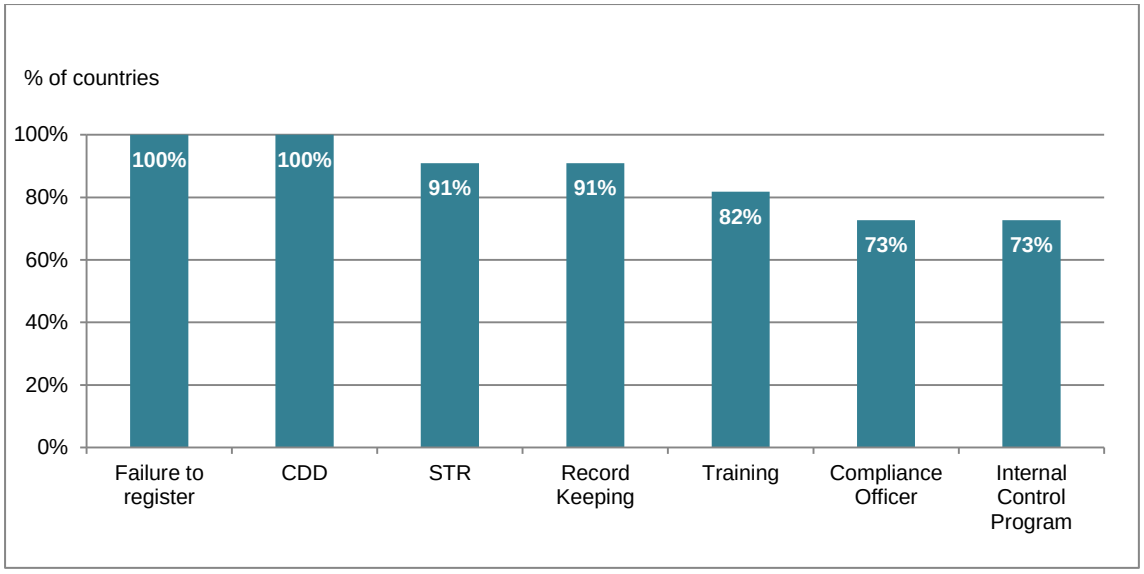
Countries	Regulatory Authority	Supervisory Authority
Australia	AUSTRAC (Australia's AML/CTF regulator and FIU)	AUSTRAC (Australia's AML/CTF regulator and FIU)
Germany	BaFin (Financial Services Authority)	BaFin (Financial Services Authority)
Republic of Guinea	Central Bank	Central Bank
Norway	Finanstilsynet (The Financial Supervisory Authority of Norway, FSA)	Finanstilsynet (The Financial Supervisory Authority of Norway, FSA)
Lebanon	Central Bank	Central Bank
Hong Kong	Customs and Excise Department	Customs and Excise Department
Slovenia	Central Bank	Central Bank, Office for money laundering Prevention
Netherlands	Central Bank	Central Bank
Sweden	Finansinspektionen (The Swedish Financial Supervisory Authority)	Finansinspektionen (The Swedish Financial Supervisory Authority)
New Zealand	Department of Internal Affairs	Central Bank
Indonesia	Central Bank	Central Bank
UK	HM Revenue and Customs, Financial Services Authority	HM Revenue and Customs, Financial Conduct Authority
US	FIU	FIU (HOSSPs examinations delegated to tax authority)
Canada	FIU	FIU

Source: FATF project questionnaire.

3.5.3 SANCTIONS APPLICABLE TO REGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS FOR FAILURE TO IMPLEMENT AML/CFT REQUIREMENTS

Survey results (Figure 3.4) highlight the range of compliance issues that can lead to sanctions applied to regulated *hawala* and other similar service providers (failure to register/become licensed; failure to comply with AML/CFT obligations such as CDD, STR, record keeping, training, compliance officer and internal control program) and the percentage of surveyed countries having such sanctions available.

Figure 3.4 **Sanctions for Failure to Implement AML/CFT Obligations (percentage of countries)**



Source: FATF project questionnaire.

Note: *Hawala* and other similar service providers are legal in 15 countries. Out of 12 FATF member countries where Hawala and other similar service providers are legal, 11 countries provided the data. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

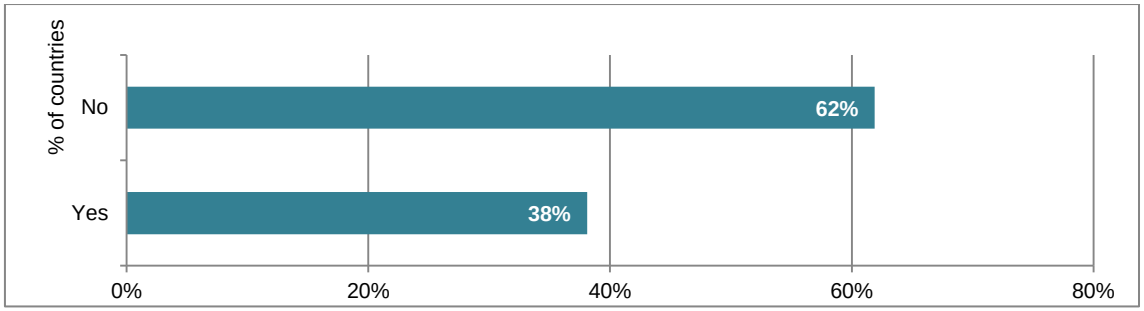
As *hawala* and other similar service providers are treated the same as any other remittance companies for the purpose of AML/CFT obligations, sanctions applicable to *hawala* and other similar service providers for failure to implement AML/CFT requirements are general provisions that apply to all MVTS whether they are called remittance companies, money service providers, or payment institutions. The questionnaire did not specifically ask whether sanctions are the same for all the financial institutions including MVTS or not, but some countries impose the same range and scale of sanctions for all the financial institutions while others have different scale and range of sanctions depending on types of financial institutions (for example, there are differences between banks and MVTS).

Though sanctions are applicable for failure to implement AML/CFT requirements in most of the countries, survey data pointed out that actual enforcement cases where sanctions were imposed against *hawala* and other similar service providers have been very few in most of the countries in the last five years.

3.5.4 REQUIREMENTS ON FOREIGN COUNTERPARTIES

Twenty one surveyed countries answered the question whether money transmitters in their countries can only deal with registered/licensed money transmitters in the ultimate recipient country and only eight out of these twenty one impose such a requirement (Figure 3.5).

Figure 3.5 **Requirement to Deal only with Regulated Money Transmitter in Ultimate Recipient Country (percentage of countries)**

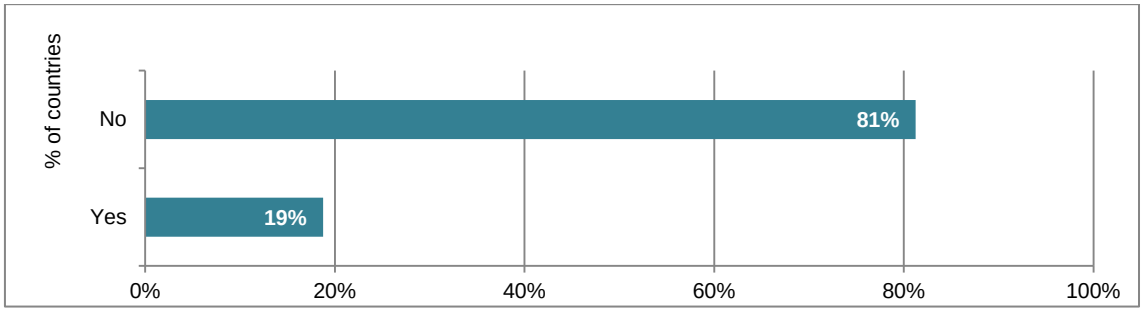


Source: FATF project questionnaire.

Note: Out of 25 FATF member countries, 21 responded to this question. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Only three out of the 16[16] countries that responded to the question whether "it is a requirement in their country that funds should be sent directly to the pay-out countries by the originating money transmitter." answered positively (Figure 3.6).

Figure 3.6 **Requirement to Send Funds Directly to Pay-Out Country by Originating Money Transmitter (percentage of countries)**



Source: FATF project questionnaire.

This would suggest that further discussion of Recommendation 13 in the context of money transmitters would be useful, in particular whether countries should interpret R13 to require that money transmitters, including *hawala* and other similar service providers, should only deal with licensed or registered foreign counterparties.

3.6 SUPERVISION AND ENFORCEMENT RELATED TO UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

This section discusses the survey results of the oversight of and enforcement against unregulated *hawala* and other similar service providers, sanctions against unauthorized money transmitters, as

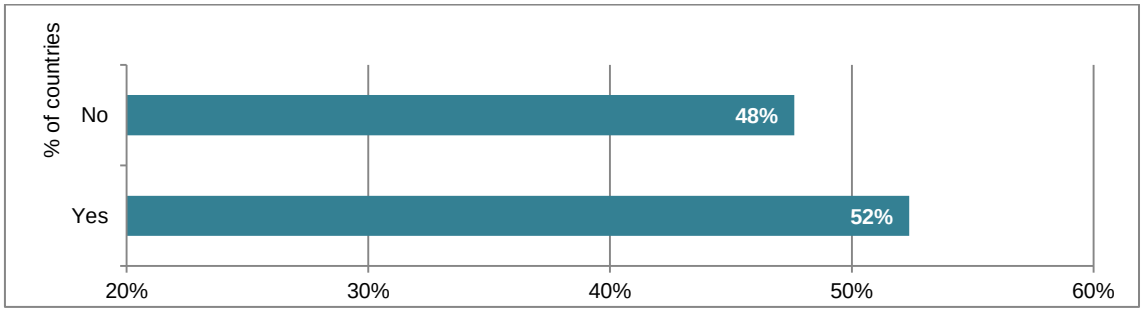
16 Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, 16 countries provided an answer to this question. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

well as various strategies used by countries to identify unregulated *hawala* and other similar service providers and steps taken to shift unregulated players to regulated channels.

3.6.1 IDENTIFICATION OF UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

A majority of surveyed countries have set up specific mechanisms to identify HOSSPs. Out of the 21[17] countries that provided answers to whether they have set up any mechanism to identify illegal *hawala* and other similar service providers in their country, a small majority provided a positive answer (eleven out of 21), see Figure 3.7. Many countries have not yet devised effective mechanisms to identify, monitor and take action as needed against illegal *hawala* and other similar service providers – either in terms of promoting their integration in the AML/CFT regime or cracking down on illegal operations. Given the vulnerabilities of unsupervised financial services providers, this lack of identification and lack of enforcement actions means that HOSSPs may remain a significant vulnerability.

Figure 3.7 **Taskforce to Identify Illegal Hawala and Other Similar Service Providers (percentage of countries)**



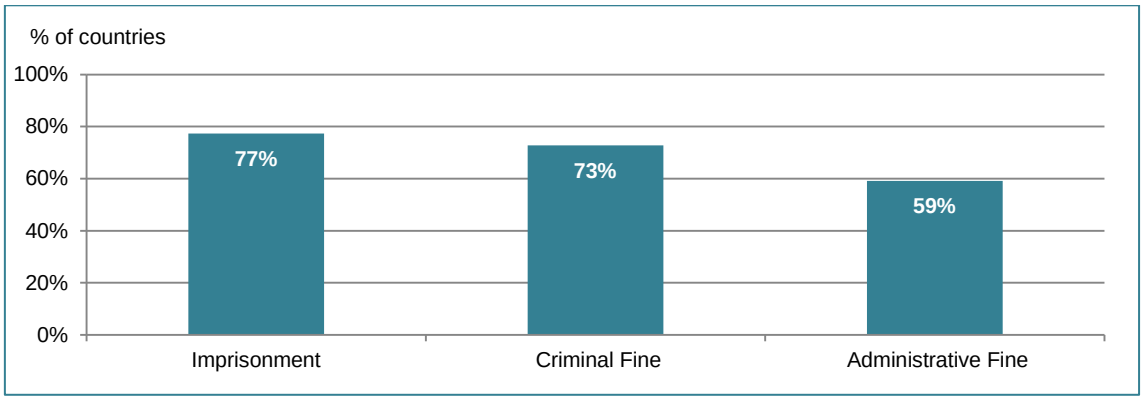
Source: FATF project questionnaire.

3.6.2 SANCTIONS AGAINST UNAUTHORISED MONEY TRANSMISSION OPERATIONS

Most countries have some form of sanctions available for unlicensed/unregistered money transmitters, but few surveyed countries appear to have used them. Surveyed countries indicate having both criminal and administrative sanctions available if HOSSPs keep operating as money transmitters without a license or registration after initial warnings. Most of the surveyed countries consider unauthorized operations as a criminal violation and apply sanctions such as imprisonment and criminal fines. As shown in Figure 3.8, in respectively 77% and 73% of the 22 countries that provided data, imprisonment and criminal fine can be imposed for unauthorized money transmission operations. In only 59% of the countries administrative sanctions are available.

[17] Only FATF member countries responded to this question. Out of 25 FATF member countries that responded, 21 countries provided an answer to this question. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Figure 3.8 **Sanctions against Unauthorized Operations (percentage of countries)**



Source: FATF project questionnaire.

Note: Out of 25, 22 FATF member countries provided the data on sanctions. This question was not included in the abbreviated APG questionnaire, therefore, no response from APG member countries.

Though sanctions are available, the survey shows that countries have not used them effectively against unauthorized operations in the last five years.

3.6.3 IMPORTANCE OF SUSPICIOUS TRANSACTIONS REPORTING OBLIGATIONS IN IDENTIFYING ILLEGAL *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS

Suspicious Transaction Reporting (STRs) can be a very effective tool in identifying illegal *hawala* and other similar service providers. The survey sought information on suspicious transaction reports (STRs) submitted by regulated *hawala* and other similar service providers or by banks on unregulated *hawala* and other similar service providers for the last three years. The majority of the surveyed countries were unable to provide the data, with only seven countries providing such statistics. For these countries, STRs filed by both regulated *hawala* and other similar service providers and banks on unregulated *hawala* and other similar service providers ranged from about eight reports per year to about 220 reports per year.

It is important that all types of money service businesses including regulated *hawala* and other similar service providers report promptly to the financial intelligence unit (FIU) or any relevant authority if they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing or related to unlicensed money remittance business. The information collected by FIU through STRs can be used by law enforcement agencies (or by supervisors) to conduct further investigations which can help identify illegal *hawala* and other similar service providers. STRs can be very useful technique to track down flow of money especially when banks and other financial institutions are used as a medium of settlement.

To improve STR reporting by regulated *hawala* and other similar service providers as well as by banks and other financial institutions on illegal *hawala* and other similar service providers, the regulatory authorities, in collaboration with the FIU, may issue specific guidelines. Such red flag indicators can be developed also in collaboration with MVTS players which can help detect suspicious transactions.

Box 3.1 **Guidance to Financial Institutions on Red Flag Indicators and Case Studies Leads to Increased STR Filings**

In September 2010, the United States Financial Intelligence Unit FinCEN published an advisory on informal value transfer systems (IVTS) to U.S. financial institutions, including recent case typologies. The advisory asked filers to include the term "IVTS" in SAR narratives to report IVTS related activity. Following publication of the Advisory, STR filings referencing IVTS increased over 500%. In October 2011, FinCEN published an analysis of STRs referencing IVTS. How many of the STR filings involved actual hawala and other similar service providers have not been determined. The findings were as follows:

a. Currency exchange and unregistered money transmissions dominate STR filings: 57% of filings referenced suspicious currency exchange, while 30% referenced unregistered Money service businesses (MSB) activity (with unregistered currency exchange being the leading cause). 48% of the suspicious currency exchange activity referenced Venezuela, Argentina, Brazil, and Mexico. While 89% of STRs before the advisory referenced Latin America, only 41% of post-Advisory STRs did. Post-advisory transactions involving exchange houses in the UAE, Jordan, and Kuwait, Yemen, and Iran were common.

b. For the subject location, over 49% (1 019 subjects) were associated with foreign addresses, almost 40% of them in Venezuela. Over 90% of New York filings reporting possible unregistered money services business activity involved convenience/grocery stores and the Middle East.

Source: United States.

3.6.4 INDICATORS TO DETECT SUSPICIOUS HAWALA AND OTHER SIMILAR SERVICE PROVIDERS

This sub-section provides guidance on transactions patterns that are often associated with illegal/unregulated money transfer providers, including *hawala* and other similar service providers. These transaction patterns can be identified through effective monitoring and CDD mechanisms and should often raise suspicions by the financial or reporting institutions. Such suspicious transaction patterns include:

1. Extensive use of collective accounts. These can be identified by the reporting institutions if lots of small sums are deposited into the bank account of individuals (often stating their name in the reference line), or if large cash sums are deposited at regular intervals before transfers aggregating all of the smaller amounts from the account are made to foreign accounts. Indicators of such collective accounts can be individuals possibly organized under the aegis of a cultural association collecting money through banking system, or one or more individuals making an aggregated transfer of a large sum of money to a bank or money remitter abroad.
2. Money being transferred at regular intervals to international locations such as Dubai. Dubai is a major international clearing house for remittances and other value transfers. Many trading companies/criminal groups route their money through Dubai to other destinations through *hawala* channel. Most of the hybrid *hawala* transactions are routed through some major international destination such as Dubai.

3. An account been used as a temporary repository and the funds are transferred in and out of the account immediately.
4. Usage of third party accounts to disguise and to avoid detection by authorities. Often such third party accounts have no business connection to the *hawaladar* or sender.
5. Frequent wire transfer activity from an account in sending country to international bank account.
6. Wire transfers frequently sent by traders to foreign countries, which do not seem to have any business connection to the destination countries.
7. Money remitter or trader conducting transactions such that they fall beneath the identification, STR or CTR reporting threshold.
8. Business accounts used to receive or disburse large sums of money but show virtually no normal business related activities such as payment of payrolls, invoices etc.
9. Frequent deposits of third party checks and money orders into business or personal accounts.
10. Frequent international wire transfers from bank accounts which appear inconsistent with stated business activities.
11. Frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
12. Sudden change in pattern of financial transactions from low value international fund transfers to large value transfers by a money remitter.

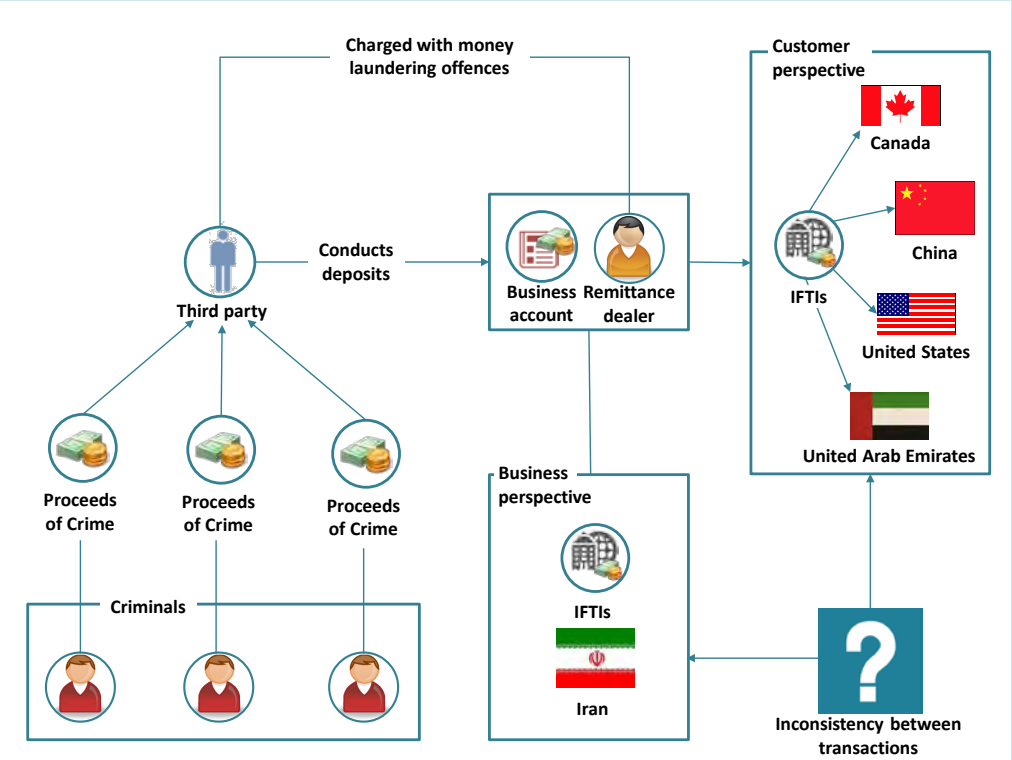
Box 3.2 **Case Study: Money laundering revealed through transaction patterns of the remittance dealer – "Suspicious Transactions"**

AUSTRAC's (Australian Transaction Reports and Analysis Centre) monitoring systems identified a substantial increase in cash activity undertaken by a remittance dealer. Further analysis identified significant inconsistencies between the information the remitter had reported to AUSTRAC, and the information reported by the financial institutions where the remitter was a customer.

This information was referred to the Australian Crime Commission's (ACC) Financial Intelligence Assessment Team (FIAT). After the AUSTRAC referral, the FIAT undertook further investigations and disseminated the intelligence to the Australian Federal Police (AFP), who conducted the investigation. As a result of the investigation two suspects were charged with money laundering offences under the Criminal Code Act 1995. One of the suspects was the remittance dealer, while the second suspect, an associate of the first suspect, allegedly acted on behalf of third parties to deposit large amounts of cash into accounts owned by the remittance dealer.

This investigation was triggered by recognized money laundering indicators. AUSTRAC data revealed significant discrepancies between the transactions reported by the remittance dealer from its own 'business' perspective, and the transactions reported to AUSTRAC by the financial institutions which dealt with the suspect remittance dealer as a customer (that is, transactions

reported from a 'customer' perspective).



Transaction reporting information received by AUSTRAC revealed a number of significant and suspicious changes in the financial transaction patterns of the remittance dealer involved:

- The remittance dealer's activities changed from facilitating small outgoing international funds transfer instructions (IFTIs), to accepting large cash deposits and facilitating large IFTIs. This spike in financial transaction activity was clearly inconsistent with the remitter's previous profile and history.
- Shortly after this increase in the size of IFTIs, business bank accounts held by the remittance business stopped receiving deposits. However, AUSTRAC analysts identified additional accounts operated by the remittance business, which had been opened under a new company name. Under this new company name, the remitter's business practices appeared to change. While the remitter continued to report to AUSTRAC that the majority of its remittances were being sent to Iran, information received from institutions dealing with the remitter as a customer reported that a significant proportion of the business's outgoing IFTIs were now being sent to the United Arab Emirates (UAE).
- The remitter's transaction activity continued to escalate while operating under the new company name. Over a three-month period the remitter recorded cash deposits of AUD34 million and outgoing IFTIs of AUD33 million. At the peak of activity, the remitter was receiving cash deposits into its bank account of AUD1 million each day, and on one occasion received almost AUD4 million in two days. The third party making these large cash deposits made no attempt to conceal them, and they were conducted at the same bank branch.
- Information provided by reporting entities was also invaluable in highlighting discrepancies in

the remitter's activities. The value of the remittance dealer's business activity as reported to AUSTRAC was significantly less than that reported by the financial institutions that dealt with the remitter as a customer. This discrepancy in reporting strongly suggested to authorities that the remittance dealer was dealing with proceeds of crime, rather than funds generated by legitimate business activities.

The following table highlights the discrepancies in the remitter's transaction activities as reported from customer and business perspectives, over a 10-month period:

Transaction Types	Value as reported by the remittance business (*i.e.*, from the "business perspective")	Value as reported by reporting entities dealing with the remittance business (*i.e.*, from the "customer perspective")	Difference
Cash deposits recorded in TTRs	AUD 48 million	AUD 92 million	AUD 44 million
Outgoing IFTIs	AUD 55 million	AUD 95 million	AUD 40 million

As the remitter's cash activity escalated, law enforcement agencies executed warrants against the syndicate and stopped its operations. The AFP arrested two individuals, and restrained AUD1.2 million. While the original source of the funds could not be established, the large amount of cash involved led authorities to suspect that the funds were the proceeds of crime.

Source: Australia.

3.6.5 STRATEGIES TO IDENTIFY UNREGULATED *HAWALA* AND OTHER SIMILAR SERVICE PROVIDERS AND POSSIBLE AVENUES TO CREATE INCENTIVES TO FORMALISE THEIR BUSINESS

There are many different strategies and techniques used by countries to identify illegal *hawala* and other similar service providers [18]. Many of those are used in combination.

Some of the most common methods used to detect such operations are:

1. identifying advertisements placed by such businesses in community newspapers,
2. conducting internet search,
3. searching through social media,
4. following up on leads from general public or service providers,
5. use of AML monitoring systems especially leveraging on useful indications originating from STRs filled by financial institutions,
6. working in partnership with other agencies and gathering information from law enforcement and AML regulatory authority's investigations and inspections and
7. specific targeted investigations and physical surveillance of suspicious entities.

[18] See also FATF (2003).

It is important for countries to foster close co-ordination within the relevant authorities for the purpose of developing inter-agency strategies and efficiently utilizing the available resources to identify illegal operators.

Box 3.3 **Specific strategies used by some surveyed countries to identify illegal hawala and other similar service providers**

Australia: AUSTRAC (Australia's FIU and AML/CTF regulator) along with relevant law enforcement and intelligence agencies identify illegal hawala and other similar service providers. AUSTRAC has an extensive transaction reporting regime entailing threshold transactions reports (TTRs), International Funds Transfer Instructions (IFTIs) and Suspicious Matter Reports (SMRs). The use of transactions reports is one of the mechanisms that are used to highlight potential illegal remittance service providers; particularly those using the banking systems to bulk settle transactions. In addition, AUSTRAC's supervision teams engage with various ethnic communities who may provide useful intelligence about the illegal operators. There have been instances where regulated remittance businesses have provided information in relation to the operation of unregulated remittance businesses.

Malaysia: A surveillance team has been formed within the Central Bank to identify unlicensed money services business (MSB) operators, generally based on public tip off and information from the licensed MSB operators. The surveillance team is also increasingly moving towards gathering its own intelligence to detect illegal hawala and other similar service providers through collaboration with the Financial Intelligence and Enforcement Department and MSB supervision team, as well as information from the internet and public database (such as company registry etc.).

Austria: Awareness training programs for the financial sector, the non-financial sector, law enforcement and supervisory authorities are organized in order to raise awareness as regards the way hawala and similar unregulated value transfer systems work to facilitate the process of cracking down illegal money transfer businesses including hawala and other similar service providers.

United States: The Department of Homeland Security's Homeland Security Investigations (HSI) runs the Cornerstone Initiative to identify illegal operators including HOSSPs. The Cornerstone Outreach Initiative seeks to: 1) Identify the means and methods used by criminals to exploit financial systems in order to transfer, launder and otherwise mask the true source of criminal proceeds, 2) Works with specific private sector industries to gather new information and reduce vulnerabilities found within existing financial systems and 3) Investigate and prosecute criminal organizations exploiting traditional and non-traditional financial systems.

In 2010, HSI published a Cornerstone report dedicated to HOSSPs. The Cornerstone Report is a public facing document and is a mechanism by which private partner sectors are informed about risks of dealing with various players in the market; the sharing of information allows the financial, trade, and retail communities to take precautions in order to protect themselves from exploitation.

The FBI makes extensive use of the over 1 million STRs filed each year in the US to identify HOSSPs. HOSSPs are also identified through linkages with FBI cases and leads from the Joint Terrorism Task Force.

Source: Country Authorities, FATF project questionnaire.

Box 3.4 **FinCEN's Unregistered Money Service Business Outreach Initiative**

FinCEN, the U.S. FIU, has adopted a strategy to identify unregistered money services businesses (MSBs) and coordinate appropriate regulatory actions. FinCEN aims to reduce the number of unregistered MSBs that should be registered by using information from Suspicious Transaction Reports (STRs) and other FinCEN data to assist in identifying these businesses. Once identified through analysis of STRs and other data, institutional outreach is conducted to raise awareness of BSA requirements for MSBs, including registration.

FinCEN data is regularly searched using special search terms (e.g., "unlicensed," "unregistered," "illegal") to identify potential unregistered MSBs named as subjects in STR filings. The FinCEN database is further queried to determine whether any additional FinCEN data exists on the subject(s), and FinCEN's MSB Registrant Search web site is also queried to determine whether they are currently registered. All subjects are also reviewed prior to outreach to identify recent or on-going investigations for determination of whether or not they should be contacted. As a result of FinCEN's July 2011 re-definition of MSBs that included foreign-located entities, foreign-located entities that may be required to register with FinCEN will now be identified for purposes of outreach as well.

An entity identified for outreach is contacted to learn more about the types of activities the entity conducts that may make it an MSB, in order to determine whether the entity must register and to assist it in the registration process. Depending on the outreach results, cases may be referred for possible BSA examination or for possible enforcement actions.

Source: United States.

Box 3.5 **Dutch Migrant Study on Payment Channels**

One potential method to better understand which payment methods remitters prefer and why is through a survey. For instance, The Netherlands Central Bank in April 2013 published a paper investigating the determinants in migrants' choice of payment channels when transferring money to relatives abroad. The paper's authors surveyed 1,680 migrants in the Netherlands and identified five remittance channels: bank services, money transfer operator services, in-cash transfers via unregulated intermediaries, ATM cash withdrawals abroad and carrying cash when travelling home. The survey identified that migrants who regularly used internet banking for other purposes were more likely to use bank services for remittances as well. The paper also found that other drivers exist in determining the choice of payment channels used, such as personal characteristics and country-specific factors, costs (real and perceived), ease of use and availability of remittance transfer options. The paper concluded that financial education, cost reduction, and mobile remittance solutions could expand use of regulated channels.

Source: Kosse, Ameka and Vermeulen, Robert (2013).

Box 3.6 **UK Project QUAVER**

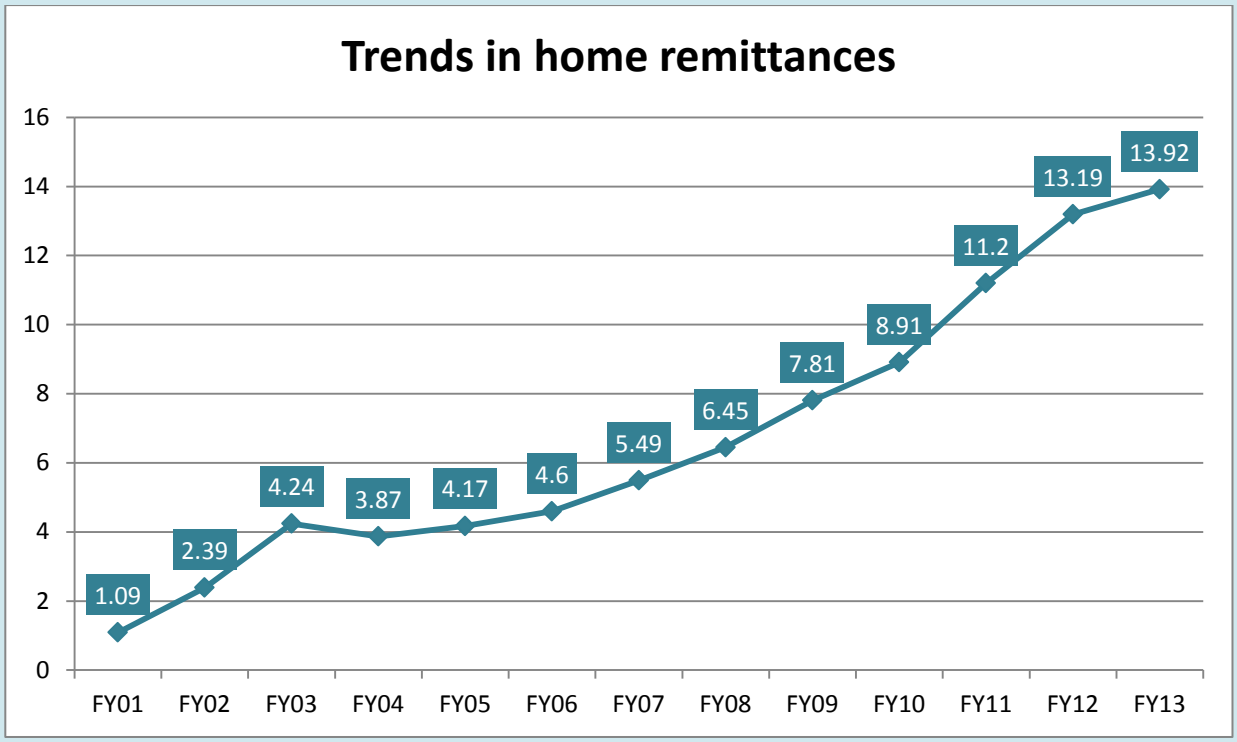
In the UK, all HOSSPs are defined by law as money service businesses (MSB) and are regulated and supervised as such, but are still subject to widespread exploitation by criminal groups. Law enforcement and regulatory bodies have for the last two years been co-operating closely on Project QUAVER, an initiative designed to minimize this criminal exploitation. The project focuses on the communication of commonly seen criminal techniques to the MSB sector, Banks and other financial institutions, designed to improve understanding and facilitate a better appreciation and management of risk in the regulated sector and, accordingly, enhanced compliance with AML/CTF requirements. In addition Serious Organized Crime Agency (SOCA) has been educating regulators and law enforcement colleagues and advising them on how to best approach criminal prosecutions of complicit HOSSPs; the UK has a number of trained Expert Witnesses in money laundering and has delivered similar expert evidence training to colleagues from the USA, Australia and the Netherlands.

The reaction to the project has been positive, with a number of banks and other financial institutions (including large scale MSBs providing payment services for other MSBs) displaying an improved attitude to risk, for example, by closing high risk bank accounts, refusing to carry out third party payments, and by insisting on independent audits of the processes of MSB customers; in addition, a number of MSBs have changed their business practices and are now unwilling to carry out the type of transactions favoured by criminal HOSSPs. The quality and number of Suspicious Activity Reports submitted by businesses in the regulated sector has also increased significantly.

Source: United Kingdom.

Box 3.7 **Pakistan Remittance Initiative (PRI)**

One possible model for moving remittances into regulated channels is the Pakistan Remittance Initiative. A sharp jump had been witnessed in inbound remittances to Pakistan after Financial Year (FY July- June) 2001 as home remittances rose from USD 2.3 billion in FY01 to USD 4.2 billion by FY03 (Figure 1). However, these inflows moderated in subsequent years and reached USD 13.92 billion by FY13. There was increasing realization that a substantial part of these inflows are routed through unregulated channels. Initially, State Bank of Pakistan made policy interventions in the FX market to discourage hawala/hundi system in the country. These efforts helped resume an uptrend in home remittances. Accordingly, in order to provide an ownership structure in Pakistan for remittance facilitation, State Bank of Pakistan, Ministry of Finance and Ministry of Overseas Pakistanis launched a joint initiative called Pakistan Remittance Initiative (PRI) in April, 2009. This initiative has been taken to achieve the objectives of (a) facilitating and supporting efficient flow of remittances and (b) leading to provide investment opportunities in Pakistan for overseas Pakistanis.



At the outset of the drive, a comprehensive objective analysis of the Home Remittance System was carried out with a view to; collect and analyse remittance related data, identify the bottlenecks and weak links in the system, review the recent international efforts on remittances specially in the global and regional perspective, evaluate schemes implemented earlier to enhance remittance flows to Pakistan, and compile practices followed by various jurisdictions to boost remittances. The subject analysis led PRI to formulate a comprehensive strategy aimed at greater commitment of financial sector towards remittance services and resultant inculcation of remittance culture, transparency of remittance market with adequate consumer protection, efficiency of payment system infrastructure, and incentives for the remitters, beneficiaries and overseas entities. These were the basic ingredients to compete with the unregulated channels and provide quality, fast, efficient, cheap and safer services to remitters and beneficiaries through regulated channels.

Through a consultative process, the number of financial institutions involved in remittance services has increased significantly. The realization of business cases in remittances by additional financial institutions has not only facilitated the larger strata of remittance beneficiaries but also resulted in creating a more competitive environment.

PRI is encouraging financial institutions in Pakistan to enhance their outreach worldwide through new remittance- specific related arrangements. Around 400 new arrangements have been finalized by banks in Pakistan with their overseas correspondents since the inception of PRI.

Reliable and efficient payment systems are vital to facilitate delivery of home remittances securely and efficiently and State Bank of Pakistan has already taken number of steps to develop related Payment Systems Architecture of the country.

- Utilization of PRISM (RTGS) to transfer and settle inter-bank Home Remittance transactions. This has enabled banks to transfer inter-bank transactions into beneficiaries' accounts on the same day.

- Apart from RTGS, through ATM Switch, instant A/C credit facility is also available for beneficiaries through IBFT Inter Bank Fund Transfer. This has reduced turnaround time considerably.

Keeping in view of the rising trend in the Home Remittances and importance of the same for the economy, SBP has allowed banks to open dedicated Home Remittance payment centres. Payments can be made to beneficiaries via cash, demand drafts and pay orders. In addition, such Home Remittance Payment Centres would also be allowed to perform the functions of Sales & Service Centres.

In order to provide a reliable and immediate contact point, 24 hours, 7 days a week; a call centre has been established by PRI. All overseas Pakistanis and their families back home can inquire about the remittance services of banks and lodge their complaints with the call centre (0092-21-111-222-774). There are toll free numbers for overseas Pakistanis residing in 12 countries/ regions of the world. Further PRI has its own website http://www.pri.gov.pk for related purposes.

With a view to encourage and to protect the remitters / beneficiaries from any losses that they may incur due to unwarranted delays in receipts of funds in the beneficiaries' accounts, the beneficiary shall be entitled to a return of sixty five (65) paisa per thousand rupees per day from the concerned bank for the number of days credit/payment on account of remittance was delayed.

PRI have organized various training programs related to various facets of remittances services ranging from strategic framework for remittance services to policy level initiatives. PRI also awarded appreciation certificates to top performer branch managers of banks in recognition of their services for the national cause.

International Association of Money Transfer Networks (IAMTN) has awarded Pakistan Remittance Initiative (PRI) with Money Transfer Award 2011 for the category of 'Asia Pacific Including South Asia' and the same has been presented during the ceremony held on November 15, 2011 in London. This award was conferred in recognition to the efforts being made by the PRI to facilitate the flow of remittances through regulated channels to Pakistan.

At the moment, all PRI efforts are aimed at bringing structural changes in the Remittance System of the country with a long-term vision about these recurring flows. It is a daunting task to introduce changes in the decades old systems and procedures with a strongly embedded particular mind-set of the stakeholders involved. The task becomes more difficult in wake lack of financial literacy, perceptual barriers and volatility of exchange rates. Notwithstanding to the impediments, PRI is geared up to achieve its objective of maximizing the flow of remittances through regulated channels in the country.

Source: Pakistan.

3.7 INTERNATIONAL COOPERATION RELATING TO HOSSPS

International cooperation is an important key component to ensure effective oversight of HOSSPs necessary to mitigate the risk of HOSSPs being exploited for money laundering and/or terrorist financing. HOSSPs often transfer funds or their equivalent in value across borders and an evidential or intelligence picture cannot be obtained by one country's authorities without the open exchange of information between all the other countries in which the HOSSPs has a presence. Unfortunately,

few examples of international cooperation were provided in the responses to the survey, likely due to lack of training and expertise of law enforcement or other competent authorities related to HOSSPs.

Box 3.8 **International Controller Investigation**

In 2006, as a result of international co-operation with the Spanish authorities in respect of a UK citizen resident in Spain who was believed to be involved in drug trafficking and money laundering, the UK authorities identified a prolific International Controller operating from Dubai. In the course of UK Operation OVERGO, Dubai Police Operation CANCER and Italian Guardia de Finanza Operation KHYBER PASS it was identified that this person was using a number of Dubai registered trading companies to launder money on behalf of criminal networks in numerous jurisdictions including the UK, the USA, Italy, Albania, India and Colombia.

After a lengthy investigation involving extensive mutual co-operation and evidence gathering between the authorities in Dubai, the UK, the USA and Italy, the Dubai Police arrested the Controller in early 2007, but released him from custody a short while later. On the same day, the Italian authorities arrested further members of the Controller's network, and subsequently issued a European Arrest Warrant for the Controller himself.

The Controller subsequently left Dubai and moved his activities to India, however following further international co-operation between the authorities in the USA and India, including the freezing of several million dollars in bank accounts linked to the Controller, the Indian Enforcement Directorate commenced an investigation and subsequently instituted proceedings for Foreign Exchange and money laundering offences against the Controller; these proceedings are on-going.

Source: UK Authorities.

Box 3.9 **Unlicensed Money Transmitter Investigations**

Case 1.

In August 2010, HSI San Francisco began investigating a U.S. based trading company (TC) suspected of operating as an unlicensed money transmitting business sending funds to Iran. Bank Secrecy Act (BSA) information disclosed wire transfers from high risk countries, as well as businesses previously identified as possibly transmitting funds to Iran in violation of OFAC sanctions. A review of bank accounts disclosed transactional activity consistent with the operation of a Money Service Business (MSB). This activity showed incoming wire transfers from suspect "Trading Companies" followed by pay-outs to individuals with no apparent logical business connection. Further investigation revealed that none of the business or individuals involved in these transactions had a license from the Financial Crimes Enforcement Network (FinCEN) or Office of Foreign Assets Control (OFAC) to transmit money and funds were being sent to/from Iran. It was discovered that the group utilized international wire transfers through a variety of overseas businesses located in the UAE, China, Sweden, and Korea to circumvent existing OFAC regulations. Once these funds were deposited into U.S. bank accounts, the funds would be paid out to other Iranians living in the U.S., or a CPA would "layer" the funds through other US bank accounts owned or controlled by the organization all in an effort to hide it from the Internal Revenue Service. In May 2012, a plea

agreement was reached for one count of Title 18 USC § 1960 and one count of 50 USC §1702 (IEEPA). The business owner later agreed to cooperate with the government admitting that he had worked with family members in Iran as well as an Iranian HOSSP to supply money transmitting services. As part of the plea agreement, it was disclosed how front companies worldwide and HOSSPs were used in conjunction with trade to circumvent OFAC sanctions.

Highlights of International Cooperation: Through numerous HSI Attaché Offices, investigative leads were coordinated with law officials from Afghanistan, the UAE and additional partner countries.

Source: United Kingdom.

Case 2

ZSQ Exchange was a HOSSP operating out of Fremont, California which had transmitted millions of dollars all over the world through a complex system of wire transfers, emails, faxes, commodity exchange and traditional hawala services. Bank Secrecy Act (BSA) documents associated with ZSQ Exchange and the owner, Qader QUDUS, indicated that over a one year period, more than USD 1.2 million dollars was deposited into Qudus' bank accounts. These deposits were followed by wire transfers to various individuals in the Middle East, Pakistan, China, Europe and Japan. A joint HSI, FBI and DEA investigation was conducted with a Confidential Informant (CI) infiltrating a Pakistani-based heroin trafficking organization operating in Maryland. The CI purchased two kilograms of heroin and was instructed to send payments through five separate bank accounts located in New York, San Francisco and Pakistan. The heroin proceeds eventually ended up in the hands of a Pakistani heroin trafficker identified as Momin KHAN-AFRIDI of Peshawar, Pakistan. KHAN-AFRIDI was known by the DEA to be a large-scale heroin and multi-ton hashish trafficker. KHAN-AFRIDI is responsible for heroin distribution throughout the United States, United Kingdom, Thailand, and Canada. The U.S. Treasury Department, Office of Foreign Assets Control (OFAC) designated Khan-Afridi as an international narcotics trafficker. (It was alleged that proceeds from the sale of heroin in the U.S. was commingled with refugee relief money and intelligence sources indicated that some of this narcotics money was being used to finance Al-Qaeda.) Qader QUDUS pled guilty to operating an unlicensed money transmitting business in violation of Title 18 USC § 1960, in the United States District Court, Northern District of California. QUDUS was sentenced to 27 months in prison and ordered to forfeit USD 406 640 to the U.S. Government.

Highlights of International Cooperation - An Internet web site for ZSQ Exchange was discovered identifying ZSQ as a HOSSP. The web site explained how money was to be deposited and identified the bank used and provided the names and address of ZSQ's overseas offices in Kabul, Peshawar, Islamabad, Quetta, Lahore, and Karachi. Bank records revealed numerous wire transfers from ZSQ Exchange to businesses and individuals in thirteen different countries, the majority of which were sent to Japan, China, and Hong Kong. Collateral leads were sent to our HSI attachés in London, Paris, Hong Kong, China, Netherlands, Germany, and Russia.

The UK Metropolitan Police began an investigation to assist HSI London. Japanese police interviewed an individual who received a large number of wires transfers from ZSQ. The individual, a former Mujahedeen General, stated that ZSQ is used to settle large financial transactions between terrorist organizations.

Source: United States.

3.7.1 REGULATOR TO REGULATOR COOPERATION

In order to understand fully the regulatory position of HOSSPs, it is important that the regulators in individual countries are able to share information about the regulatory status of companies that they supervise, and the legal framework under which they are obliged to operate. In order to facilitate this and to allow banks to determine whether HOSSPs are legally licensed or registered before providing banking services, a number of countries make these details available on line. This is the case in Pakistan, United Kingdom, United States, and others. This can be helpful when considering if an unregulated HOSSP has been used for part of the transaction. A transaction may be commenced in accordance with the regulations in the host state, but it may be settled using an operator that is illegal in the destination state. In such cases, there is a greater possibility that the unregulated HOSSP could divert the funds at a later stage and use them for other purposes, such as the payment of an unrelated business transaction between two third parties, as they pass through another jurisdiction, and not be caught.

Alternatively a transaction may be commenced by regulated entities, such as through the banking system at the 'first mile,' but may be paid out by unregulated entities. This is typically seen with remittances from European countries and the United States to Somalia, which are generally initiated with a licensed or registered money transmitter receiving customer funds and remitting them via the banking system to associated companies in the UAE, after which point the UAE companies connected to the international clearinghouse operations of the money transmitters use the funds to purchase goods for export into Somalia, with the ultimate settlement of the transaction being made from the proceeds of the sale of the goods there.

Box 3.10 **EU Passporting System**

In the EU, businesses conducting remittance activity are required to comply with the terms of the EU Payment Services Directive (full title Directive 2007/64/EC on payment services in the internal market). This directive is enacted into law in the domestic legislation of each of the EU member states. The main purpose of the directive is prudential, *i.e.,* to ensure that anyone using payment services in the EU has their money protected by a single legal framework.

Amongst the provisions of the directive is one which allows a business that is regulated in one member state to carry out payment services in another without the need to be supervised by the regulator in that state. This is known as 'passporting'. In such circumstances it is essential that, in order to adequately fulfil their regulatory responsibilities, the regulatory bodies in each country into which the business passports enter into an open information sharing agreement with the authorities in the host country.

Source: European Commission (2007).

3.7.2 EGMONT REQUESTS

The Egmont Group of Financial Intelligence Units was formed in 1995 with the aim of providing a forum for financial intelligence units around the globe to improve international co-operation in combating money laundering and terrorist financing. The group currently has 139 members. Amongst other things, the group facilitates the exchange, on an intelligence only basis, of

information and intelligence relating to suspected offences impacting the group member states. This information exchange takes place between the FIUs in the relevant jurisdictions. It also publishes information relating to typologies and indicators of criminal activity, including fraud, money laundering and terrorist financing identified in the course of its co-ordination activities.

Sharing information in this manner has led to numerous examples of persons being convicted of offences in their country of residence where information received from an overseas FIU generated a new and significant line of enquiry.

Box 3.11 **Egmont information sharing**

An African national residing in a European country (Country Z) declared that he performed hawala banking activities. His account was exclusively credited by cash deposits and numerous transfers for small amounts.

Over the course of several months the funds were transferred to company A in Africa. Shortly thereafter the funds were transferred to company B in Country Z. Companies A and B performed international money remittance services. According to the subject, he performed hawala activities for fellow countrymen wishing to send money to Africa. However, he did not hold any position within companies in country Z where he executed the transactions and he was not registered as a representative of an authorized exchange office.

Police enquiries revealed that he was known to be a member of a terrorist organisation and it is thought that this alternative remittance system may have been used for terrorism financing.

Source: Egmont group website – www.egmontgroup.org/library/cases.

3.7.3 JOINT INVESTIGATION TEAMS (JITS)

A Joint Investigation Team is an investigation team set up for a fixed period, based on an agreement between two or more European Union member states and/or competent legal authorities for a specific purpose. Non EU member states can also participate in a JIT with the agreement of all other parties. The concept of JITs is set out in Article 13 of the 2000 EU Convention on Mutual Legal Assistance.

JITs are specifically geared towards assisting EU member state law enforcement and judicial authorities tasked with instigating complex investigations into organized crime groups, by virtue of which cross jurisdictional serious criminality can be tackled by different Law Enforcement agencies and Prosecutors working in single teams. The JIT is usually set up in the member state in which the investigation begins.

Europol, the European Law Enforcement Agency, and Eurojust, the European Union's judicial co-operation unit, assist in the setting up, implementation and conduct of JITs. In addition, Eurojust, can provide legal advice to member states engaging in JITs.

The key advantages of a JIT are:

- No requirement for international mutual legal assistance requests
- Intelligence and evidence sharing between JIT members. Such evidence can be used in court

- Members of the JIT can be present at house searches, interviews of suspects and other associated areas of operational activity in all jurisdictions covered.

Funding for the establishment of JITs is available from Eurojust. This funding is available for reimbursing travel costs, accommodation, translation and interpretation; in addition, Eurojust can fund/host operational meetings.

3.7.4 MUTUAL LEGAL ASSISTANCE (MLA)

In contrast to Egmont requests, which allow for the sharing of information for intelligence purposes only, MLA requests are required (although not in all circumstances) when the authorities in one country wish to gather, or have gathered, material in another country which will be required to be used as evidence in criminal or other proceedings.

MLA requests are generally required when a request for evidence to be gathered in another jurisdiction requires some form of judicial oversight, a degree of coercion or the invasion of privacy; for example when a request is made for the obtaining of evidence by questioning of a suspect after arrest, the search of a premises under warrant, or a judicial order for the production of information, such as banking or other information held under the presumption of confidentiality.

MLA requests can result in certain types of evidence being obtained and used in one country that would not be permissible under that country's domestic legislation; for example, transcripts of telephone intercepts conducted outside the UK are in certain circumstances admissible as evidence in UK courts, even though the law in the UK explicitly excludes the use of such material gathered in the UK as evidence.

MLA requests are issued by the competent legal authority in one jurisdiction on the application of either a prosecuting authority or, where proceedings have been instituted, on behalf of the person charged. The judicial authority can only issue an MLA requests if it appears to them that an offence has been committed, or if there are reasonable grounds for suspecting that an offence has been committed, and that proceedings in respect of the offence have been instituted, or the offence is being investigated. The nature of the assistance sought must be specified in the request, as must the use to which the resulting information is to be put.

Whilst MLA requests have a vitally important role in supporting prosecutions of HOSSPs, it is frequently the case that, for various reasons, such as for example a simple lack of resources, or because the requesting country does not fully understand the legal requirements of the receiving country for dealing with such requests, that the servicing of the request by the receiving country is delayed (on occasions the results can be received after the conclusion of proceedings). This can have significant implications for the prosecution in the country issuing the MLA requests, ranging from the proceedings being delayed, to vital evidence being unavailable during court proceedings. Regular and on-going communication between the authorities in the issuing and receiving countries is therefore vital during the MLA requests process.

Ironically delays in the MLA requests process can work to a defendant's advantage as there are numerous cases whereby a defendant's legal team has been able to adduce evidence gathered in an

overseas jurisdiction, due to them not having to follow the MLA requests procedure, when an MLA requests in respect of similar prosecution evidence has been held up by judicial procedures.

BIBLIOGRAPHY

European Commission (2007), *Directive 2007/64/EC on payment services in the internal market*, EU Payment Services Directive.

FATF (2003), *Combating the Abuse of Alternative Remittance Systems: International Best Practices, June 2003,* OECD, Paris.

Kosse, Ameka and Vermeulen, Robert (2013), *Migrants' Choice of Remittance Channel: Do General Payment Habits Play a Role,* DNB Working Paper, No. 375, April 2013.