Risks Associated with Remittance Transactions

Preview

This chapter provides:

- An overview of the specific vulnerabilities of remittance channels to money laundering/terrorist financing risks.
- A discussion of regulatory and supervisory challenges when mitigating these risks.
- Guidance on key money laundering/terrorist financing risk mitigation measures for remittances.

Remittances are an important source of income for poor households in developing countries. At the same time, however, remittance channels can be a source of money laundering and financing of terrorism (ML/FT) risks. As remittance volumes grow, so do concerns about potential risks. Therefore, it is important for countries to promote accessible, efficient, but also secure remittance flows and to mitigate these risks. The most effective way to achieve this is by adopting a risk-based approach (RBA) to anti-money laundering/combating the financing of terrorism (AML/CFT) regulation and supervision. Financial institutions must ensure that such risk-based AML/CFT policies and procedures are proportionate with the ML/FT risks, and that they are relevant to the size and complexity of the institution, products offered, and customer types. Hence, to effectively regulate and supervise remittance service providers (RSPs), it is critical to understand the various risks present in the remittance market and transactions. This chapter provides a better understanding of the various types of ML/FT risks faced by RSPs by analyzing different aspects of the remittance business, and provides guidance on key risk mitigation measures.
How Vulnerable Are Remittance Channels to ML/FT Risks?

There is a general perception that remittances and wire transfers are more vulnerable to ML/FT risks than other financial activities such as deposit taking, lending, leasing, and money management. Indeed, there is a dedicated Financial Action Task Force (FATF) Recommendation to mitigate ML/FT risks arising from wire transfers (which also includes remittances). This is understandable since funds can be moved instantaneously to another country, and given the past evidence that remittances have been used in a criminal context for both money laundering and terrorism financing. Sending funds abroad makes tracing the money extremely challenging, particularly when transactions are conducted by operators not subject to or complying with AML/CFT obligations. This is even more so because reconstructing a money trail requires international cooperation, which is challenging, costly, and usually slow.

Within various remittance channels, Money or Value Transfer Services (MVTS)\(^1\) are usually perceived as more vulnerable to ML/FT risks than banks. Given that MVTS is a broad term used in the FATF Recommendations, which include not just money transfer systems but also value transfer systems, this study uses money transfer businesses (MTBs) as the collective term for certain non-bank financial institutions providing money transfer services (see figure 1.1 and table 1.1 in chapter 1).

Risks Related to Remittance Business Models

By the mere existence of recommendations specific to MTBs (FATF Recommendation on Money or Value Transfer Services and Wire Transfers) and the exclusion of MTBs from certain optional exemptions,\(^2\) the FATF Standards signal that they deserve special attention, as do certain other service providers or types of business relationships. Occasional or very limited activity cannot be the reason for exempting MTBs from being subject to FATF Recommendations. The other exemption clause, to prove that there is a proven low risk of ML/FT, can still be applied. Although meeting this exemption clause is certainly challenging, it is theoretically feasible.

Do we have evidentiary data to assert that MTBs are more vulnerable to ML/FT risk than other financial institutions? The short answer is that the results of the survey conducted for this study did not provide enough data to allow a definitive answer—either way. The survey attempted to collect information on cases and typologies where money transfer services are abused for ML/FT purposes, in order to gather fact-based evidence of possible increased exposure to ML/FT risks. Only a few countries were able to provide some responses to these questions. Where countries were able to provide information, it was available only in aggregated form that did not permit detailed analysis. For example, a total number of money-laundering cases was provided without a breakdown as to which financial institutions were used as conduits in such cases.

Based on this lack of evidentiary support, this study reaches the preliminary conclusion that a uniform and across-the-board perception of higher ML/FT
risks in the remittance sector is not warranted. As a consequence, the value and fairness of imposing higher AML/CFT requirements for every single country, every single channel, every single transaction, and every single service provider in the same manner is questionable. Rather, country-based assessments of risks are needed as a platform upon which to design and implement a genuinely risk-based AML/CFT regime for the remittance sector and transactions, in line with the RBA enshrined in the international standards.

The following two questions are analyzed to further elaborate on our arguments.

**Question 1: Do MTBs face higher ML/FT risk than banks?**

To the extent that countries assess the ML/FT risks in MTBs, take appropriate measures to mitigate the risks, regulate the industry by enacting laws and regulations, and enforce laws and regulations, MTBs should pose no greater risk than banks. In other words, MTBs do not necessarily face inherently higher ML/FT risks than banks through remittance services, nor do they pose inherently higher ML/FT threats than banks. The risks and threats are largely influenced by the risk mitigation measures, namely effective risk-based regulations and supervision. For example, if MTBs are unregulated, the risk of illicit flows through these MTBs increases not because of an aspect of risk that is inherent to remittances. The increase in risk occurs because of a simple consequence of the lack of regulation and supervision and, therefore, lack of internal control and due diligence measures by service providers. The risk is not related to the types of transactions but to the weakness in the supervisory regimes and supervision applicable to MTBs. Those wishing to hide illicit financial flows are likely to seek unsupervised entities to reduce their chance of detection.

Therefore, the answer in each country greatly depends on the exact business model framework, relevant national regulations, and other country circumstances and conditions, which combined define the country and sector ML/FT risk profile.

Before 2001, it was uncommon to regulate and supervise MTBs in most of the countries around the world. This informality of service providers certainly led to higher ML/FT risk. Now that most countries regulate MTBs or on a limited basis, ban MTB operations, the perceived risk generalization no longer seems justified—and, based on the available data, is not backed by a compelling typology. While 26 countries were surveyed, only 23 have MTBs that provide remittance services. Of those 23, 17 countries, or nearly 74 percent, indicated they had distinct laws, regulations, or directives regulating MTBs (see table B.9 in appendix B). Moreover, AML/CFT obligations applicable to MTBs in these countries appear to cover all key areas—customer due diligence (CDD), Suspicious Transaction Reports (STRs), currency transactions reports, record keeping, training, and internal control (see table B.13 in appendix B).

The surveyed countries provided data on the number of STRs filed by the various types of RSPs. The majority of sending countries were able to produce STR statistics with a breakdown by sector or type of financial institution. However, only 20–30 percent of the receiving countries were able to provide...
equivalent data. This reveals the need for an improvement in the way statistics are gathered; data segregation by sector is critical to a sound and comparative analysis, and to underpin risk analysis and risk-based supervision.

Analyzing STRs is only one method of risk analysis. Based on available STR data, in some countries (such as Jamaica), MTBs file the majority of STRs related to suspicious activity. This might indicate potentially higher ML/FT risks in MTBs, or it might simply represent defensive STR filing by MTBs, which would not indicate higher risks.

MTB involvement in ML/FT cases provides an additional perspective. Some surveyed countries provided the number of ML/FT cases involving financial institutions. However, only a few were able to point to the specific involvement of MTBs. Others did not provide disaggregated information pointing to the types of financial institutions involved in the schemes or used as a vehicle to launder money. This is an area where countries need to capture and make public more detailed information.

National regulations may also play a role in determining the overall ML/FT risk perception of banks compared to MTBs in a country. For example, regulatory requirements for CDD, Currency Transactions Reports, thresholds, and other requirements can differ between banks and MTBs, even if both types of institutions are conducting similar funds transfer/remittance transactions. While in some cases, this is important and warranted, in other cases, it is not. For example, if banks do not entertain walk-in customers\(^2\) or the type of customers is very different from those of MTBs,\(^5\) then having different CDD and other preventive measures may make sense. However, if the remittance market is very competitive and customers can easily go to banks or MTBs for services, then applying the same CDD and other regulatory requirements to remittances between banks and MTBs is natural.

In many sending countries, it is observed that banks view the MTBs and their agents as higher risk and even de-bank those client relationships. This de-banking has become an extremely pressing issue for regulators in those countries. One of the rationales put forward for such moves by banks is that banks are concerned about enforcement actions by regulators for serving customers whose AML/CFT standards are not compatible with or stringent enough to match banks’ internal controls.\(^5\) From this perspective, it may help banks if AML/CFT requirements for remittances are the same for banks and MTBs and this is indeed enforced. However, regulators need to carefully consider whether this move is feasible, practical, and suitable in their market and whether it will meet the overall objectives of enhancing integrity without pushing remittance transactions to the informal market. Remittance transactions are usually of smaller value, with an average of a few hundred dollars. In addition, some countries impose a ceiling on the permissible transaction value, usually around several thousand dollars. The small remittance value should be of less money-laundering concern, although there is still a debate about the risk related to terrorist financing. This debate is complex but, thus far, given the recent typology on terrorism financing, evidence of terrorist financing suggests that other channels such as banks are also often involved along with remittance channels.
Question 2: Do local MTOs generally face higher ML/FT risks than international MTOs when engaged in international remittances?

Most regulators largely consider international money transfer operators (MTOs), with their globalized operations, significant resources, and globally well-known names, to have established well-recognized regulatory compliance programs that mitigate ML/FT risks arising through their system. Local MTOs with smaller scale operations, fewer resources, and a lack of globally well-known names, are viewed as not having resources to develop effective compliance programs. This view, of course, presumes that the internal controls of international MTOs are reviewed for compliance and effectiveness by their home regulators and supervisors.

That said, the sheer number of transactions conducted by international MTOs dwarfs those of local MTOs. International MTOs also operate in a wider range of locations and countries, including in conflict zones and high ML/FT risk countries. The point here is not to favor local MTOs over international MTOs or vice versa, but to try to put things in context. Again, however, the survey provides no clear evidence on which to compare the risk profiles of local and international MTOs.

The role of agents in remittances is also an important factor in ML/FT risk assessment. As explained in chapter 1, agents may come in very different forms, ranging from established financial institutions such as banks, to nonfinancial institutions such as “mom and pop shops,” grocery stores, and gas stations. That local MTOs are more likely to enter into principal-agent relationships with such a range of actors is and should be part of the risk assessment, and of the design of the regulatory/ supervisory requirements to mitigate risks.

Such a survey and research cannot provide a definitive answer on the comparative level of ML/FT risks in the remittance sector. That said, and as noted above, the current lack of evidence calls for ML/FT risk assessments to be undertaken in each country, as a basis for undertaking a genuine RBA. Data are obviously needed in order to conduct an objective and accurate risk assessment; however, even with the limited data available, risk assessment can be undertaken, and this would be better than policy actions based on mere perception.

**Risks Associated with New Remittance Products**

Many MTBs are increasingly developing various innovative products and services for remittance transfers, expanding their distribution network, and improving their marketing and promotional strategies. Such developments have allowed MTBs to compete more effectively, reduce transfer costs, and improve financial accessibility and convenience for migrant workers and their families. Survey results show that nearly half of the sampled countries have MTBs that provide remittance transfers and applications through technological channels (see table 2.1). The most popular application observed in the surveyed countries is mobile phones, followed by Internet-based remittance services, use of debit or preloaded cards, and withdrawal from automated teller machines (ATMs) by the recipient. The use of credit cards is more prevalent in sending than
receiving countries. Table 2.1 shows that sending countries are far more advanced than receiving countries in terms of the use of various technologies, except with respect to the use of mobile phones, which is more widespread for remittances among receiving countries than sending countries.

Understanding the risks related to each of these products and services and appropriately regulating them is extremely important to ensure that ML/FT risks are mitigated, while not suppressing the growth and sustainability of these products and services in an increasingly competitive marketplace.

**Mobile Money**

Mobile money (M-Money) is often the first noncash service that clients in developing countries are able to access. While M-Money is not without ML/FT risk, it still poses less risk than cash. The transactions are recorded and are traceable, especially if clients are identified. Even when clients are not pre-identified, if law enforcement wishes to identify a particular unidentified client, the M-Money framework generally provides them with a rich source of identifying details, such as voice recordings, patterns of communication, and patterns of transactions. In addition, a mobile phone acts as a tracking device that can lead investigators to the actual person. Individually and collectively, these facts can render M-Money unattractive for abuse, thereby reducing the likelihood of the risk materializing.

Another important mitigating factor is that usually M-Money providers impose limits on the balance and frequency of M-Money transactions. It would require a significant and costly level of smurfing to launder proceeds through such channels.

Evidence on the impact of the availability of electronic channels on the use of cash is emerging. Japan’s central bank, the Bank of Japan, has already observed a correlation between the increased use of electronic channels, including M-Money, and an aggregate reduction in the level of physical cash (thus, the overall level of ML/FT risk involved with having physical cash in Japan may also have declined). The advance of electronic money systems in Japan has largely been the result of the ability to carry an electronic purse on a near field communication (NFC)-enabled mobile phone. A report published by the Bank of Japan has documented this trend, showing that there has been a slowing of the rate of increase in the amount of large coins in circulation (¥500 and ¥100) and a decrease in the amount of smaller coins in circulation (¥50, ¥10, ¥5, and ¥1) (see figure 2.1).
Risks Associated with Remittance Transactions

M-Money can therefore be used strategically to lower national ML/FT risk by facilitating the move away from “higher risk” cash transactions to relatively “lower risk” M-Money transactions (Chatain et al. 2011).

Prepaid Cards

During the last decade, prepaid cards have evolved rapidly and their functionalities have expanded, so that some prepaid cards can now be used to send and receive funds and to withdraw cash from ATMs.

The two main types of prepaid cards are open-loop and closed-loop cards. Prepaid cards gained popularity because they enable storing and carrying of value and substitute for carrying cash. Because closed-loop prepaid cards have limited use, open-loop prepaid cards are much more popular. Open-loop prepaid cards can be used to quickly move funds around the world by using the ATM network to withdraw funds, by purchasing goods and services, or by transferring funds to another card. No face-to-face transaction is required, which makes them attractive for ML/FT purposes. Prepaid cards are also particularly vulnerable to ML/FT threats because they could be loaded with high monetary values and are easier to transport undetected than transporting equal cash value using cash couriers.

The risk posed by anonymity or not identifying the cardholder when a card is purchased, registered, loaded, or reloaded, is relative to the card’s scope of use with respect to funding or purchasing limits, accessing cash, and whether the card can be used outside the country of issue. Prepaid cards can be funded in various ways—through banks, the Internet, small retail shops, or ATMs—thus,
involving different degrees of CDD. While funding prepaid cards via a bank account or through the Internet normally starts from an account or a payment instrument whose holder has been identified, cash funding can be totally anonymous (FATF 2013b).

The ML/FT risk posed by prepaid cards has increased in the last decade as prepaid cards have evolved to allow unlimited reloading and access to funds through the international ATM network. In addition, prepaid cards can easily be passed on to third parties, which is of particular concern when the card is anonymous. The risks are magnified when the prepaid card has a dual-user capability feature that allows the second card to be passed on to third parties to allow for remittance withdrawals.

The global outreach of prepaid cards for making payments or transferring funds is an important factor to consider when determining the level of risk. That is, the larger the number and wider the geographic location of the potential counterparties, the higher the ML/FT risk. In fact, regulatory and supervisory agencies in many jurisdictions worldwide have been hesitant to permit the use of prepaid cards because their vulnerability to ML/FT abuse is greater than that of traditional financial offerings.

Therefore, although prepaid cards are very useful, it is essential to have adequate AML/CFT policies, internal checks embedded in the product itself, and robust internal controls and monitoring mechanisms for transactions by service providers to ensure the cards are not used for illicit purposes.

**Internet-Based Remittance Transfers**

The rapid development and growth of Internet-based payment services has created opportunities for consumers and challenges for countries and private sector institutions in ensuring that these products and services are not misused for ML/FT purposes. Many Internet-based payment services have emerged globally using a variety of business models.

For large-value remittances, lack of verification of the users poses the greatest risks in terms of Internet-based remittance transfers. Fund transfers via credit card or bank account pose the least risk of ML/FT; however, this limits access only to those with a banking relationship. Nonbank wire transfers can fund online accounts via another Internet-based payment service that does not verify customer identification (ID), or by third-party funding. Some Internet-based service providers partner with prepaid card issuers and offer cash access to payment recipients via ATMs. While services that offer a cash option for both funding and payout can boost access among the unbanked, this may increase the potential threat of ML/FT risks by eliminating a paper trail on the source and use of funds transferred if no due diligence is conducted.

Not having physical contact, which is inherent to Internet-based transfers (access of service or in reloading) can lead to weaker customer verification, resulting in higher ML/FT risks. Such risks would vary with both the functionality of the product and the strength and enforcement of AML/CFT measures governing
these transactions. This poses challenges to the authorities to allow for wider financial inclusion opportunities to be gained through these innovative products while identifying and mitigating potential ML/FT risk factors.

To successfully mitigate the potential ML/FT risks related to Internet-based remittance transfers, the risk assessment should include various risk factors. Overall, Internet-based payment service providers that handle all aspects of the customer relationship (that is, registration, cash-in/cash-out, and transactions) that are subject to AML/CFT requirements are most likely to manage ML/FT risks better than decentralized service providers. The Internet-based providers can manage these risks better because they have more comprehensive information to monitor customers and their transactions and to enable better risk analysis.

**Risks Related to the Informal Remittance Market**

Whether the remittance market is regulated and supervised or not is one of the key factors in determining the vulnerability of the remittance sector to ML/FT risks. While many counties have moved to formalize the remittance market, the informal market still exists in many countries, albeit perhaps on a smaller scale. Informal players are commonly used by both illegal migrants who want to send remittances to their home country for legitimate needs and by criminals to move illicit money (such as proceeds from drugs, tax evasion, or other types of illegal activities) across borders. Informal channels can be used by undocumented migrants because they are usually cheaper, are faster, need less documentation than required by legal channels, and are the culturally preferred way of transferring funds. Criminals use informal channels because they lack CDD procedures, which facilitates the movement of criminal money without a paper trail.

Informal channels pose particular challenges not only because they may be used more frequently by criminals, but the informal channels may also be facilitators of money laundering and may even be controlled by criminal organizations and enterprises. There is no oversight of these informal service providers; in addition, paper trails may not be readily shared by these service providers, or the paper trails might not be easily understandable by law enforcement authorities.

While there appears to be an increasing trend toward formalization of the remittance market, many remittance corridors continue to remain less formalized (see map 4.1 in chapter 4).

**Regulatory and Supervisory Challenges**

Effective regulation and supervision are central to risk mitigation. This study emphasizes the need for risk-based regulation and supervision. However, in practice, it can be difficult to design the most effective RBA, but it should reflect each country’s specific circumstance. Recognizing that an ill-designed regulatory framework and poor supervision can increase ML/FT risks, this section provides guidance on how best to design effective risk-based regulation and supervision.
Detailed discussions on regulation and supervision are provided in subsequent chapters.

Avoiding Overregulation of the Remittance Market
In an effort to mitigate risks associated with remittances, some countries have in fact overregulated the sector to the extent that competition has been hindered by not allowing a variety of remittance business models to operate. Whereas banks are the entity most frequently permitted to conduct remittance services in the countries surveyed, enabling of a more diverse range of entities is advisable in countries with large informal sectors where most population segments still cannot access basic financial transfer services. This is particularly so because it will help formalize the sector, which in turn assists ML/TF prevention.

The establishment of a regulatory framework should not create access hurdles (such as too stringent CDD regulation that requires a number of documents even for a small transaction, irrespective of risks) and excessively push costs up by adopting either onerous one-size-fits-all, rules-based regulations or risk-based requirements based on an inaccurate (too high) analysis of risks.

Strengthening Supervision Mechanisms
In general, on-site supervision in most of the receiving countries surveyed is weak. Only 18 percent of the receiving countries examined all the MTBs at least once, while 55 percent of countries managed to conduct on-site examination on some MTBs. Another 27 percent of countries have not yet started examinations. Though off-site examination of MTBs is more common, a majority of the countries have adopted neither risk-based supervision nor ongoing monitoring of regulated entities in order to detect the red flags and take targeted actions where appropriate.

Although the supervising authorities in many countries have appropriate sanctioning powers, such as revocation and suspension of license or registration, in practice the number of suspensions and revocations is very small. In the surveyed countries, only one receiving and one sending country had more than five revocation or suspension cases in the last five years. It is imperative for countries to strengthen enforcement action because lack of enforcement of regulations increases vulnerabilities to ML/FT risks.

Risk Mitigation Measures for Remittance Markets
This section summarizes guidance on risk mitigation measures that can be helpful in addressing ML/FT risks in remittance markets.

1. Assess and understand ML/FT risks in remittance transfers. Assessing and understanding risk is a prerequisite in designing risk-based regulation and supervision. If a country already has a risk-based regulatory and supervisory framework, risk assessment can be used to evaluate whether the current framework needs to be revised. As risk assessment becomes even more important, the collection
of statistics in a manner that would assist better risk assessment will be critical. It is important to explore and analyze the detected money laundering and terrorist financing cases, record the available information, and break down the information on various sectors, classify the cases, identify typologies that involve the use of MTBs, and analyze the inherent risks posed by RSPs, delivery channels, products, clients, and others involved in the remittance market. The existence of inherent risk is, in itself, not necessarily a negative factor. The important question is whether those inherent risks can be mitigated. Effective risk mitigation, however, does not necessarily mean the complete elimination of risk. An example of the ML/FT risk assessment tool for financial inclusion product including remittances can be found in appendix C.12

In conducting risk assessment, all the relevant stakeholders need to be involved. Among those stakeholders are the financial sector regulator and supervisor, the Financial Intelligence Unit (FIU), and law enforcement authorities (police, prosecutors, and tax authorities, among others), depending on whether the assessment is national or sectoral. Private sector (industry representatives) participation is often useful to gain insights on the products and services being offered and to reflect on ML/FT risk concerns the sector faces. At the same time, the private sector is required to undertake its own ML/FT risk assessment of its services, products, customers, and more.13 The private sector is also required to conduct a risk assessment before the launch of new products or business practices or the use of new or developing technologies.14 FATF issued a guidance paper on risk assessment in February 201315 that provides information for countries to consider when undertaking the risk assessment.

2. Allow innovative mechanisms for customer identification and verification. CDD through customer ID and verification is a key ML/FT risk mitigation measure. ID is essentially asking basic information about the customer. Verification is confirming whether the information provided is correct. At the verification stage, reliable, independent source documents, data, or information are required. The verification of customer ID may be difficult in countries that have no reliable national identity card scheme due to an underdeveloped, insecure, or inadequate national ID infrastructure, or lack of other appropriate alternative forms of ID. In such circumstances, alternative verification methods should be considered. International standards and practices illustrate that significant flexibility and creativity can be applied in that respect. Examples of risk-based verification include15:

- Introduction of a threshold below which customer ID is done but does not require verification of customer’s identity.
- Verification of customer’s identity at their home and in their community in the absence of a formal ID.
- Requiring the loading or transfer of funds from a bank account or credit card.
3. **Set limits on loading value and use.** Placing limits on the maximum value that can be held or transferred through remittance products can be an effective mechanism to mitigate ML/FT risk. To counter the heightened ML/FT risk of open-loop prepaid cards, many prepaid card programs have introduced loading, withdrawal, and duration limits. If prepaid cards are used for person-to-person funds transfers, limits imposed on possible transfers can be an effective measure to mitigate the ML/FT risk. This can be enhanced through combining transfer limits with loading or withdrawal limits. Such limits may reduce the incentive for criminals to use prepaid cards for ML/FT purposes. However, threshold limits should be determined for each product on a risk-sensitive basis, and depending on the existence of other AML/CFT measures.

4. **Ensure adequate monitoring and other internal controls of MTBs.** Service providers can use their operating systems to facilitate effective internal controls by incorporating monitoring mechanisms. Installing automated controls in their information technology systems can be an effective AML/CFT risk mitigation measure, because transaction patterns can be more easily analyzed. For example, automated controls can quickly scan name, date of birth, and other relevant ID information and compare the data with various United Nations terrorism lists and other relevant data. Effective monitoring systems can be particularly useful where adequate up-front CDD measures cannot be undertaken. When the operation of certain MTBs is limited and small in size, they may not be able to install automated controls. In that case, software such as Excel can be used, which is still more effective than paper-based monitoring. Some small MTBs or certain agents may not have the capacity for any computer-based monitoring tool, however.

5. **Strengthen supervision/licensing/registration of remittance service providers.** National authorities should ensure that all MTBs (natural or legal persons) that provide remittance services are licensed or registered. As will be explained in chapter 4, there are pros and cons of choosing a licensing versus a registration regime. All MTBs should be subject to effective monitoring systems that are in line with FATF Recommendations. Countries should identify informal MTBs that provide these services without a license or registration, and offer appropriate incentives to the informal service providers to join the formal system. It is important to build awareness among the informal MTBs about the merits of joining the formal system. At the same time, authorities should understand incentives that drive service providers to be formal rather than informal. Addressing these incentives will most likely require tools beyond the AML/CFT realm because such action could pertain to tax issues, mistrust of government agencies, and, therefore, avoidance of government scrutiny or
oversight. The AML/CFT supervisory and regulatory requirements and thresholds should also be carefully reviewed.

After all these efforts, those who do not join but continue to be informal players should be identified and sanctioned. Targeted risk-based enforcement action is a powerful tool authorities can use. Informal agents should also be legalized through licensing or registration or by making the principal MTBs maintain a list of agents. As explained in chapter 4, while there are pros and cons of the respective approaches, the listing approach seems to provide the most effective method to bring agents under regulatory mechanisms and ensure better compliance. Countries should take measures to ensure that providers that use agents include them in their AML/CFT programs and monitor them for compliance.

In principle, every country should strive to achieve a balance between financial inclusion and financial integrity objectives with respect to remittance markets through an RBA to regulation and supervision. Chapters 3, 4, and 5 discuss the regulatory and supervisory framework followed in the surveyed countries, and include a review of regulating market entry and suggest how to best design the risk-based regulatory and supervisory framework.

Notes

1. The FATF Recommendations define MVTS as follows: “MVTS refers to financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi, and fei-chen.” The concept of MTB used in this paper is similar to the concept of MVTS used in the FATF Recommendations, but is slightly narrower than MVTS in that MTB does not include the concept of “value” transfer services as opposed to “money” transfers. And the type of money transfer is limited to “person-to-person remittances.”

2. See the Interpretative Note to FATF Recommendation 1 (Assessing risks and applying an RBA). Recommendation 1 provides an exemptions clause stating that “countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs [Designated Non-Financial Businesses and Professions] to take certain actions, provided: (a) there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or (b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.” However, the latter provision does not apply to MTBs, while all other financial activities are eligible for exemption if the criterion is met under this provision.
3. Nigeria has a bank-only model and the Republic of Korea and Serbia have bank and post office models.

4. Although MTB customers are usually considered walk-in customers in the majority of the countries surveyed, MTBs have many repeat customers. In Jamaica, for example, if a customer is a repeat customer who transfers at least once every three months, this customer will not be eligible for lower due diligence. See section “Threshold for the CDD Requirements” in chapter 3.

5. Whereas banks tend to have more substantial business relations with most of their customers, MTB customers are usually walk-in customers transferring cash one way. Because of different levels of business relationships, banks necessarily tend to have more information about their customers, sources of the customer’s funds, and expected transaction profile. This information provides a more solid base on which to “know your customer.”

6. Reasons for de-banking may also arise simply due to market competition, including because banks are interested in starting their own remittance business or service (beyond SWIFT transfers). Under this scenario, AML/CFT can be used as an excuse to de-bank MTBs.

7. Several studies have analyzed risks of M-Money and other new payment services and products. See, for example, Chatain et al. 2011. The FATF has issued two typologies papers on new payment methods (FATF 2006, 2010, 2013b).

8. See appendix D for more information on private sector adaptations undertaken to compete in an increasingly competitive remittance market.


10. Near field communication (NFC)-enabled mobile phones enable users to make payments and purchases through a mobile phone as if it was a credit or debit card, as long as participating merchants have NFC capability.

11. Closed-loop cards are merchant-specific, so they can be used for transactions exclusively with a particular merchant. Open-loop cards are associated with and bear the logo of an electronic payment network, such as Visa (2009), and they are honored wherever these networks are accepted (http://usa.visa.com/microsites/goresponsibly/pdf/pms_guide_prepaid_card.pdf).

12. The financial inclusion risk assessment tool was developed under a broader project to develop a national risk assessment methodology and its tool. Emiko Todoroki, the lead author of this study, was the project leader of the risk assessment tool, and Kuntay Celik and Wameek Noor were members of the project team sponsored by the Financial Market Integrity Service Line of the World Bank. Whereas not all remittance products may fall under the notion of “financial inclusion” product, given the focus of this study on how to balance the financial integrity and financial inclusion, appendix C focuses on the risk assessment of financial inclusion product.


15. See FATF 2013a. The lead author of this study was a member of this project and contributed to the drafting of this guidance paper.

16. Standard CDD measures would include identifying the customer (client) and verifying his or her identity; and identifying the ultimate beneficial owner (who would receive the money), where relevant, and verifying his or her identity.
References


