

JOINT CONFERENCE ON REMITTANCES

12-13 September 2005
ADB, Manila, Philippines

Presentation

**ADB'S AMLCFT POLICY &
ALTERNATIVE REMITTANCE SYSTEMS**

RITA O'SULLIVAN
Counsel
Office of General Counsel, ADB

ADB - IDB/MIF - UNDP JOINT CONFERENCE ON REMITTANCES
12-13 September 2005
ADB, Manila, Philippines

“Remittances and Poverty Reduction:

Learning From Regional Experiences and Perspectives”

Session III: Remittances and Anti-Money Laundering Efforts

ADB’s AMLCFT Policy & Alternative Remittance Systems

by Rita O’Sullivan¹

I. Background

Money laundering² and terrorist financing³ are major concerns in the regulation and overall efficiency of financial systems. Attempts to regulate remittance channels to prevent misuse by money launderers or terrorist financiers, require a clear understanding their inner workings. Over-regulation will drive operators underground, thereby possibly losing a vital link to information, which is critical in the fight against money laundering (ML) and terrorist financing (TF).

Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. TF may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes. At all stages, funds can be channelled through alternative remittance systems (ARS).

II. ADB’s AML/CFT Policy

ADB’s Anti-Money Laundering policy entitled ‘*Enhancing The Asian Development Bank’s Role in Combating Money Laundering and the Financing of Terrorism*’ (“ADB AML/CT Policy”)⁴ was adopted on 1 April 2003 to enable ADB to respond effectively to its developing member countries’ (DMC) needs related to establishing and implementing their AML/CFT regimes⁵. The four main components of the policy are: (i) assisting DMCs in establishing and implementing effective legal and institutional systems for AML/CFT; (ii) increasing collaboration with other international organizations; (iii) strengthening internal controls to safeguard ADB funds; and (iv) upgrading ADB’s staff capacity.

ADB in implementing its Policy is guided by several principles:

¹ Rita O’Sullivan is currently Counsel at Asian Development Bank. (rosullivan@adb.org) The views expressed herein are those of the writer and do not necessarily reflect those of ADB.

² Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

³ **Terrorist financing (TF) is generally understood as an act of providing or collecting funds with the intention that they should be used or in the knowledge that they are to be used in order to carry out terrorism.**

⁴ See <http://www.adb.org/Documents/Others/OGC-Toolkits/Anti-Money-Laundering/aml0200.asp>

⁵ The Policy is being implemented under Operations Manual (OM) Section C6/BP.

- AML/CFT activities are to be found within the broader context of its existing goals, policies, and strategies for assisting developing member countries (DMCs) such as poverty reduction, strengthening financial systems, and promoting good governance and anticorruption.
- Ongoing efforts and programs should not duplicate activities of the International Monetary Fund, the World Bank, Financial Action Task Force on Money Laundering (FATF), and the Asia/Pacific Group on Money Laundering (APG).
- Additional measures are to be identified that it might usefully complement the efforts of these and other agencies, either through its lending operations or training of government officials and other forms of technical assistance.
- ADB's role is to be tailored to take into account the special problems and circumstances faced by its DMCs. Notable among these problems and circumstances are lack or weakness of AML/CFT laws, weak institutional capacity to effectively implement and enforce AML/CFT laws, and lack of specialized and sustainable training for government officials.

III. ADB AML Projects and Toolkit

To date, ADB has provided direct assistance to a number of DMCs to develop their AML/CFT regime through a regional technical assistance (TA) project, country-specific financial sector loans which include AML/CFT reform measures, TA projects, and ad hoc technical legislative drafting and implementation support⁶. TA activities have included country-specific research on AML/CFT regimes and how to introduce reforms, training for officials, including judges and prosecutors involved in AML/CFT operations, assistance in drafting AML/CFT legislation, and technical advice to establish financial intelligence units (FIU).

Internal training is undertaken as it is recognized that ML/TF issues are specialized and distinct from the professional disciplines normally undertaken by ADB staff. ADB's AML/CFT Toolkit at www.adb.org/Documents/Others/OGC-Toolkits/Anti-Money-Laundering/default.asp was developed to support staff and DMCs and contains a wealth of operational information and links to other AML/CFT-related internet sites. An AML Technical Assistance and Training Coordination matrix⁷ and a model for sequencing reforms⁸ have also been prepared to assist staff and DMCs to integrate AML objectives into their project work and related activities and to ensure coordination with other donors providing assistance in the Asian region.

Much of ADB's AML assistance has been undertaken and will continue to be undertaken within the broader context of its strategies to facilitate poverty reduction, promote good governance, reduce corruption, and strengthen national financial systems. ADB's approach for regulating remittance channels follows Financial Action Task Force on Anti-money Laundering (FATF) and supports regulatory authorities to find the appropriate balance between preventing misuse with the need to ensure that flows of legitimate funds are not unnecessarily interrupted or pushed underground, while remembering that regulation is not a panacea to the larger problems that arise from ML and TF.

IV. Remittance Channels⁹

⁶ For a list of related projects see <http://www.adb.org/Documents/Others/OGC-Toolkits/Anti-Money-Laundering/aml0500.asp>

⁷ See www.adb.org/Documents/Others/OGC-Toolkits/Anti-Money-Laundering/documents/AML-ta-matrix-revised.pdf

⁸ See www.adb.org/Documents/Others/OGC-Toolkits/Anti-Money-Laundering/documents/sequencing-of-events.pdf

⁹ This section draws heavily from the FATF Working Group Paper on MONEY LAUNDERING & TERRORIST FINANCING TYPOLOGIES 2004-2005 at <http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>

Experience over the last decade has shown that ARS can be misused for illegal purposes, including for both ML and TF. While ARS are largely composed of legitimate operators, some channels have nevertheless been involved in the transfer of funds related to illegal activities – or are themselves operating without proper authorisation from an oversight authority.

Hence ARS is a source of concern as far as their vulnerability to misuse for ML or TF purposes: however, increasingly other considerations have also become more evident, such as balancing the prevention of misuse with the need to ensure that flows of legitimate funds are not unnecessarily interrupted or pushed underground.

The FATF defines a *money or value transfer system* as a “financial service that accepts cash, cheques other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer system belongs.”¹⁰ This broad definition is intended to cover the full range of financial services involved in transferring money, including everything from banks to systems operating in full or in part outside conventional banking channels. *Alternative remittance systems* includes money/value transfer systems regardless of their legal status in particular jurisdictions and regardless of whether or not they are currently covered in part or in total by national regulatory systems.

Any internet search of ‘AML AND ARS’ will reveal that many organizations including the FATF are examining the subject of identifying areas where vulnerabilities and risks are present in terms of exposure to ML and TF, and proposing ways to minimize these risks.

The FATF has developed several measures that may be applied to ARS through the FATF Forty Recommendations¹¹ and in the Nine Special Recommendations (SR). For example, SR VI states that each country should ensure that individuals and entities that provide money transmission services are licensed or registered and otherwise subjected to the international standards on combating money laundering and terrorist financing, represented by the FATF 40 Recommendations and Nine Special Recommendations.

A number of countries have introduced specific measures as well. The FATF has noted that increasing awareness of the risks of misuse of ARS for transferring, transforming or disguising funds derived from criminal activities or intended for support to terrorist is important. Such an awareness can foster additional initiatives by national authorities in developing appropriate regulatory systems, as well as in strengthening the enforcement of those measures.

Harmonised approaches to legislative solutions and stronger international co-operation to detect criminal activities performed through ARS are fundamental, especially taking into account that countries are invariably linked to each other in a sending – receiving relationship.

Criminals are continuing to develop new and more sophisticated methods to avoid detection and to achieve their objectives more effectively. New trends are always emerging, including the current use of new payments methods and the application of cell phone technology to transfer remittances via e-money¹².

¹⁰ Interpretative Note to FATF Special Recommendation VI: Alternative Remittance, issued in February 2003.

¹¹ The Recommendations were revised in 2003.

¹² This is a term for digital money used for transactions over the Internet. In order to turn the Internet into a giant cybermall (online shopping center), companies have developed software that provides complete and secure order fulfilment over the Internet.

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

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

V. Regulatory Systems

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

Regulation varies substantially, from countries that require a banking licence for all institutions that transfer money to countries (mainly in the developing world) with no regulatory requirements, with the majority of countries between those two extremes, applying a regulatory regime to money remitters outside the banking sector.

In most cases there is one regulatory regime that applies to the entire ARS sector, although there are examples where countries apply a lighter or voluntary regime to certain categories of providers (*hawaladars*) or where a distinction is made between smaller and larger providers.¹³

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

¹³ The UAE, for example, has developed a registration system for hawala operators. For additional information, visit :<http://www.cbuae.gov.ae/>

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

The differences in the regulatory regime in different countries are largely mirrored in the way these entities are supervised or monitored. Supervision in a licensing regime is often in the hands of a financial supervisor, entails regular on site visits and strict reporting requirements and goes beyond AML/CFT requirements. Under a registration regime the checks are substantially less frequent or more “risk-based”; the monitoring focuses mainly or exclusively on AML/CFT requirements and is often implemented by other entities, such as the FIU, the tax authorities or the customs authorities.

Whether a country has a licensing or registration regime, most countries apply the regular AML/CFT requirements to the ARS sector, in particular the requirement to keep records, identify customers and to report suspicious transactions. Relevant differences occur in the thresholds that are applicable for the identification of customers, which vary from zero to EUR 15,000, and in the fact some countries require all transactions above a certain threshold to be reported (in addition to the reporting of suspicious transactions irrespective of the amount). Countries that apply a high threshold for identification will have to shift to a lower (or no) threshold to meet the requirements in SR VII. The FATF has not yet decided on the acceptability and the level of a threshold.

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

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

VI. Risk Areas

1. Terrorist Financing

The level of vulnerability for ARS misuse for terrorist financing differs from that associated with money laundering. ARS operations are used to provide funds for a specific terrorist action or to transmit funds that have been collected from legitimate (or illegal) sources to support future terrorist activities. The best defence against these transactions is the application of normal AML policies, that is, customer identification, know-your-customer procedures and suspicious transaction reporting.

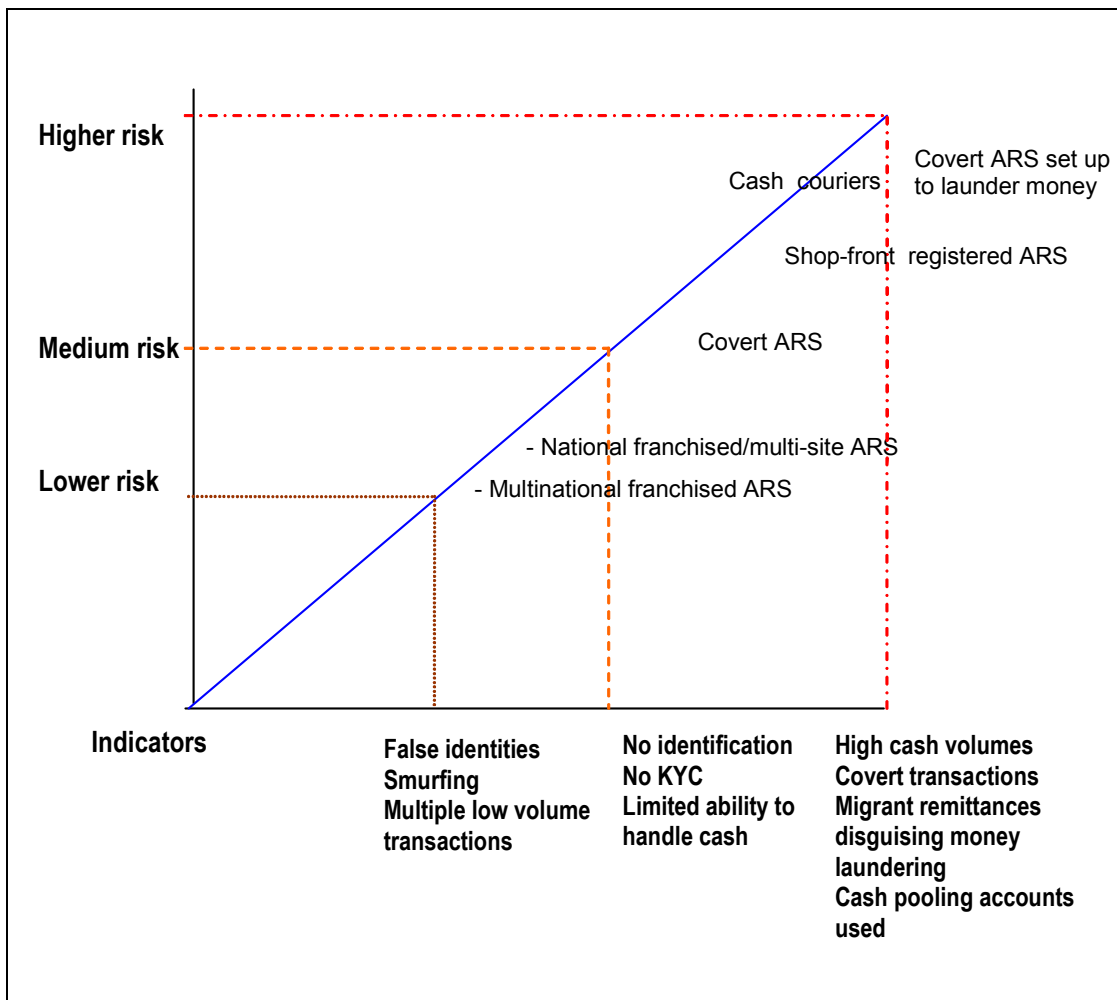


Figure 7: UK Risk Assessment; Source: United Kingdom

2. Money Laundering

The risks in ML are clearer. Any ARS can be misused to launder the proceeds of crime. The use of false identities and structuring are common techniques to which ARS is vulnerable. While specific risks will vary between jurisdictions, common elements can be identified. Factors to be considered in assessing risks are:

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

B. Risk Associated with Specific Types of ARS

Analyze the corridors — both for legitimate remittances and for the flows of criminal funds to determine risk and note that specific categories of ARS are different depending on the location, although common elements can be identified.

1. Franchised Multinational Companies

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

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

2. Multi Premises or Franchised National Companies

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

3. Signed Shop-Front Premises (one or more premises)

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

4. Overt ARS within Another Business

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

5. Covert ARS within Another Business

The extent of criminal activity is limited by the level of cash deposits that can be made without arousing suspicion. Suspicious transaction reports from banks and referrals from financial intelligence units are key ways of identifying this activity. This sector tends to

be tied to specific ethnic or immigrant groups and may therefore in some cases be a higher risk for exploitation for terrorist ML.

6. Covert ARS – No Premises

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

In the FATF study¹⁴, the highest volumes of criminal cash were handled by shop-front ARS that provided their services to a specific ethnic community. These operations have tended to be located in an urban area with a high concentration of the ethnic or immigrant population. Collectors in such money laundering operations have generally come from the same communities. These “collectors” have interacted with and provided ML services to a full range of criminals. The size of individual transactions has been between GBP 100,000 and GBP 500,000.

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

VII. How to Detect Illegal Activity

C. General ML/TF Indicators for Banks and Regulators

The following factors could be useful to indicate covert ARS operations and perhaps ML/TF activity:

- Regular high levels of cash deposits.
- Cash deposited at banks located at a distance from the ARS business premises.
- Regular high-volume international transfers to third party accounts in countries which are not destination countries at the end of known or usual remittance corridors.
- Cash volumes and international transfers in excess of demand for migrant remittances in the area (taking account of other operators).
- Cash volumes and international remittances in excess of average income of migrant account holders.
- Regular return of cheques for insufficient funds.
- Cash volumes and international remittances in excess of average income of migrant accountholders and/or in excess demand for migrant remittances in the areas (taking account of other operators)
- No business explanation for the size of business or cash volumes; and international remittances that are incongruent with the normal resources of legal entities (for example, foundations) in migrant community; wholesale *hawala* used to explain source of cash.

¹⁴ See Footnote 9.

- Book keeping records do not match banking operations.
- Transfers to jurisdictions where the ARS operator has no apparent relationship.
- Large transfers from account to potential cash pooling accounts.
- Large volume transactions recorded informally, using unconventional book keeping methods or in “off-the-record” books.
- Structuring of deposits to avoid reporting thresholds or simply in an attempt not to draw attention.

D. Specific Indicators for Banks in Connection with Cuckoo Smurfing

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

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

VIII. Role of Regulators

Role of the Financial Intelligence Unit (FIU)

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

However, remittance transactions related to ML or TF are more frequently than not carried out by occasional customers that do not enter into any durable relationship with the ARS provider. This lack of a continuing business relationship thus makes know your-customer and evaluation procedures more difficult to carry out. Moreover, one-off transactions can be disguised using a number of different deception techniques, and often no anomalies can be detected in the first instance.

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

these circumstances, the detection and analysis of suspicious transactions can prove particularly difficult.

a. The Role of the Supervisor

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

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

E. Active Detection by Law Enforcement and Customs Authorities

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

F. General ML/TF Indicators for Law Enforcement

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

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

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

G. Indicators for ARS Operators to Detect Criminal Misuse

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

IX. Issues for Consideration

Matters for policy makers to consider include the following:

- Need for **harmonised terminology** related to ARS.
- A relatively effective way to detect undeclared ARS-operators is the detection of the settlement transactions of these entities. Banks and money remitters should be provided with appropriate guidance for CDD and suspicious transaction reporting, in particular when dealing with (other) money remitters as customers.
- sharing of intelligence and evidence between countries effectively disrupts criminal ML or TF groups using ARS.
- **Currency transaction reports** (CTRs) help detect criminal activity in the money remittance sector.
- A **risk-based approach** focuses efforts on studying the ML techniques associated with ARS to help orient future investigative activity.

- Possible ARS settlement activity can be indicated by the regular **use of cash couriers** who attempt to avoid declaring cross-border carriage of funds.
- Money remitters engaged in ML or other illegal operations make use of **commercial operations** – in particular under- and over invoicing - to hide their settlement transactions.
- The use of **cash pooling accounts** by ARS operators, as well as incomplete or inaccessible book keeping techniques, would seem to require appropriate regulation and supervision.
- Impose regulations to identify depositors and beneficiaries of ARS transactions that do not have an apparent tie to the account holder.
- **Disruption of ARS ML controllers** is a valid tool which relies on close co-operation between investigators, regulators and criminal intelligence practitioners.

Elements of an Effective System

The choice of a registration or licensing regime is still an open debate with the common basic element of any regime remaining the need to identify ARS operators. Although it is difficult to determine which factors drive money remitters underground, overly strict regulation and supervision and associated costs could indeed play a role. However, given the evident involvement of registered money remitters in ML and TF schemes, it is equally clear that adequate regulation and supervision, including background checks on managers and owners of ARS-services, as well as legal measures to remove unsuitable managers after a negative background check are equally essential.

The lack of a threshold could be one of the factors that drives customers and therefore also operators underground. Suspicion-based identification below the given threshold is a recommended tool to combat smurfing. Automated analysis of ARS accounts, both by the ARS themselves and by banks, is also a useful tool for identifying and reporting this activity.

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

Money launderers and terrorist financiers will use "regulatory arbitrage" in exploiting ARS, by channelling their money through markets with limited supervision/monitoring of ARS or where it is easy to operate underground. Since money remittance (and settlement) can flow to different entities in different countries, it is relatively easy to take advantage of such weakness even if money is eventually remitted between two well-regulated markets. This underlines the need for a global implementation of AML/CFT standards in this sector.

Competent authorities, banks and money remitters must maintain an up to date knowledge of new methods and techniques. There remains a need to maintain a balance that includes and recognises the needs of migrant communities but prevents abuse of ARS. No regulatory system can ever be considered perfect, and there cannot be a "one-size-fits-all" solution. There is furthermore a need to maximise controls where the risks are highest while minimising the administrative burden on the industry and consumers. Covert ARS tend to serve specific communities. Therefore, creating a strong AML regulatory regime within which ethnic ARS can be included but still retain their traditional values is the best defence with international co-operation on intelligence, investigation and regulation the most

important tools in generating a respected global ARS sector as nearly all remitted funds will use conventional banking facilities and have an essential role to play.

X. Conclusion

The issues and risks of AML/CFT to financial sectors globally, that arise from the use of ARS are many and varied. The implications for developing new regulatory measures or refining existing ones are still being examined and there are a number of approaches to be adopted. Meanwhile the challenges posed by ARS continue to grow.