Alternative Remittance Systems and Terrorism Financing

*Issues in Risk Management*

*Matteo Vaccani*
Alternative Remittance Systems and Terrorism Financing

Issues in Risk Management

Matteo Vaccani
Contents

Foreword ................................................................. iv
Acknowledgments .......................................................... v
Acronyms and Abbreviations ........................................ vi
Author’s Biography ......................................................... vii
1. Introduction ................................................................ 1
2. Anatomy of the System .................................................. 3
3. Vulnerability to Terrorism Financing ................................. 7
4. Risk Mitigation Measures ............................................... 13
   Detecting Informal ARS .................................................. 14
   The Debate on Licensing and Registration ......................... 16
   The Essential Role of Enforcement ................................ 18
5. Conclusion .................................................................. 21
Appendix. ARS Settlement Models ...................................... 23
   Reverse Transaction ..................................................... 23
   Bilateral Financial Settlement ......................................... 24
   Multilateral Financial Settlement ..................................... 24
   Bilateral Trade ............................................................. 25
   Multilateral Trade ........................................................ 25
   Under/Overstatement of Trade Values ............................... 27
   Smuggling .................................................................. 27
References ...................................................................... 28
Figures
Figure 2.1. Basic ARS Transaction Model ......................... 3
Figure 3.1. Ranjha Case Alleged Transfer Network, 2004–2007 ....... 9
Figure 4.1. Remittance Inflow Recurring Patterns, 1994–2007 ........ 15
Figure A.1. Offsetting Transaction Settlement .................... 23
Figure A.2. Bilateral Financial Settlement ............................ 24
Figure A.3. Multilateral Financial Settlement ....................... 25
Figure A.4. Bilateral Trade Settlement ................................ 26
Figure A.5. Multilateral Trade Settlement ............................ 26
Figure A.6. Smuggling Settlement ...................................... 27
Boxes
Box 3.1. Al Barakaat: An Essential Chronology ........................ 11
Foreword

Terrorism can endanger innocent human life and tear the very threads that hold society together, namely, trust and security. Governments have mobilized a variety of tools in response, ranging from the political to the economic. In attempting to prevent and detect terrorist financing and other forms of material support, those offering financial services have been required to heighten their vigilance of potential terrorist abuse of those services.

While protecting financial services from potential abuse, care should be taken not to deny access to those services to those most in need. Dejection and social exclusion are very often conducive to terrorism; therefore, ensuring inclusion of the disenfranchised and creating possibilities for their advancement are key parts of the broader, long-term struggle against terrorism and extremism. Expanding access to the financial system while promoting market integrity is critical to delivering real opportunities and relieving despair.

International standards and best practices on the fight against money laundering and terrorism financing have been developed over the past two decades. A review of the implementation and effectiveness of the standards on terrorism financing has recently been conducted under the aegis of the United Nations, with the World Bank playing a leading role. A recently published report, *Tackling the Financing of Terrorism*, by the UN Counter-Terrorism Implementation Task Force, made nearly a hundred recommendations on an array of terrorist financing issues, including new technologies, nonprofit organizations, informal remittance providers, and international cooperation.

This paper addresses one of those recommendations, that the international community should provide guidance on alternative remittance systems and best practices in regulating them. We hope that it will bring useful insight to policy makers and practitioners as they work to protect their markets and communities from these terrorist threats while ensuring that the financial system works to facilitate economic development for the poor.

Consolate Rusagara
Director, Financial Systems
World Bank
Acknowledgments

This paper finds its roots in the World Bank’s participation in the United Nations Counter-Terrorism Implementation Task Force. This important exercise gathered practitioners from a diverse range of expertise, providing access to many great minds in fields such as law enforcement, economics, law, intelligence, banking, and finance. The opportunity to discuss, debate with, and listen to these many individuals made this paper possible.

The substantive inputs from Kevin Stephenson, Jean Pesme (both from Financial Market Integrity Unit, World Bank), and Thomas Hansen (Canadian Security Intelligence Service) were particularly appreciated.

The peer reviewers for this paper—Michael Defeo (United Nations Office on Drugs and Crime), Constantinos Stephanou (Financial Systems, World Bank), and Carlo Corazza (Payment Systems, World Bank)—also played a fundamental role in highlighting possible avenues to improve this work.

Finally, special thanks to Emile Van der Does (Financial Market Integrity Unit, World Bank) for his guidance both during the drafting of this paper and as a mentor at the World Bank Financial Market Integrity unit.
<table>
<thead>
<tr>
<th>Acronyms and Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIAI</td>
</tr>
<tr>
<td>AML</td>
</tr>
<tr>
<td>ARS</td>
</tr>
<tr>
<td>CDD</td>
</tr>
<tr>
<td>CFT</td>
</tr>
<tr>
<td>EU</td>
</tr>
<tr>
<td>FATF</td>
</tr>
<tr>
<td>FBI</td>
</tr>
<tr>
<td>FI</td>
</tr>
<tr>
<td>FIU</td>
</tr>
<tr>
<td>FT</td>
</tr>
<tr>
<td>IVTS</td>
</tr>
<tr>
<td>KYC</td>
</tr>
<tr>
<td>ML</td>
</tr>
<tr>
<td>NGO</td>
</tr>
<tr>
<td>OBL</td>
</tr>
<tr>
<td>OFAC</td>
</tr>
<tr>
<td>SAR</td>
</tr>
<tr>
<td>US$</td>
</tr>
</tbody>
</table>
Author’s Biography

Matteo Vaccani joined the World Bank Financial Market Integrity unit (FPDFI) in 2007. His analytical work has focused mainly on money laundering and terrorism financing (ML/TF) risk assessments of both country systems and specific financial markets. He has participated in FPDFI missions to Asia, Central America, and North America, including anti-money laundering on-site assessment visits. Mr. Vaccani also co-authored a World Bank study on ML/TF risks and mitigation policies along the Canada-Jamaica and Canada-Haiti remittance corridors. His work at FPDFI further includes the search for trends and patterns in the misuse of corporate vehicles in grand corruption cases under the World Bank-UNODC Stolen Asset Recovery Initiative (StAR). Mr. Vaccani holds a Laurea Magistralis from Bocconi University in Milan, Italy and an MA in Strategic Studies and International Economics from the Johns Hopkins University School of Advanced International Studies (SAIS) in Washington, DC.
Access to financial services is provided by a wide range of actors. Governments, through their regulatory bodies, typically regulate formal financial sector players such as banks, which can leave providers working in informal systems outside the regulatory regime. Value transfer services—financial transfers performed domestically or across borders on behalf of clients—are an essential component of the financial system, and as such are often offered by both formal and informal actors.

The Financial Action Task Force (FATF) in its 2005 ML/TF Typologies report defines Alternative Remittance Systems (ARS), as “any system used for transferring money from one location to another, and generally operating outside the banking channels.” Such a definition includes a wide array of channels, ranging from large, fully regulated multinational companies to small, covert value transfer outlets operating incognito.

This paper is designed to cover a subset of such category, that is, the realm of unregulated/informal Alternative Remittance Systems, also known as informal value transfer systems (IVTS). In these cases, operators form a parallel, underground financial system aimed at rapidly and effectively moving value within or between jurisdictions, often without being detected by regulators and law enforcement, and usually without available transaction records.

Where prevalent (as it is often the case in low-income economies), ARS are frequently the only mechanism by which poor or isolated people can send and receive funds and therefore provide an essential service to facilitate economic activity.

On the other hand, money and value transmission channels are being evaluated for vulnerabilities that may make them attractive for illicit use, including the financing of terrorism. Informal channels are often unregulated and have therefore been a focus of study and international standards definition. Regulatory attention to ARS has among its key objectives the prevention of abuse for money laundering (ML) or terrorist financing (TF) purposes. By monitoring the access of new players to the market and fostering transparency, regulation seeks to deter abusers and co-opt market actors in this mission.

Policy makers are thus looking for ways to measure and mitigate among others the risks of terrorist financing that ARS pose while ensuring the economic development benefits they bring are not diminished in the process. The World Bank is committed to assist governments in expanding access to financial services in a safe and sound regulatory environment.

An essential point to be made is that while the provider of the service may be acting outside the regulated financial sector and thus regulatory oversight, the majority of funds travelling across this channel, as well as the needs met by the same system, are completely legitimate. Speed, low cost, and reliability of transactions are in fact the most appealing characteristics for users. These attributes are the foundation for the success of a circuit that, while originating in the Indian
subcontinent and China, has been spreading out to include many economies and communities both within and outside Asia. Informal ARS can be found in major remittance recipients (India, Pakistan, the Philippines, Bangladesh, Sri Lanka, Somalia, Colombia), but also on the opposite end of major remittance corridors (the United States, the United Kingdom, Canada, and the EU).

The paper begins with a brief description of ARS models and their prevalence. It then covers their potential relationship with terrorist financing, citing cases where ARS have been abused for TF purposes. Ways in which countries may control these risks and indications of their effectiveness are covered next. The final chapter provides recommendations on how best to mitigate the risks while ensuring legitimate access to financial services via ARS.

Notes

1 The terminology employed in the World Bank/BIS General Principles for International Remittance Services (GPs) refers to Money Transfer Operators (MTOs) to indicate this kind of players. Given the focus of the present work—terrorism financing and associated risk mitigation—this paper will employ the FATF terminology currently used in the implementation of international AML/CFT standards.

2 Zerzan 2009.

3 The same factors usually constitute the main incentives guiding the choice of the preferred financial channel by remitters, including the choice between formal and informal avenues. See for example the World Bank Bilateral Remittance Corridor Analysis (BRCA) Working Paper series: http://web.worldbank.org/WEBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/EXTAM L/0,,contentMDK:21996399~pagePK:210058~piPK:210062~theSitePK:396512~isCURL:Y,00.html.

4 Passas 2003.
The basic mechanism of an informal ARS is based upon two relationships: the first between the clients and their respective operator, the second between the operators themselves (figure 2.1). Once a client at one end of the system pays the sum to be transferred plus an agreed fee to the provider (which can be part of the exchange rate gain), the provider contacts his counterpart in a designated country, who then pays the recipient. Both operators will need to have a sufficient amount of funds ready at their disposal, and enough trust in each other to conduct the transaction (that is, the disbursement to the identified recipient) and enter the settlement phase. The settlement can be conducted through different ways, based upon the operators’ needs and the circumstances surrounding the transaction (see below in the appendix).
Not all ARS models are identical. Informal remittance systems exist through a plethora of specific models tailored to the communities of reference, hence the existence of multiple names used in their respective locations. Examples of informal ARS include *Hawala* (Arabic peninsula/Afghanistan), *Hundi* (India/Pakistan), *Fei ch’ien, Hui k’uan, Ch’iao hui, Nging sing kek* (China), *Poey Kuan* (Thailand), and *Banglap* (Indonesia). One of the South American variants of ARS is the Black Market Peso Exchange (BMPE), well-known in connection to Colombian money laundering schemes.

These types of channels have in many cases succeeded in eliminating the most basic—yet challenging—barriers to access to financial services: affordability, physical access and eligibility.³

- **Affordability.** Unregulated ARS are able to offer their transfer services at extremely competitive prices, often undercutting almost any formal competitor. Decisive in this case is the strong trust among operators and between providers and users, which helps limit transaction costs. Similarly, costs are contained by escaping regulatory burdens, by sharing fixed costs with an existing business in which the ARS is embedded, and avoiding rigid foreign exchange controls.

- **Physical access.** When facing embryonic or inexistent formal financial infrastructure, as in the case of many developing rural areas, ARS often provide a much needed alternative to cash smuggling. In general, the growth of ARS has been found to be negatively correlated to the level of development of local financial sectors.

- **Eligibility.** By avoiding AML/CFT requirements that are common in the formal sector, ARS operators can accept clients and establish a relationship with them more easily than their formal sector counterparts. This is particularly so in the case of customer due diligence (CDD) obligations. Typically, banks and other formal financial system operators are required by law to meet certain know-your-customer (KYC) rules which can sometimes work as a barrier to the business relationship and, ultimately, to providing access to financial services. Conversely, operators of informal ARS do not generally implement the same CDD procedures, allowing them to reach a wider range of clients, especially those who lack or are unwilling to provide identity documentation.

These incentives are in many cases compounded by strong ties of an ethnic, tribal, or religious nature providing the necessary trust in and among operators, often not shared by formal financial institutions. This is particularly pivotal in the aftermath of major financial crises, when users are reluctant to entrust their funds with institutions that were involved in recent meltdowns. Extremely strong trust between clients and operators is equally of paramount importance. As the features described above, this characteristic suggests how informal ARS are essentially a grassroots channel, often created on the basis of pre-existing trust relationships, and molded to fit the needs of specific local communities.

While the basic ARS usually follows the model outlined above, several alternative settlement options can be identified, depending on how the operators involved proceed to manage their outstanding positions. In general, this is the phase of the system in which the actual money—or, more generally, value—is actually transferred.
from one actor to another within the formal system. Possible ARS settlement processes —ranging from legitimate to possible illicit practices—include the following\(^6\) (for a detailed description of each, please refer to the appendix):

- **Reverse transaction** (a transaction in the same amount is conducted in the opposite direction)
- **Bilateral financial settlement** (a formal financial transfer is performed between the two operators' jurisdictions)
- **Multilateral financial settlement** (a third country is involved in the financial transaction)
- **Bilateral trade settlement** (goods or services of equal value to the claim are exchanged between the two operator’s jurisdiction)
- **Multilateral trade settlement**; (a third jurisdiction is involved in a trade settlement)
- **Under/overstatement of trade values** (by under/over invoicing in trade deals value is created and transferred to the claimant)
- **Smuggling** (high-value goods are exchanged illegally across borders to satisfy the claim).

The array of settlement systems described above basically illustrates the potential strengths of ARS. The service provided can offer high speed,\(^7\) relatively affordable costs, and in many cases underlying trust bonds born from shared values or strong kinship ties. As for the infrastructure required, an affordable and effective message system and two readily available pools of funds provide the core elements required to perform the transaction. The range of alternatives available for settlement allows the operators involved to tailor the system to the changing environment, including evolving regulation. Its diversity thus renders the system highly resilient. Furthermore, informal ARS can also rely on multilayered structure, where communities of operators are linked through multiple settlement chains going beyond the simple two-agent structure involved in the individual transaction.

Given the general features and success of the model, the dilemma faced by regulators with reference to ARS is clear. On the one hand, where informal systems play a substantial role in the local economy, funneling a significant share of financial transfers in the jurisdiction, a clear incentive to access transaction records (to estimate the flows involved) and ensure the integrity of the system exists. On the other hand, where ARS supply much needed financial services otherwise not accessible by a significant share of the local population, authorities fear that the introduction of regulation may lead to the disappearance of the sector (by eliminating the cost advantage due to the compliance burden), or to incentives driving operators further underground.

When seeking to mitigate abuse risks faced by ARS (including TF risks, described in the next section), it should be underlined how any measure should also take into account the perils of ARS disruption. While guarding against possible abuse is fundamental, ensuring that preventive and provisional measures have minimal impact on legitimate flows is equally pivotal. As outlined above, ARS often play a key role in providing channels for financial transactions within developing economies, and in their relations with foreign markets.

The prompt and reliable mobilization of funds for investment and consumption is a pillar of sound economic development. Disrupting ARS circuits when fearing they
may be abused for terrorist purposes may often result in long-term costs hardly offset by short-term gains in risk mitigation. If excessive suppression measures are mistargeted to operators eventually found innocent, the overall net losses may be very significant. This is particularly true where, due to embryonic financial systems, ARS constitute the main avenue for cross-border financial transfers.

This tension between risk mitigation and possible mistargeting/abuse of anti-abuse measures is a central issue in regulating ARS, and should be discussed when relevant policy decisions are to be made. This is equally important when considering initiatives seeking to mitigate TF risks. The next section will delineate both components: (i) the TF risks, real and undeniable, faced by ARS operators, as shown by theory and past incidents; and (ii) the possible impact of mistargeted CFT measures against ARS networks, epitomized by the post-9/11 al Barakaat case in Somalia.

Notes

1 Jost and Sandhu 2000.
2 Passas 2003. See also Ranjan 2005.
4 On the economic advantages of high trust, see for example Fukuyama 1995.
6 World Bank and IMF 2003.
7 In post-conflict Afghanistan, transferring funds to Kabul from Peshawar, Dubai, and London took an average of 6 to 12 hours, with most transfers from Kabul to other major regional center carried out within 24 hours. See Maimbo 2003.
CHAPTER 3

Vulnerability to Terrorism Financing

Informal ARS can be—and have been—appealing to organizations and individuals engaged in the financial support of terrorism. Factors leading to the attractiveness of the sector to TF include those responsible for its success (speed and accessibility in prinis), but may also be linked to elements external to the mechanics. In absolute terms (that is, only considering the channel itself), it is reasonable to regard informal ARS as vulnerable to terrorist financing endeavors, and real life tends to confirm this.

Compiling a consistent and exhaustive list of ARS-based terrorist financing cases can be a challenging task. At this stage, it is safe to state that the use of hawala-type channels for this purpose has been reported in multiple occasions, and with reference to a diverse range of terrorist groups worldwide.

For instance, hawala has been reportedly employed to finance terrorist operations against Indian targets. In the 2000 Red Fort attack, in which members of the Lashkar-e-Toiba anti-Indian Kashmir-based group killed three Indian soldiers, the prime suspect allegedly received Rs 3.5 million through a Dubai-based hawaladar.1 The same group is also allegedly behind the November 2008 Mumbai attacks. Similarly, in the 1993 Mumbai serial bombing case, funds were transferred to the main suspect by a local hawala dealer.2

In the case of al Qa’ida, the 9/11 Commission found no clear evidence of the use of hawala-type systems to finance the New York and Washington, DC attacks, yet it acknowledged that before 2001 the organization had frequently moved funds using this method through Pakistan, United Arab Emirates, and Afghanistan.3 In addition, the group allegedly resorted to this kind of channels in other occasions. In the aftermath of the Nairobi embassy bombings in 1998, after escaping death one of the bombers was able to obtain emergency funds from a contact in Yemen through a Somali-based hawaladar (Dihab Shill), who agreed to disburse the funds upon explicit request of the sender despite the absence of any proof of identity by the recipient.4 Furthermore, al Qa’ida operatives allegedly moved funds and gold outside of Afghanistan and into Pakistan in the early stages of Operation Enduring Freedom, using hawaladars in both countries.5

Further indications on the abuse of ARS for supporting terrorism come from a case opened in Sweden in 2004, when two Iraqi citizens of Kurdish origin were arrested for funneling US$148,000 to finance Ansar al-Islam/Ansar al-Sunna in the Kurdish areas of Northern Iraq. The two allegedly resorted to two parallel means of transfer: cash couriers and a hawala enterprise run by one of the defendants in the city of Malmoe.6

A more recent case can be found in the United States. In November 2008, a Pakistani national, Saifullah Anjum Ranjha (henceforth Ranjha), legally residing in Washington, DC and the U.S. state of Maryland was sentenced to more than nine years
of jail time and three years of supervised release for conspiring to launder money and for terrorist financing. The man, who pled guilty and was the only defendant originally charged with activities relating to TF, was the operator of a money remitting business in Washington, DC.

Between 2003 and 2007, Ranjha and his accomplices allegedly provided money transfer services to a cooperative witness acting as an individual involved in large-scale criminal activities (including drug trafficking, smuggling, arms trafficking, and TF supporting al Qaeda). The case provides a clear example of the potential reach of a single ARS operator in supporting terrorist groups on a global scale.

While not all transactions were performed through the use of hawala channels, a total of 21 transfers were carried out using ARS in the process. Three main kinds of transactions were allegedly used by the defendant to transfer and launder funds. In some cases, only bank-to-bank transfers through cross-border wire transfers. In others, hawala-type transfers and bank-to-bank transactions were used in the process. Finally, “pure” hand-to-hand hawala transactions were performed multiple times. Overall, a total of 21 hawala transactions ranging from US$13,000 to US$300,000 per transfer were performed using a network of persons and/or businesses across national borders.

Of particular interest is the reach that the organization was able to obtain through such channels. Just taking into account the transactions involving hawala transfers, the perpetrators were able to transfer money from the United States and often through Canada (Montreal) to locations spread over the globe (see figure 3.1). Combining hawala and bank-to-bank transactions, destinations included the United Kingdom, Spain, the United Arab Emirates, Pakistan, Japan, and Australia.

If informal ARS therefore seem to constitute an attractive option to terrorism financiers, what are the elements shaping this perception? A first factor is the evolution of terrorist financing strategies in the aftermath of 9/11. The 2001 attacks apparently caught the international community unprepared in its positioning against the abuse of financial infrastructures for TF purposes. Following the attacks, much of the pressure from authorities has been unleashed to target the formal financial system. Formal channels had in fact been the main avenue used to finance the most daring terrorist operation of modern times. Yet this same pressure can be reasonably expected to influence perpetrators’ choices: taking al Qa’ida as an example, terrorist groups seem to be monitoring official responses to tailor their strategies. In the case of financing, this may be translated in a shift from formal financial channels to the informal world, and therefore ARS.
Alternative Remittance Systems and Terrorism Financing: Issues in Risk Management

Figure 3.1. Ranjha Case Alleged Transfer Network, 2004–2007

Source: Author’s representation based on USA vs. Saifullah Anjum Ranjha et al.
Secondly, and with reference to cross-border informal remittance transfers, the use of foreign communities as financial supporters of terrorist organizations has already been reported as an ongoing practice. For example, Hezbollah reportedly enjoys financial support from wealthy like-minded members of the Lebanese diaspora in the Americas.\(^8\) While in many cases such transfers have been performed using foreign nonprofit organizations, the use of ARS seems an attractive complement to terrorist financing abuse of nonprofit organizations. Al-Qaeda is once again a case in point: wealthy sympathizers residing in the “hawala triangle” (Dubai–Pakistan–India)\(^9\) might find informal remittance channels an attractive alternative to formal cross-border transfers—away from CFT controls—to finance the organization in its regrouping efforts.

A third aspect that should be considered in assessing TF risks is the combination of elements that brought the system its widespread success. ARS can be an effective means for fund transfers, both for operational purposes (that is, the provision of financial means to cell members by the top echelon of the organization) and for the general financing of the central structure of the terrorist group.

For operational purposes, the speed of the service, competitively superior to that of wire transfers, can be decisive in making funds available to cells already deployed in the field and in urgent need for financial support. The alleged abuse of hawala systems in the case of the African embassy bombing by al Qaeda is a case in point, as the operative in question requested emergency funds after unexpectedly surviving the attack (see above).

ARS can be equally effective in providing general funding of the terrorist network. ARS often rely on existing close-knit communities based on common ideological, religious, or tribal ties. This is highly beneficial to users who wish to keep their activities, or indeed their identities, secret. A favorable underlying social environment (as the one found in Pushtun areas along the Afghan-Pakistani border by al Qaeda) might not only be a general advantage in seeking a safe harbor, but also a source for reliable financial channels for economic support to the group’s growth. Furthermore, the fact that large transactions (sometimes exceeding US$500,000 in Afghanistan)\(^10\) can be effectively carried out also provides an incentive to the use of these channels to fund the development or regrouping of a terrorist organization.

A further incentive to use informal ARS is the typical approach to record keeping adopted by the sector. In general, customer records referring to single transactions are destroyed after the completion of the operation, or kept in aggregate for settlement purposes. Therefore, in the absence of specific regulation and corresponding compliance, informal transactions do not leave audit trails, making subsequent investigations particularly challenging, and terrorists relatively safe from rapid tracing of disbursed funds. Even when an IVTS operator is found to have connections to terrorist groups, the identification of actual individual transactions involved in TF remains a daunting task. Equally challenging in several cases has been the successful prosecution of individuals implicated in ARS-based TF cases.\(^11\)

Despite the multiple elements that seem to point at ARS as a viable option for TF, in fact building a case against their alleged abuses of ARS for terrorist financing purposes has often proved daunting in the past. The well-known al-Barakaat case, where one of the major Somali-based hawala companies had been accused of supporting al Qaeda, is a case in point. Al Barakaat had come to the attention of U.S. authorities in the late 1990s, when a local bank had filed SARs regarding transactions between the Minneapolis branches of the Somali remitter and its account in the United Arab Emirates.\(^12\) Later on, intelligence reports had linked al Barakaat to al Qaeda and even Osama bin Laden himself, alleging that the remittance service provider had
both facilitated fund transfers for al Qa’ida and had skimmed profits to finance the group.13

Corroborating such reports had been incredibly difficult, since the trail had almost disappeared once the funds had been moved to the United Arab Emirates. However, the 9/11 attacks put growing pressure on authorities to build a case against the entity, which was designated a terrorist organization subject to asset freezing and blocking in the fall of 2001. This move prompted the freezing of approximately US$1.1 million in the United States, and—according to U.S. Treasury estimates—the temporary disruption of US$65 million in annual remittances from the United States. Abroad, authorities closed al Barakaat offices in the United Arab Emirates, Djibouti, Ethiopia, Kenya, and Somalia.

**Box 3.1. Al Barakaat: An Essential Chronology**

<table>
<thead>
<tr>
<th>Year</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>SARs regarding al-Barakaat transactions in the United States begin to reach U.S. Treasury.</td>
</tr>
<tr>
<td>May 1997</td>
<td>The Federal Bureau of Investigation (FBI) opens a criminal ML case file on al-Barakaat.</td>
</tr>
<tr>
<td>August 1998</td>
<td>The FBI closes its investigation, unable to substantiate SARs.</td>
</tr>
<tr>
<td>1998–2000</td>
<td>First intelligence reports in Minneapolis on al-Barakaat’s ties with Al-Ikhwaad Al-Islamiya (AIAI) and OBL.</td>
</tr>
<tr>
<td>November 1999</td>
<td>The FBI opens a new criminal TF investigation on al-Barakaat in Minneapolis.</td>
</tr>
<tr>
<td>December 1999</td>
<td>The FBI opens a criminal investigation on al Barakaat in Seattle.</td>
</tr>
<tr>
<td>November 7, 2001</td>
<td>Al-Barakaat offices in United States, United Arab Emirates, and Somalia are integrated in to the OFAC’s SDN List. A total of US$1.1 is frozen in al-Barakaat accounts in the United States and United Arab Emirates, disrupting US$ 65 million in remittances from the United States.</td>
</tr>
<tr>
<td>December 2001</td>
<td>Al-Barakaat offices are closed in the United States, United Arab Emirates, Djibouti, and Ethiopia.</td>
</tr>
<tr>
<td>January-March 2002</td>
<td>Two U.S. investigative missions are sent to the United Arab Emirates. An FBI memorandum to United Arab Emirates officials says no substantiating evidence is found.</td>
</tr>
<tr>
<td>January 2002</td>
<td>Sweden and Canada move to have citizens of Somali origin taken off the OFAC list.</td>
</tr>
<tr>
<td>Spring 2002</td>
<td>U.S. Treasury presents a de-listing procedure to the UN.</td>
</tr>
<tr>
<td>August 2002</td>
<td>OFAC removes U.S.-based remitters in Minneapolis and Columbus, and two Somali Swedes from the designated entities list.</td>
</tr>
<tr>
<td>Late 2002</td>
<td>FBI closes the criminal investigation in Minneapolis.</td>
</tr>
</tbody>
</table>

*Source: Roth et al. 2004.*

Such developments resulted in a crushing blow to the credibility of the company, and of the entire Somali informal ARS sector worldwide. In addition, development agencies operating in Somalia and heavily relying on al Barakaat for their transfers had to frantically search for alternative avenues to transfer funds. Ironically, the collapse of remittance flows to Somalia was avoided by the prompt intervention of
other ARS operators, ready to fill the vacuum.\textsuperscript{14} Eventually, long-sought access to seized records in the United Arab Emirates revealed no evidence of any real connection between al Barakaat and any terrorist group, and prosecutors were ultimately unable to file charges against any of the company participants for terrorism, terrorist financing or related crimes. In fact, the only charge that came from the investigation was against a single customer for welfare fraud.\textsuperscript{15}

The considerations noted above and the examples presented illustrate the potential role of ARS in terrorism financing, that is, the \textit{absolute} TF risk stemming from such practices. However, one should not neglect to consider the \textit{relative} weight of informal ARS as a weapon of choice for terrorist support. In other words, since prevention efforts should be allocated adopting a risk-based approach—tailored to each jurisdiction’s features—when analyzing the chances that an informal system might be used for TF purposes, special attention should be dedicated to the identification of all available options appealing to terrorist operatives.

Afghanistan—or any other case where the local financial infrastructure is embryonic and control on the territory scarcely effective—is a case in point. While local \textit{hawaladars} might present an attractive route for fund transfer, the presence of long, extremely porous borders traditionally exploited for smuggling is very likely to offer a better chance for undetected fund movement. In particular, resorting to cash couriers or precious metal smuggling would avoid the involvement of more intermediaries (reducing detection/leak risks) and allow for the movement of larger sums per transfer than in the case of ARS.

This highlights a fundamental point in the approach to ARS risks: the mere existence of informal remittance systems does not imply their use as exclusive or primary means for TF purposes. Investigative and enforcement resources should be allocated on a case-by-case basis, proportional to the relative risk of the sector in comparison to others available. To minimize opportunities for regulatory arbitrage by perpetrators, any increase in regulatory and enforcement pressure by authorities on ARS operators should be balanced by a parallel strengthening of other controls. Underlying this approach, a pivotal principle: tailor regulation design and enforcement to the specific features of the local market, and avoid one size-fits-all temptations, as explained in the next section.

\textbf{Notes}

1 Ranjan 2005. See also Bhatnagar 2001.
2 Ibid.
3 Roth et al. 2004.
5 Kiser 2005.
7 “\textit{Money remitter sentenced to over 9 years for money laundering conspiracy and concealing terrorist financing}”, DOJ Press release, November 4, 2008.
8 LaVerle et al. 2002.
14 Omer 2003.
CHAPTER 4

Risk Mitigation Measures

Bearing in mind that ARS, in all their forms, are generally serving legitimate needs for legitimate clients, the ideal response to TF risks must be aimed at separating legitimate flows and clients from those that do not fit in such a description. One of the main lessons from the al Barakaat case is that preventive measures adopted where channels are feared to have been abused—like massive account freezing—can result in considerable disruption of financial flows when mistargeted. The adoption of a complementary preventive approach based on market regulation assumes paramount importance in moving risk mitigation upstream (that is, even before terrorist activity is suspected or detected). This can contribute to minimize disruption risks from mistargeted intervention. Underlying this approach is the pivotal objective of balancing risk mitigation and the promotion of feasible legitimate financial transactions.

Adopting such an approach, the Financial Action Task Force (FATF)\(^1\) has issued a specific Special Recommendation addressing ARS and their informal variants. The recommendation constitutes the minimum set of measures required to manage AML/CFT risks. According to Special Recommendation VI (SR.VI):

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

The recommendation has three main components, which are pivotal in providing an effective positioning against the risk of ARS involvement in TF. The first is the requirement to impose registration or licensing on all ARS, be they linked to the formal financial system or not. The second is that such entities should be subject to the full array of FATF Recommendation applicable to financial institutions (FIs). Finally, sanctions should be put in place against operators acting outside the legal framework. The rationale of SR.VI is almost self-explanatory: in order to avoid intense regulatory arbitrage aimed at escaping AML/CFT obligations applied to traditional FIs, informal ARS should not be left out of the regulatory regime so that they implement measures to prevent abuse, as required from other financial entities in the formal sector.

Such a plan can be roughly divided into three equally important components. First, a fundamental precondition for implementation of preventive risk mitigation measures is the detection of ARS operators. Second, once the targets for regulatory
requirements have been identified, the careful *definition* of rules is equally pivotal. Third, the *enforcement* of regulation is key both in providing credibility to the CFT regime and in ensuring its effectiveness.

**Detecting Informal ARS**

Dealing with a sector that has traditionally thrived on informality, detection can easily become a frustrating endeavor, even when the avoidance of public scrutiny was not the sole or main purpose for setting up the system. No single recipe for effective detection of informal ARS operators can be suggested as a panacea for the problem. As informal operations tend to adapt their features to the field they are embedded in, so should tactics aimed at detecting operators and their systems.

However, from a strategic point of view, and considering the basic structure of any informal ARS, detection efforts should be mostly focused not on the service itself (that is, the remittance transfer between the two clients), but on the elements the average operator needs to provide the service in question. Three main elements stand out as likely requirements for ARS managers: a link to the formal financial sector (for example, one or more accounts with FIs to manage the pool of fund at each end of the corridor); access to foreign currency; visibility to potential clients for marketing purposes.

To these three elements corresponds a three-pronged approach to informal ARS detection.

*Cooperate with Formal FIs to Recognize ARS Operators’ Accounts*

The most vulnerable element to detection is likely to be the link of any ARS to the formal system, in particular for the purposes of position settlement between operators. While the settlement of outstanding positions does not necessarily require the use of formal payment systems, it would be fair—beyond a given flow size and complexity of services provided—to expect the use of formal accounts (also to manage the pool of funds at each end of any *hawala*-type operation). In many cases, the operator could use an existing account linked to the standing business in which the ARS is embedded.

Hence, monitoring such accounts may be valuable in identifying informal ARS operators when the situations described below are present. A significant indicator that ARS services are being provided is the concurrence—with reference to the monitored accounts—of two or more of the dynamics described below:

- The size of the flows passing through the account and the average account balance are inconsistent with the stated business run by the holder. In other words, whether the cash flow observed within the account matches its stated sources.
- The direction and frequency of flows involved, especially with cross-border transactions, seem inconsistent with the actual needs of the stated business activities of the account holder.
- The account shows frequent outgoing transfers to a major financial center known to be involved in *hawala*-type operations, such as United Kingdom, Switzerland, and Dubai.
- The timing of sudden increases in cash deposits/withdrawals seems to match known peaks in migrant remitting practices. Soaring cash withdrawals might signal the need for frequent disbursements on the recipient end of a remittance corridor, while sudden increases in cash deposits might indicate frequent originations of remittance transfers in sending countries. In both
cases, if the timing of such phenomena coincides with religious holidays, the beginning of the school year, or other occasions when migrants typically remit more than usual to cover peaks in expenses or to send gifts (see figure 4.1), the account might be used for ARS purposes.

In the figure 4.1 below, monthly remittance inflows in a high-volume recipient country show recurring patterns, with frequent spikes in December (Christmas) and at the beginning of spring. Spikes in withdrawal activity from local business accounts following similar patterns can be indicators of ARS operations when there is a mismatch with the cash flows expected in a specific business.

By notifying the proper authorities of such discrepancies or coincidences, formal financial institutions might contribute to effectively guide investigators toward the identification of informal operators. Authorities can then ensure they are properly implementing mitigation measures (see below). Similarly, monitoring of ARS accounts (once detected) by FIs would be valuable in preventing abuse of the system. For instance, FIs could report transactions that defy the normal direction of remittance flows in the specific corridor, or cross-border transfers that individually or cumulatively exceed the capacity of the community of reference in terms of frequency and average individual transfers based on the average earning of migrants.

**Figure 4.1. Remittance Inflow Recurring Patterns, 1994–2007**

![Figure 4.1 Remittance Inflow Recurring Patterns, 1994–2007](image)


**Coordinate with Foreign Exchange Dealers both Domestically and Internationally**

In many cases, bulk money transferred across borders signals the existence of ARS, often with couriers as part of the picture. Focusing on the couriers, and the origin of the currency involved, might provide valuable hints in order to trace the IVTS operator involved in the transfer. Foreign exchange entities within the jurisdiction of reference and in foreign jurisdictions which are known to be active along the specific corridor should be involved in these efforts. Similarly, information sharing between foreign custom authorities—especially along corridors where ARS are particularly present—would bring much value add to investigative efforts.
Monitor Local Media for ARS Service Advertisement

The “informal” component of ARS might suggest the image of a channel relying almost exclusively on word-of-mouth for promotion purposes. The opposite appears to be true: informal ARS are similar to average financial service ventures: *hawaladars* are players on an often fiercely competitive market, which calls for equally aggressive marketing. The use of a fairly wide array of media channels, ranging from ethnic/local press to TV, radio and Internet depending on the market of reference, is thus often common among ARS operators to attract business.

Monitoring the media and searching for advertisement from informal remittance service providers can be a valuable tactic. This approach may even be effective when informal operators do not publicize their services openly, but rather advertise the business in which remittance services are embedded and often hidden on purpose. In these cases, profiling businesses and shops targeting a clientele likely to use ARS could offer precious indications to guide investigators. Such activities include discounted international communication services (“call-centers”), travel agencies targeting specific routes along major migrant corridors, shops serving specific ethnic groups in countries hosting foreign migrants. Other examples include import/export businesses, precious stones dealers, foreign exchange dealers, rugs/carpet importers, used cars dealers, and car rentals. While the embedded ARS services may not be clearly recorded in the business’ books, observing the stated business volume and comparing the data reported with the nature of the front business itself, and detecting discrepancies are often the first steps in identifying a hidden IVTS. Parallel to this basic approach to detection, surveys by covert solicitation of ARS services may also be productive sources of intelligence.

The Debate on Licensing and Registration

Parallel to efforts aimed at detecting active informal operators, authorities are called by SR.VI to impose a regulatory framework that should allow government officials to at least be aware of the existence of ARS businesses. That would subsequently provide the foundation to apply other AML/CFT measures (for example, recordkeeping, CDD) to ARS operations, according to their risk profile. Under this framework, licensing (implying that a regulatory body has subjected the operator to an ex-ante inspection before authorizing) or registration (requiring that the operator voluntarily enters a pre-arranged list of active businesses) are considered key to the effective regulation of any financial service sector.

A heated debate has recently emerged over the impact of the introduction of such regimes on the typical informal ARS sector. On the one hand, detractors of this approach contend that since anonymity and avoidance of public controls are a natural component of the business, any effort to bring the informal sector under registration/licensing schemes will just push operators further underground, and therefore increase their risk of abuse by terrorist financiers. On the other hand, advocates of regulatory efforts argue that legitimate ARS operators will have incentives to register or apply for a license, to preserve their reputation on the market, any links to the formal sector they might have, and to gain visibility among clients. While providing a definite answer to the debate remains a challenging task, looking at regulatory experiences in the field may offer valuable indications on the way forward.

Policy approaches around the globe vary from the outright prohibition to engage in informal practices, to licensing and simple registration. Evidence from the field seems to point at prohibition of informal remittance systems as a tactic requiring substantial efforts and strict conditions to work effectively. Since the creation of
informal ARS is ultimately based on a legitimate need for financial services, the simple prohibition of the mechanism will not make those incentives disappear.

Therefore, prohibiting the use of informal ARS—while still a legitimate regulatory practice at the disposal of authorities—will have to be coupled with prompt efforts to provide access to equally or even more effective formal alternatives. This does not translate into the simple promotion of standard remittance services offered by traditional operators (such as banks), but into the creation of competitive alternatives that respond as effectively as informal ARS to affordability and access barriers faced by the average user. In the absence of such alternatives, when facing the unconditional prohibition of operations, the informal sector is likely to go further underground under growing pressure from those unable to access formal services.\(^6\)

The positive effect of the promotion of effective formal alternatives to informal systems can be seen in the case of the Philippines, where the Central Bank has actively promoted innovation among banks to replicate the advantages of informal services.\(^7\) These efforts were translated into the introduction of door-to-door funds disbursement, bank personnel secondment to main remittance sending countries,\(^8\) and the introduction of mobile financial services, accessible by any client in possession of a cell phone.\(^9\)

In addition, advocates of informal ARS prohibition should be aware of the challenges stemming from enforcement of such rules: unless substantial resources are available to constantly search for active informal operators, the underground sector is likely to thrive and distrust of authorities by operators is likely to grow.\(^10\) Considering the chronic lack of human and financial resources often experienced by regulators and supervisors in developing economies (where informal ARS are more likely to be widespread), the issue should not be neglected. Finally, even assuming the effective removal of the informal sector, without appropriate alternatives the result would be to simply punish both legitimate users and potential abusers alike (as shown by the impact of the al Barakaat company closure in Somalia). A possible backlash against international counter-terrorism efforts and their perceived compatibility with economic development objectives should not be ruled out within such a scenario.\(^11\)

The introduction of registration regimes might be a more suitable option for jurisdictions where the formal financial sector has not developed to a point where viable alternatives to ARS are available. In general, registration has been found to be the most cost-effective solution for both operators and authorities who are not required to engage in costly inspections of each applicant.\(^12\) On the other hand, markets where informal remittance service providers are more organized and structured (and often connected through industry associations) might see the effective introduction of licensing requirements. Licensing has undoubted advantages in preventing the entry into the market of operators unwilling or unable to meet basic AML/CFT requirements, as defined by authorities. A mature ARS sector would be more likely to have higher compliance capacity—also through industry association actions and peer pressure—and would have a better chance to step in and fill the void left by non-compliant operators left out of the market.

Evidence from the field does not seem to support the argument that informal ARS are inherently resistant to regulatory initiatives, both within sending and recipient countries. For instance, major Somali hawala companies operating in Canada have been reportedly operating with effective awareness of the regulatory requirements imposed by authorities, with their top echelons claiming that all necessary efforts to comply with such obligations have been made both at headquarters and agents’ levels.\(^13\) While such statements cannot act as a guarantee of full compliance, they signal
the willingness by operators to acknowledge their obligations, as opposed to the avoidance of such requirements.

Yet the proactive response of ARS operators to the introduction of regulatory framework is not limited to developed economies. Afghanistan, rightly pointed at as the epitome of an informal ARS-dominated financial sector, is a case in point. After a voluntary registration regime had been set up as part of reform efforts started in 2002, many operators were willing to participate in the system, mainly to set themselves apart from other competitors. As a matter of fact, the registration of hawaladars had a positive response from the market itself, with clients showing a significant preference for registered operators, perceived as more reliable.14

Local authorities showed great ambition in trying to engage a system that—given its role as the financial backbone of the country—had previously been left untouched. A fundamental role in the process was played by the tradition of self-regulation in the sector, with players organized around an eight-member Executive Committee that provided a precious interlocutor for regulators.15 The enforcement of tacit rules has been traditionally effective, with violators often forced out of the market once other operators—whose cooperation is fundamental to perform large-scale transactions—"blacklisted" them.16 This shows once again, that the argument that informal ARS are by definition resistant to regulation does not necessarily hold.

The main lesson to be drawn from such cases, however, is that the effective design of regulation must be tailored to the unique characteristics of each ARS market. The risk profile of clients and transactions, the compliance capacity of operators, the existence of an informal self-regulation structure and of alternative financial transfer mechanisms are all elements that can combine differently in each jurisdictions, soliciting different responses.

The Essential Role of Enforcement

Studying the anatomy of ARS, understanding associated TF risks, and designing a regulatory framework to address those risks are only some of the components of a sound TF risk mitigation strategy. No matter how well-designed and tailored, no regulatory framework will attain results without proper enforcement of rules and requirements upon covered entities.

The case for prompt and effective enforcement rests on two major elements. First, without proper supervision and administration of sanctions for noncompliance, the resources spent on building the regulatory regime would be wasted. In developing economies, this may have serious repercussions on local governments and their reputation in administering resources. Secondly, a regulatory regime lacking proper enforcement would be void of any credibility among market players. Faced with ineffective supervision, non-compliant actors will have no incentives to comply with rules, while compliant operators face a powerful incentive to cease their compliant behavior to remain competitive in the market.

Yet in many instances, once a regulatory framework has been designed and established, and ARS operators are detected, enforcement is not systematic. In some cases, major operators—well known by both the population and authorities—are able to remain underground and escape regulatory requirements with no sanctions. The failure to effectively enforce previously agreed rules can often be traced to at least three main factors, (not necessarily mutually exclusive), which call for specific approaches to obtain a fully functional regulatory regime.

The first factor relates to capacity: in many cases supervision and enforcement are not effective due to human and technical resource constraints. Authorities are able to
detect ARS operators, they aim at enforcing regulation, but fail to do so lacking the necessary expertise/tools to reach all actors across the jurisdiction, identify noncompliant behavior, and administer sanctions. In these instances, a fully functional regulatory regime calls for the reallocation of resources to allow effective enforcement. Where the overall allocation of resources does not allow for such, and financial sector development programs are being designed, foreign or international organizations’ technical assistance in this realm should be considered as an option.

The second possible element behind the lack of proper enforcement of ARS regulation relates to integrity. ARS operators seeking to escape supervision can mobilize their financial means to achieve this. Particularly in jurisdictions characterized by widespread corruption and a lack of governance, those in charge of enforcing regulation may be bribed by ARS operators aiming at remaining in the shadow. Local authorities may have the right resources allocated to enforcement, but their use is rendered ineffective by corrupt practices. These instances highlight how the design and implementation of regulation—be it focused on ARS TF risks or other market failures—is doomed without a coherent anti-corruption framework providing the foundation for enforcement.

The final factor that can thwart the effective enforcement of ARS regulation pertains to the fear of disruption of financial flows. In developing economies heavily reliant on workers’ remittances (accounting in some cases for close to 20 percent of the national GDP), authorities are often reluctant to apply risk mitigation strategies (and thus regulatory requirements) to those channels handling the bulk of remittance inflows. Such reluctance can be traced to the concern that introducing new rules will bring excessive additional costs to operators, which will be forced either to exit the market or pass the additional cost to users via increased fees. In turn, the belief is that such changes will lead to a fall in remittance inflows and thus the shrinkage of such an important balance of payments component.

Yet TF mitigation measures targeting ARS operators are unlikely to result in market disruption if well tailored to local market features (see above). On the contrary, as mentioned and shown by previous studies, reliability and safety of transfers are often among the top priorities shaping senders and recipients’ behavior. Registered/licensed operators can be perceived as more reliable providers, and thus gain the users’ favor. Authorities should consider these possible advantages when faced with the choice between enforcement and half-hearted application of rules.

Notes

1 The Financial Action Task Force (FATF) is an intergovernmental policy-making body created in 1989, whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. As part of its mandate, between 1990 and 2004, FATF has issued a total of 40 Recommendations on ML and 9 Special Recommendations on Terrorism Financing, which now constitute the core international standards on AML and CFT.
2 Jost and Sandhu 2000.
3 FATF 2003.
4 Jost and Sandhu 2000.
5 FATF 2003.
6 See CTITF 2009.
8 World Bank 2003.
9 For an in-depth analysis of the potential role of mobile financial services and their vulnerability to ML and TF, see also Chatain et al. 2008.
Countries that have prohibited the creation of IVTS are still struggling to combat the proliferation of parallel foreign exchange and remittance services markets. See for example World Bank 2003, p. 34.

See CTITF 2009.

FATF 2003.

Hamza 2006.

Interview with members of the intelligence community, 2008.


See for example the World Bank BRCA studies series.
Steps toward the introduction of regulatory frameworks into the informal ARS sector should follow a principle valid in any regulation effort: rules should be tailored to the reality they are intended to apply to. Blanket regulation is doomed to fail in general, but particularly so when the sector in question is traditionally built upon the needs of a tight local community. Simply applying generic, one-size-fits-all rules to any informal ARS setting will be likely to result in limited effectiveness. In addition, outreach and education efforts by authorities would be essential in improving awareness among operators, explaining the rationale for reforms and obtaining entities’ feedback on the impact of regulatory requirements.

The analysis conducted above highlights six main points concerning unregulated Alternative Remittance Systems, their potential role in the financing of terrorism, and the possible responses to such risks:

1) **Informality does not imply illegality.** While informal ARS have traditionally operated outside regulated framework, they have been created to serve both legitimate needs and legitimate users, and not necessarily abusers. In general, unregulated ARS have often provided a response to needs common to any financial sector, which in more developed settings have found accessible formal responses.

2) **Informal ARS can play a pivotal role in the financial sector.** Previous research has found a negative correlation between the development status of financial systems and the proliferation of informal ARS. There are scenarios where informal operators can constitute the backbone of the local financial system, as in post-conflict Somalia and Afghanistan, where ARS were even chosen by aid agencies to funnel funds for development purposes. When remittances accounting for a significant share of GDP target financially undeveloped jurisdictions, the importance of informal ARS reaches its acme.

3) **Links to the formal financial system are often present.** While in general the successful completion of an informal ARS transaction (that is, the transfer of value between two subjects) does not pass through formal financial channels, informal ARS often have links to the formal financial system in order to facilitate settlement of outstanding positions between operators. Such links are more likely to exist as the average transaction volume and the complexity of the system increase, and can be exploited for detection purposes.

4) **Both absolute and relative TF risk should be considered.** The speed and anonymity generally characterizing unregulated ARS can be attractive features for terrorist financiers, underlining the absolute risk of TF faced by these channels. However, the mere existence of unregulated ARS in a jurisdiction does not imply their selection as
the main channel for TF: the relative risk of abuse of ARS should be thus considered by taking into account all locally available options for terrorism financing.

5) Detection is a precondition of risk management. To effectively manage TF risks within informal ARS, authorities must first and foremost be aware of the existence of active operators and assess the size of the phenomenon. Detection can be implemented using three main avenues: co-operating with FIs and exploiting the link of ARS to the formal system, co-ordinating with major foreign exchange dealers, and monitoring local media for operators’ advertisements.

6) Informal ARS are not incompatible with registration/licensing. While prohibition of informal systems can push the sector further underground when accessible formal alternatives are not present and enforcement is not uniformly effective, evidence shows that registration of operators can be a viable option, with a potentially positive feedback from users. Field experience in both developed and developing jurisdictions shows that informal ARS are not inherently incompatible with registration/licensing. A key element in making such practices possible is to tailor regulatory pressure to local features, taking into account:

- the relative weight of the informal ARS sector in the overall system
- compliance capacity of operators and users
- relative attractiveness of the sector to terrorist financiers
- capacity of regulators to enforce compliance and develop relationships with operators.

7) Enforcement is a pivotal component in a TF risk mitigation strategy. No matter how successful the detection of informal ARS operators, no matter how well designed the regulatory framework, the lack of proper enforcement will doom a risk mitigation strategy to failure. Monitoring regulation enforcement efforts, detecting shortcomings in supervision, and identifying their root causes is fundamental. Factors underlying the lack of enforcement (such as resource constraints and lack of proper governance) have to be identified and addressed with ad hoc measures, either at the national or multilateral level.
The following sections describe possible and common ARS settlement processes, as cited in Section 1.

Reverse Transaction

The simplest, yet probably least likely option for settlement between ARS operators is to perform a second transaction—equal in amount to the first transfer—but in the opposite direction (figure A.1). In other words, considering a transnational ARS transfer between country X and Y, after paying off recipient 1 the operator uses a new client (sender 2) to send an equivalent order of payment to the other end of the corridor, offsetting the previous transfer(s) and settling the outstanding position.¹

![Figure A.1. Offsetting Transaction Settlement](image)

Source: Author’s representation.

Note: Arrows under Sender 1 and Recipient 1 indicate initial transactions; arrows under Recipient 2 and Sender 2 indicate settlement transactions.

While appealing in theory, this option would be unlikely to be widespread on actual ARS channels. The asymmetric nature of remittance flows along significant migration routes (with one end of the corridor characterized by net inflows, and the other by net outflows) is a major challenge to the diffusion of simple reverse transactions as a major settlement mechanism.²
Bilateral Financial Settlement

In this case, operator B—acquiring a claim after a transaction (that is, disbursing the payment to the recipient of the transfer)—later receives an offsetting payment directly, or into a bank account of his property (figure A.2). However, since in many cases the original reason behind the creation of the ARS is the existence of foreign exchange or other capital controls in one or both countries involved, the direct deposit would probably not be feasible into the claimant’s country. If the payment were to be performed in foreign currency, the existence of official controls would then translate into an unfavorable mandatory currency exchange for the claimant. In these cases, operators would be unlikely to resort to such a mechanism as a habitual means for settlement.

![Figure A.2. Bilateral Financial Settlement](source: Author's representation.)

Multilateral Financial Settlement

To escape financial restrictions, in this case the outstanding position is settled by using accounts in a third country (country Z) enjoying free foreign exchange transactions (figure A.3). The claimant (Operator B) will receive a payment in a foreign currency to be deposited in a foreign currency denominated account abroad. The position is therefore settled, according to the exchange rate agreed between the parties (no formal foreign currency purchase is made), through a de facto capital flight mechanism from the country of the former claimant to the third country hosting the account.
Bilateral Trade

The operator acquiring the claim (operator B) can see his outstanding position settled by means of accepting foreign goods from the country originating the original ARS transaction (country X). To satisfy the claim, the operator that has previously ordered the payment (operator A) can finance the purchase and transfer of goods to the other party (figure A.4). This settlement model is an appealing solution especially when the ARS itself is embedded into an existing import-export business.

Multilateral Trade

As in the case of multilateral financial settlements, a third country or party is involved in this settlement mechanism (figure A.5). The operator originating the initial transaction finances the export of goods to a country of choice of the claimant, with the object of the trade not necessarily coming from the settler’s country. For instance, a claim emerged after an ARS transaction from Canada to Vietnam might be later settled with the transfer of goods purchased in China and transferred to the claimant in Vietnam or to another country, where a third subject holds a claim against the Vietnamese operator. A slightly modified version of this mechanism would imply the financing of the purchase of international services (travel, health care, education) by the Canadian operator for the other party, or other residents of Vietnam identified by the claimant.
Figure A.4. Bilateral Trade Settlement

Source: Author’s representation.

Figure A.5. Multilateral Trade Settlement

Source: Author’s representation.
Under/Overstatement of Trade Values

In this case, under/over invoicing of export/import is used to settle the outstanding position. For instance, in the example made between Canada and Vietnam, the claim acquired by the Vietnamese operator is met by under-invoicing the export of goods to the country by the Canadian counterpart, a practice likely to provide also a discount on tariff obligations to the importer/claimant.7

Smuggling

Moving further towards outright illegal settlement mechanisms, claims between two ARS operators can be met by undeclared trade in commodities, epitomized by the well-known gold smuggling circuits popular in the “hawala triangle” between Dubai, India and Pakistan (figure A.6). The use of commodities not only allows the storage and transportation of highly concentrated value with relative easiness, but can also be extremely popular where local regulation forbids private imports of the items in question.

Figure A.6. Smuggling Settlement

Source: Author’s representation.

Notes

6 Wilson 2002.
References


Available at: http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf.

USA vs. Saifullah Anjum Ranjha et al., Second superseding indictment, Criminal No. MJG-07-0239.


Eco-Audit

Environmental Benefits Statement

The World Bank is committed to preserving Endangered Forests and natural resources. We print World Bank Working Papers and Country Studies on postconsumer recycled paper, processed chlorine free. The World Bank has formally agreed to follow the recommended standards for paper usage set by Green Press Initiative—a nonprofit program supporting publishers in using fiber that is not sourced from Endangered Forests. For more information, visit www.greenpressinitiative.org.

In 2008, the printing of these books on recycled paper saved the following:

<table>
<thead>
<tr>
<th>Trees*</th>
<th>Solid Waste</th>
<th>Water</th>
<th>Net Greenhouse Gases</th>
<th>Total Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>355</td>
<td>16,663</td>
<td>129,550</td>
<td>31,256</td>
<td>247 mil.</td>
</tr>
</tbody>
</table>

*40 feet in height and 6–8 inches in diameter

Pounds, Gallons, Pounds CO₂ Equivalent, BTUs
Alternative Remittance Systems and Terrorism Financing: Issues in Risk Management is part of the World Bank Working Paper series. These papers are published to communicate the results of the Bank’s ongoing research and to stimulate public discussion.

Governments, through their regulatory bodies, typically regulate formal financial sector players such as banks, which can leave providers working in informal remittance systems outside regulatory channels. Value transfer services—financial transfers performed domestically or across borders on behalf of clients—are essential to the financial system, and as such, are often offered by both formal and informal actors. Law enforcement and counter-terrorism authorities are evaluating money and value transmission channels for vulnerabilities that may make these channels attractive for illicit use, including the financing of terrorism. This paper aims to help countries bring these informal alternative remittance systems into their counter-terrorism programs, without hindering the ability of those who depend on these systems to send and receive money at low cost.

World Bank Working Papers are available individually or on standing order. This World Bank Working Paper series is also available by subscription to the World Bank e-Library (www.worldbank.org/newelibrary).