FATF

GUIDANCE FOR A RISK-BASED APPROACH

MONEY OR VALUE TRANSFER SERVICES

FEBRUARY 2016

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

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2016), *Guidance for a Risk-Based Approach for Money or Value Transfer Services,* FATF, Paris
www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML/CFT	Anti-money laundering / countering the financing of terrorism
CDD	Customer due diligence
DNFBPs	Designated non-financial businesses and professions
FIU	financial intelligence unit
HOSSP	Hawala and other similar service providers
INR.	Interpretive Note to Recommendation
ML	money laundering
MSB	money service business
MVTS	money or value transfer services
NPPS	new payment products and services
R.	Recommendation
RBA	risk-based approach
STR	suspicious transaction report
TCSP	trust and company service providers
TF	terrorist financing

GUIDANCE FOR A RISK-BASED APPROACH FOR MONEY OR VALUE TRANSFER SERVICES

This Guidance should be read in conjunction with:

- the FATF Recommendations, especially Recommendations 1, 10, 14, 16 and 26 (R. 1, R. 14, R.16 and R. 26), their Interpretive Notes (INR) and the Glossary
- the *FATF RBA Guidance for the banking sector*

other relevant FATF Guidance documents, such as:

- the *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*
- the *FATF Guidance on Politically Exposed Persons*
- the *FATF Guidance on AML/CFT and Financial Inclusion*
- the *FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services*
- the *FATF Guidance on the Risk-Based Approach for Effective Supervision and Enforcement*

relevant FATF typology reports, such as:

- *the FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers*
- *the FATF Report: The role of Hawala and other similar service providers in money laundering and terrorist financing*

INTRODUCTION AND KEY CONCEPTS

A. BACKGROUND AND CONTEXT

1. The risk-based approach (RBA) is central to the effective implementation of the revised FATF *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*, which were adopted in 2012[1]. The FATF has reviewed its 2009 RBA Guidance for money service businesses (MSBs), in order to bring it in line with the new FATF requirements[2] and to reflect the experience gained by public authorities and the private sector over the years in

1 FATF (2012).

2 The FATF Standards are comprised of the FATF Recommendations, their Interpretive Notes and applicable definitions from the Glossary.

applying the RBA. This revised version applies to the money or value transfer services (MVTS)[3] sector. The FATF will also review and update its other RBA Guidance papers[4] (based on the 2003 Recommendations), to be consistent with the 2012 FATF Recommendations.

2. The first draft of the RBA Guidance for the MVTS sector was drafted by the MVTS Project group, co-led by the UK and Mexico.[5] Representatives of the private sector were associated with the work and consulted on the draft document.[6]

3. The FATF adopted this updated RBA Guidance for MVTS providers at its February 2016 Plenary.

B. PURPOSE OF THIS GUIDANCE

4. The purpose of this Guidance is to:

- Support the development of a common understanding of what the RBA to AML/CFT entails for MVTS providers, banks and other financial institutions that maintain relationship with MVTS providers and competent authorities responsible for monitoring MVTS provider's compliance with their AML/CFT obligations;
- Outline the key elements involved in applying a RBA to AML/CFT associated to MVTS;
- Highlight that financial institutions that have MVTS as customers should identify, assess and manage the ML/TF risk associated with individual MVTS, rather than avoid this category of customers;
- Assist countries, competent authorities and MVTS providers in the design and implementation of a RBA to AML/CFT by providing general guidelines and examples of current practice;

---

3 These services are included in the FATF Glossary under "Financial institutions: Money or Value Transfer Services (MVTS) at point 4.

4 Between June 2007 and October 2009, the FATF adopted a set of guidance papers on the application of the RBA for different business sectors: financial sector, real estate agents, accountants, trust and company service providers (TCSPs), dealers in precious metals and stones, casinos, legal professionals, money services businesses (MSBs) and the life insurance sector: www.fatf-gafi.org/documents/riskbasedapproach/.

5 The project group was composed of FATF-members (Spain, Switzerland, South-Africa, Singapore, Japan, Norway, European Commission, New Zealand, United Kingdom, United States and Italy), Associate members (GIABA-Secretariat, Moneyval -through Albania, APG- through Sri Lanka, GIFCS-through Guernsey) and Observers (World Bank, UNODC), co-led by the UK and Mexico.

6 Comments were received from Bank of Tokyo-Mitsubishi UFJ, Russian Electronic Money Association, MoneyGram International Inc., Mizuho Bank Ltd, Asociación de Bancos de México, Actors Federal Credit Union, Association of UK Payment Institutions, Banking Association of South Africa, European Payments Institutions Federation (EPIF), Australian Bankers' Association, Union of Arab Banks, World Savings and Retail Banking Institute/European Savings and Retail Banking Group (WSBI/ESBG), Canadian MSB Association, The Netherlands Association of Money transaction offices (NVGTK), Western Union Company and Hong Kong Association of banks (HKAB).

- Assist countries in the implementation of the *FATF Recommendations* with respect to MVTS, particularly Recommendations 14 and 26; and
- Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on preventive and mitigating measures.

C. TARGET AUDIENCE, STATUS AND CONTENT OF THE GUIDANCE

5. This Guidance is aimed at the following audience:

- Countries and their competent authorities, including AML/CFT supervisors of MVTS providers and AML/CFT supervisors of banks that have MVTS providers as customers, and Financial Intelligence Units (FIU);
- Practitioners in the MVTS sector; and
- Practitioners in the banking sector that have or considering MVTS providers as customers.

6. It consists of four sections. Section I sets out the key elements of the RBA and needs to be read in conjunction with Sections II to IV, which provide specific Guidance to MVTS providers (Section II), to supervisors of MVTS providers on the effective implementation of a RBA (Section III) and to banks that have MVTS providers as customers and supervisors of banks that have MVTS providers as customers (Section IV). There are five annexes which provide examples of:

- countries' actions against unauthorised MVTS providers (Annex 1),
- supervisory practices for the implementation of the RBA to MVTS (Annex 2),
- supervisory practices for the implementation of the RBA to banking MVTS customers (Annex 3),
- private sector effective practices in application of RBA (Annex 4) and,
- compliance practices of and in relation to a low risk MVTS (Annex 5).

7. This Guidance recognises that an effective RBA will reflect the nature, diversity and maturity of a country's MVTS sector, the risk profile of the sector, the risk profile of individual MVTS providers operating in the sector and the legal and regulatory approach in the country. It sets out different elements that countries and MVTS providers could consider when designing and implementing a RBA. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the supervisory approach and legal framework as well as the risks present in their jurisdiction.

8. The Guidance takes into account that any financial institution, including certain MVTS providers can be abused for ML or TF. The TF risks were also highlighted in the recent FATF report in the context of emerging terrorist threats[7]. However, the Guidance also seeks to clarify that while certain MVTS providers may act as a conduit for such illegal funds transfers, this should not necessarily result into categorisation of all MVTS providers as inherently high ML/TF risk. The

[7] FATF (2015c).

overall risks and threats are influenced by the extent and quality of regulatory and supervisory framework as well as the implementation of risk-based controls and mitigating measures by each MVTS provider. The Guidance also recognises that despite these measures, there may still be left some residual risk, which would need to be considered by competent authorities and MVTS providers in devising appropriate solutions.

9. This Guidance is non-binding and does not overrule the purview of national authorities, including on their assessment and categorisation of the MVTS sector as per the country or regional circumstances, the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of countries and of the private sector and may assist competent authorities and financial institutions to effectively implement applicable *FATF Recommendations* using a risk-based approach.

D. SCOPE OF THE GUIDANCE: TERMINOLOGY, KEY FEATURES AND BUSINESS MODELS

Terminology

10. This Guidance applies to the provision of Money or Value Transfer Services (MVTS) as defined by the FATF:

> *Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, 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.[8]

11. There is a range of participants involved in the provision of MVTS. For the purpose of this Guidance, the following terminology is used:

- *MVTS provider*: Any natural or legal person who is licensed or registered to provide MVTS as a business, by a competent authority, including through agents or a network of agents.[9] This also includes HOSSPs meeting the aforementioned criteria.
- *Hawala and other similar service providers ("HOSSP")*: Generally referred to as entities that provide MVTS, particularly with ties to specific geographical regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value which is settled through trade, cash and/or net settlement over an extended period of time, rather than simultaneously with the transfer.[10]
- *Agent*: Any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.[11]

---

8 Glossary to the *FATF Recommendations.*

9 Consistent with the definition of *financial institution* in the Glossary to the *FATF Recommendations*. This does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. Refer interpretive Note to Recommendation 16.

10 For a full description, refer to the FATF typology report on *The role of Hawala and other similar service providers in money laundering and terrorist financing* (FATF, 2013b, 12-13). The report also lists out legitimate reasons for existence of these services as well as their vulnerability to abuse based on survey results. In some countries, these types of transactions are considered illegal.

11 Glossary to the *FATF Recommendations.*

MVTS Key features

12. Some of the key features of MVTS are as follows:

- MVTS can be an attractive, often lower cost option for persons that need to send money quickly to another person as funds can be picked up by a recipient in a relatively short timeframe, as opposed to waiting for domestic or international wire transfers that may take several days to process in some cases. The financial service provided by MVTS providers is often cheaper than more conventional banking services and is frequently used in regions with limited or no banking services.

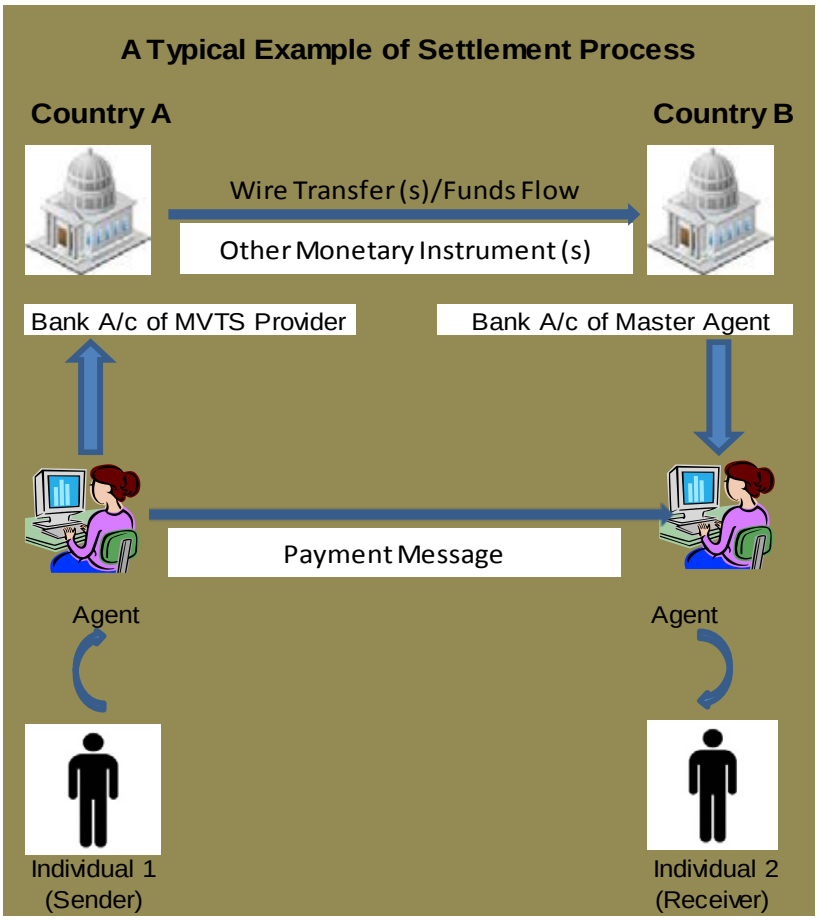
- MVTS providers operate in a variety of ways, but typically a MVTS provider or sending agent (acting on behalf of a MVTS provider) accepts payment of the money transfer, collects the required identification information, and enters the transaction and sender's applicable identification information and the destined receiver systematically at the point of origination.

- In the case of money transfer, the MVTS providers transfer the payment details to the pay-out agent that will provide the funds or their equivalent to the beneficiary of the transfer. The message is either sent directly to the agents or through a centralized clearing house that serves as a centralized hub for information that connects different agents of a provider.

- The money transfer is made available to the ultimate recipient, in the appropriate currency, at a receiving agent (acting also on behalf of a MVTS provider) location in the paying jurisdiction. The receiving agent will also collect and maintain the required identification information at the point of destination in accordance with the local applicable law.

- Pay-out methods vary by jurisdiction, but may include cash, cheque, money order, pay-out cards, mobile wallet, bank deposit or a combination.

13. A simple MVTS transaction and settlement process can be presented as follows:



14. The MVTS sector is made up of a very diverse group of organisations. An MVTS provider may be a small organisation with limited outlet locations such as grocery stores, drug-stores, pharmacies or convenience stores. It may also include a regional network of post offices or banks or other entities, which can be branches or agents. Most licensed or registered MVTS providers hold accounts at banks in order to process transfers and settle accounts with agents both domestically and internationally. However, settlement may be done through wire transfers, often involving aggregated amounts, processed through the international banking system. In addition, settlement can be done through third party payment providers.[12] However, settlement between and among MVTS providers and agents may also be undertaken through cash courier, net settlement or other mechanisms, without any direct wire transfer[13] between the originator and beneficiary.

12 FATF (2013b), p. 14.

13 The term wire transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to beneficiary person at a beneficiary financial institution. The originator and the beneficiary may be the same person. See Glossary Interpretative Note to Recommendation 16.

MVTS business models

15. There is a wide range of MVTS business models around the world. Not all MVTS providers are the same as they vary in size from small independent business to large multinational corporations. Some engage only in domestic transfers and others have a global footprint and transfer funds internationally. Others still may only have limited global transactions or operate in limited corridors, often between two countries that have a diaspora community. Besides the brick and mortar business models, there are also some MVTS providers that operate exclusively through the internet without any physical premise or network of agents. This Section does not seek to provide a complete description of all the MVTS business models; rather it seeks to provide an overview of common business models.

16. For the purposes of this Guidance, MVTS providers generally fall into the following broad groups:[14]

- **Banking institution offering MVTS** – Institutions that provide banking services including acceptance of deposits and other repayable funds from public; lending; and issuing or managing means of payment.[15]
- **Non-banking institution offering MVTS** – Any natural or legal person that provide MVTS as business, including through agents or a network, most commonly without the acceptance of deposits and other repayable funds from public. This includes HOSSP. Non-banking institutions offering MVTS may settle through the banking system and/or outside the banking system by cash or net settlement. Many MVTS providers may settle with agents, through the banking system either through centralized account and sub-accounts or through settlement between a centralized bank account held by the provider and individual bank accounts held by agents of the MVTS. It may also include virtual currency exchangers that fall within the definition of MVTS, where regulated as such.

17. Within the market of non-banking MVTS providers, the size and complexity of the providers vary significantly and various business models are adopted. Providers can include international MVTS providers, post offices, micro-finance institutions, mobile network operators[16], exchange houses, payment institutions[17], escrow account services, bill payment and IT and digital payment services and money transfer operators. Providers of MVTS services typically specialise along retail, commercial and wholesale lines.

---

14 Described based on financial activity being performed and may vary depending upon the regulatory framework of each jurisdiction.

15 Banking activities are activities or operations described in the FATF Glossary under "Financial Institutions", in particular 1, 2, and 5.

16 *Mobile Network Operator*: An entity that provides the technical platform to allow access to the funds through the mobile phone. In some jurisdictions, these can also be MVTS providers if they extend remittance services.

17 The term *"Payment Institutions"* is mostly related to the EU context (Payment Services Directive), which offer payment services alongside banks and other financial institutions.

18. While this Guidance is applicable to all MVTS providers, it is primarily intended for non-banking institution MVTS, including HOSSP. Banking institutions offering MVTS should consider this Guidance in conjunction with the *FATF Guidance for a Risk-Based Approach: The Banking Sector*.

Distribution channels: Agents

19. The nature and structure of agents and their relationships with MVTS providers similarly vary. International MVTS providers often have extensive agent networks spread across multiple jurisdictions. Some MVTS providers operate only domestically. Agents can include small independent entities with a contractual relationship directly with the MVTS provider to provide services on their behalf. Alternatively, agent networks may operate on a tiered structure where an agent operating on behalf of its established network of entities (e.g. through a chain of retail outlets) enters into a contractual relationship with the MVTS provider. Depending on domestic regulations, agents may require licensing or registration. Some agents may be financial institutions or obliged entities in their own right, while others may provide financial services as an ancillary business only.

20. MVTS providers may rely on foreign banks or other MVTS providers to pay funds to beneficiaries through currency drawing arrangements or otherwise, without entering into an agent relationship with these counterparties.

21. MVTS providers that are not multinational institutions may also use agents or a network of agents. The number of agents may be limited and they may be present only in certain geographical areas. In such cases, agents may have a contractual relationship with the principal MVTS provider, or services may be offered on behalf of the MVTS provider without the presence of a formal, written contract.

HOSSP

22. MVTS providers also include providers of *hawala* and other similar services. Providers of *hawala* and other similar services, like many other MVTS providers, generally send remittances of low value, though at times, this may also include high value business transfers. Such providers provide services to migrant communities, operate within a community, and are visible and accessible to their customers. Many such providers often run other businesses in addition to MVTS, and belong to networks of similar operators in other countries.[18] Some hawala providers also offer a more 'mainstream' non-hawala MVTS and mix and match the two approaches.

Relation to NPPS and VC Guidance

23. Some New Payment Products and Services (NPPS) fall within the definition of MVTS and should be licensed or registered and subject to effective monitoring systems as required by Recommendation 14. The *FATF 2013 Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services* (FATF 2013 NPPS Guidance) is relevant for NPPS

[18] FATF (2013b), p. 13. The report further highlights that while the most significant reasons for vulnerability of these services are jurisdiction-specific, lack of supervisory resources and settlement through value or cash makes HOSSPs transactions particularly difficult for law enforcement to follow the money.

which fall within the definition of MVTS. In some jurisdictions virtual currency exchangers may fall within the definition of MVTS. The FATF published a separate Guidance document on a Risk- Based Approach to Virtual Currencies in 2015.[19]

E. FATF RECOMMENDATIONS APPLICABLE TO MVTS PROVIDERS

24. The *FATF Recommendations* relating to MVTS under Recommendation 14 and its Interpretive Note include specific requirements for countries with respect to MVTS. Additionally, MVTS providers are also considered to be *financial institutions* under *FATF Recommendations*[20] and should be subject to the full range of AML/CFT preventive measures in Recommendations 9-23, including, for example, Customer Due Diligence (CDD), record keeping and reporting of suspicious transactions. R.10 requires financial institutions to conduct CDD measures when:

i) establishing business relations;

ii) carrying out occasional transactions:

   1. above the applicable designated threshold (USD/EUR 15 000); or

   2. that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

iii) there is a suspicion of money laundering or terrorist financing;

iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

25. Under Recommendation 26, MVTS providers should be subject to adequate regulation and supervision or monitoring, having regard to the ML/TF risks in that sector. This is outlined further in Section III(b) of this Guidance.

Box 1. **Recommendation 14: Money or value transfer services**

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use

19 FATF (2015b).

20 MVTS providers are considered financial institutions- Refer point 4 of the definition of the term 'financial institution' as contained in Glossary.

agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

Interpretive Note to Recommendation 14

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the *FATF Recommendations*) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the *FATF Recommendations*.

Box 2. **Interpretive Note to Recommendation 16**

[…]

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

(a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

[…]

Cross-border provision of services

26. Some MVTS providers provide services across national borders through establishments, including through a network of agents operating in another country. Competent authorities of the MVTS provider, acting across national borders with a physical presence through one or several agents established in another country (home country licensing/registration competent authorities), should liaise with the MVTS's host authorities to ensure any ML/TF concerns are adequately addressed[21]. Under the *FATF Recommendations*, countries should ensure that MVTS providers are

[21] Through applicable passport mechanisms. In the context of MVTS' cross border activities through agents established in another country, refer to the directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and

subject to supervision and monitoring for compliance with AML/CFT laws[22], in accordance with the institutional framework of the host country. This is without prejudice to supranational rules that would enable MVTS providers to supply services throughout the supranational jurisdiction on the basis of the legislation prevailing in the countries in which they are situated, without requiring from the host country to impose licensing or registration obligations on entities situated in another country and providing cross-border services.

27. In certain cases, MVTS are also often offered over the internet and there may be no physical presence (i.e. head office, branch or agent network) in the country where the transaction is sent or received. Competent authorities of the host jurisdiction in which the MVTS provider provides services without being physically present should liaise with the MVTS's home authority (which licenses/registers that MVTS provider and in whose jurisdiction, the MVTS provider is incorporated or resides), as appropriate to ensure that any ML/TF concerns are adequately addressed without prejudice to the right of the host country to require the submission of STRs, other threshold reports or other relevant information to the local authorities of the country where the MVTS provider operates. Similarly for AML/CFT supervision or monitoring of the MVTS providers, the home country authorities should also engage with the competent authorities of the host country where MVTS provider provides services.

28. Cross-border provision of services (including through agents or over the internet or otherwise) highlights the importance of international cooperation among the competent authorities of the relevant jurisdictions. Such international cooperation can be spontaneous or on request depending upon the nature of the specific situation.

SECTION I – THE FATF'S RISK-BASED APPROACH TO AML/CFT

A. WHAT IS THE RISK-BASED APPROACH?

29. The RBA to AML/CFT means that countries, competent authorities and MVTS providers[23], are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively and efficiently.

30. When assessing ML/TF risk[24], countries, competent authorities and MVTS providers should analyse and seek to understand how the ML/TF risks they identify affect them and take appropriate measures to mitigate and manage those risks. The risk assessment, therefore, provides the basis for the risk-based application of AML/CFT measures.[25] For MVTS providers, this will require an investment of resources and training in order to maintain an understanding of the ML/TF risk faced

repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

22 R.14, R.16 and R.26.

23 Including both legal and natural persons, see definition of "Financial institutions" in the FATF Glossary.

24 FATF (2013a), paragraph 10.

25 FATF (2013a), paragraph 10. See also Section I D for further detail on identifying and assessing ML/TF risk.

by the sector as well as specific to its products and services, its customer base, jurisdictions operated in, and the effectiveness of actual and potential risk controls that are or can be put in place. For supervisors, this will require maintaining an understanding of the ML/TF risks specific to the MVTS providers they supervise, and the degree to which AML/CFT measures can be expected to mitigate such risks. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken reasonable AML/CFT measures to identify and mitigate risks, but is still used for ML or TF purposes in isolated instances.

B. THE RATIONALE FOR A NEW APPROACH

31. In 2012, the FATF updated its Recommendations to keep pace with evolving risk and strengthen global safeguards in order to further protect the integrity of the financial system by providing governments with the tools they need to take action against financial crime.

32. One of the most important changes introduced was the increased emphasis on the RBA to AML/CFT, especially in relation to preventive measures and supervision. Whereas the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations consider the RBA to be an 'essential foundation' of a country's AML/CFT framework.[26] This is an over-arching requirement applicable to all relevant *FATF Recommendations*.

33. According to the introduction to the *FATF Recommendations*, the RBA allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.

34. The application of a RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Recommendations by countries and financial institutions.[27]

C. APPLICATION OF THE RISK-BASED APPROACH

35. The FATF standards do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML/TF; however the overall risk should be determined through an assessment of the sector at a national level. Different entities within a sector will pose higher or lower risk depending on a variety of risk including products, services, customers, geography and the strength of the entity's compliance program. Recommendation 1 sets out the scope of the application of the RBA as follows:

- Who should be subject to a country's AML/CFT regime: In addition to the sectors and activities already included in the scope of the *FATF*

26 R. 1.

27 The effectiveness of risk-based prevention and mitigation measures will be assessed as part of the mutual evaluation of the national AML/CFT regime. The effectiveness assessment will measure the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyse the extent to which a country's legal and institutional framework is producing the expected results. Assessors will need to take the risks, and the flexibility allowed by the RBA, into account when determining whether there are deficiencies in a country's AML/CFT measures, and their importance (FATF, 2013f).

Recommendations[28], countries should extend their regime to additional institutions, sectors or activities if they pose a higher risk of ML/TF. Countries could also consider exempting certain institutions, sectors or activities from some AML/CFT obligations where specified conditions are met, such as proven low risk of ML/TF and in strictly limited and justified circumstances.[29]

- How those subject to the AML/CFT regime should be supervised or monitored for compliance with this regime: Supervisors should ensure that financial institutions and DNFBPs are implementing their obligations under R.1. AML/CFT supervisors should consider a MVTS provider's own risk assessment and mitigation and acknowledge the degree of discretion allowed under the national RBA, while INR 26 further requires supervisors to themselves adopt a RBA to AML/CFT supervision.
- How those subject to the AML/CFT regime should be required to comply: The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are assessed as lower, simplified measures may be permitted. This means that the range, degree, frequency or intensity of preventive measures and controls conducted will be stronger in higher risk scenarios. Conversely, where the ML/TF risk is assessed as lower, standard AML/CFT measures may be reduced, which means that measures must respond to each of the required four CDD components at applicable thresholds[30]. ((i) identification and verification of the customer's identity; (ii) identification of the beneficial owner; (iii) understanding the purpose of the business relationship; and (iv) on-going monitoring of the relationship), but the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. In all the individual cases of MVTS providers, where risk is assessed at a standard level, the standard AML/CFT controls should apply.
- Consideration of the engagement in customer relationships with MVTS providers: Through the implementation of the RBA, financial institutions should identify, assess and understand their ML/TF risks, and manage the risk by taking commensurate action to mitigate the identified risks. This does not imply that institutions should seek to avoid risk entirely, for example, through wholesale termination of customer relationships for certain sectors. Wholesale refusal of services or termination of services to a

28 See Glossary, definitions of "Financial institutions" and "Designated non-financial businesses and professions".

29 See INR.1.

30 Recommendation 10 requires that CDD measures are always required where there is a suspicion of ML/TF.

class of customers may give rise to financial exclusion risk and may also give rise to reputational risk. Even if the MVTS services are considered as vulnerable to the risks of ML/TF based on risk assessment, it does not mean that all MVTS providers and all MVTS customers or operations pose a higher risk when taking into account the risk mitigating measures that have been put in place.

- The FATF does not support the wholesale termination or restriction of business relationships to MVTS providers (or other sectors) to avoid, rather than manage, risk in line with the FATF's risk-based approach. Rather, financial institutions should take into account the level of ML/TF risk of each individual MVTS provider customer and any applicable risk mitigation measures whether these are implemented by the financial institution or the MVTS provider customer. Usually the RBA presumes that the risk associated with any type of customer group is not static and the expectation is that within a customer group, based on a variety of factors, individual customers could also be classified into risk categories, such as low, medium or high risk, as appropriate. Measures to mitigate risk should be applied accordingly.

D. FINANCIAL INCLUSION AND AML/CFT

36. MVTS play an important role in supporting financial inclusion. In general terms, financial inclusion is about providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural and undocumented persons, who have been underserved or excluded from the regulated financial sector at an affordable cost in a fair and transparent manner. It is also about making a broader range of financial services available to individuals who currently may have access to only basic financial products.

37. Money transmitters, a type of MVTS, transfer remittances. Remittances are an important financial service for people in many developing countries and are a powerful enabler of financial inclusion. However, for AML/CFT purposes, it is important that financial products and services, including MVTS, are provided through financial institutions subject to adequate regulation in line with the *FATF Recommendation.*[31] This will potentially reduce overall ML/TF risk in the financial system by bringing customers into the regulated sector. MVTS may be many customers' first or only interaction with the financial sector. Therefore, a well-designed and functioning AML/CFT policy and supervisory framework for MVTS may foster greater financial inclusion. Similarly policies that encourage financial inclusion may in turn lead to stronger AML/CFT regime, thereby reinforcing the complementary objectives of the two approaches.

38. A RBA may help foster financial inclusion, especially in the case of low-income individuals who experience difficulties in accessing the mainstream financial system. On the contrary, an indiscriminate termination or restriction of business relationships to MVTS providers without

31 FATF (2013d), p. 12.

proper risk assessment and mitigation measures could potentially increase the level of financial exclusion, diverting the customers towards services and channels bearing an increased level of risk.

SECTION II – GUIDANCE FOR MVTS PROVIDERS

39. The RBA to AML/CFT aims to foster the development of managing and mitigating measures that are commensurate with the ML/TF risks identified. In the case of MVTS providers, this applies to the types of products and services MVTS providers offer, the way they allocate their compliance resources, organise their internal controls and internal structures, and implement policies and procedures to manage and mitigate risk and deter and detect ML/TF, also taking into account agent networks.

A. RISK ASSESSMENT

40. The risk assessment forms the basis of a MVTS provider's RBA. It should enable the MVTS provider to understand how, and to what extent, it is vulnerable to ML/TF. It will often result in a stylised categorisation of risk, which will help MVTS providers determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk. It should always be properly documented, regularly updated and communicated to relevant personnel within the MVTS provider. MVTS provider's risk assessment should be commensurate with the nature and complexity of the business, the type of products and services offered, the conditions of the proposed transactions, the distribution channels used and the customers' characteristics. This includes consideration of the following factors: the nature and size of the MVTS providers' business, including whether there are multiple subsidiaries, branches or agent networks offering a wide range and variety of financial products and services; the risk profile of its customers, including whether their customer base is more diverse across different geographical locations; the extent to which the products and services offered are consistently below a given threshold; and the extent to which the MVTS provider is vulnerable to ML/TF threats.

41. Combating terrorist financing and money laundering is a global priority. MVTS providers should consult various sources of information in order to identify, manage and mitigate these risks.[32] This includes taking into account the typologies, risk indicators, red flags, guidance and/or advisories issued by the national competent authorities and FATF. Furthermore, in identifying and assessing indicators of ML/TF risk to which they are exposed, MVTS providers should consider a range of factors which may include:

- The nature, scale, diversity and complexity of their business and their target markets;
- The proportion of customers already identified as high risk;
- The jurisdictions the MVTS provider is operating in or otherwise exposed to, either through its own activities or the activities of customers, especially in jurisdictions with greater vulnerability due to contextual and various risk

[32] For example, in relation to terrorist financing, see the FATF, 2015c and 2015d, and the countries that are in the FATF's International Cooperation Review Group (ICRG) process.

factors such as the prevalence of crime, corruption, financing of terrorism, as well as the general level and quality of governance, law enforcement, AML/CFT controls, regulation and supervision, including those listed by FATF;

- The distribution channels, including the extent to which the MVTS provider deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD, the complexity of the payment chain and the settlement systems used between operators in the payment chain, the use of technology and the extent to which agent networks are used;
- The internal audit and regulatory findings; and
- The volume and size of its transactions, considering the usual activity of the MVTS provider and the profile of its customers.[33]

42. Where appropriate, MVTS providers may cooperate, for example, at an industry or country level to produce institutional assessment tools that may be used by individual providers to produce their risk assessments.[34]

43. In preparing their assessment, MVTS providers should take into account quantitative and qualitative information obtained from relevant internal and external sources, such as heads of business, national and sector risk and threat assessments, crime statistics, lists and reports issued by inter-governmental international organisations and national governments, and AML/CFT mutual evaluation and follow-up reports by FATF or associated assessment bodies as well as typologies. They should review their assessment periodically and in any case, when their circumstances change or relevant new threats emerge.

44. ML/TF risks may be measured using various categories. Application of risk categories provides a strategy for managing potential risks by enabling MVTS providers to subject customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer risk; product/service risk and agent risk. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary from one institution to another, depending on their respective circumstances and risk management. Consequently, MVTS providers will have to make their own determination as to the risk weights; however, parameters set by law or regulation may limit a business's discretion.

45. While there is no agreed upon set of risk categories, the examples provided herein are the most commonly identified risk categories. There is no one single methodology to apply to these risk categories, and the application of these risk categories is intended to provide a strategy for

33 INR 1 and 10.

34 The *Groupe Speciale Mobile Association* (GSMA), which is a global association of mobile service providers, has developed a paper which sets out their view and interpretation of how the *FATF Recommendations* apply to mobile payment service providers and what risks and risk mitigation measures might apply. This paper has not been endorsed by the FATF, but is referenced here as one example of a relevant industry initiative. See also Chatain *et al* (2011) for a mobile money risk assessment matrix.

managing the potential risks. The following risk categories could be considered alone or in conjunction with other risk categories:

Country/Geographic Risk

46. There is no universally agreed upon definition or methodology for determining whether a particular country or geographic area (including the country/geographical area within which the MVTS provider operates) represents a higher risk for ML/TF. Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may be considered as indicators of risk include:

- Countries/areas identified by credible sources[35] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations organisation.
- Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

Customer Risk

47. MVTS providers should determine whether a particular customer poses higher risk and the potential impact of any mitigating factors on that assessment. Such categorisation may be due to customer's occupation, behaviour or activity. These factors individually, may not be an indication of higher risk in all cases, but a combination thereof may certainly require greater scrutiny. Categories of customers whose business or activities may indicate a higher risk include:

- Customer or counterpart is another MVTS or a financial institution which has been sanctioned by respective national competent authority for its non-compliance with the AML/CFT applicable regime and is not engaging in remediation to improve its compliance.

35 "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

- Customer conducting their business relationship or transactions in unusual circumstances, such as:
  - Customer who travels unexplained distances to locations to conduct transactions.
  - Customer networks; i.e. defined groups of individuals conducting transactions at single or multiple outlet locations or across multiple services.
  - Customer owns or operates a cash-based business that appears to be a front or shell company or is intermingling illicit and licit proceeds as determined from a review of transactions that seem inconsistent with financial standing or occupation.
- Politically Exposed Person or his/her family members or close associates and where beneficial owner of a customer is a politically exposed person, as covered under Recommendation 12.
- Non face-to-face customer, where doubts exist about the identity of such customer.
- Customer who uses agents or associates where the nature of the relationship or transaction(s) makes it difficult to identify the beneficial owner of the funds.
- Customer knows little or is reluctant to disclose details about the payee (address/contact info, etc.)
- Consumer gives inconsistent information (e.g. provides different names).
- Customer involved in the transactions that have no apparent ties to the destination country and with no reasonable explanations.
- Suspicion that the customer is acting on behalf of a third party but not disclosing that information or is being controlled by someone else (his/her handler). For example, the customer picks up a money transfer and immediately hands it to someone else or someone else speaks for the customer, but puts the transaction in his/her name.
- Customer who has been the subject of law enforcement sanctions (in relation to proceeds generating crimes), known to the MVTS provider.
- Customer who offers false/fraudulent identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents (e.g. use of identification cards or documents in different names without reasonable explanation).
- Customer whose transactions and activities indicate connection with potential criminal involvement, typologies or red flags provided in reports

produced by the FATF or national competent authorities (e.g. FIU, law enforcement etc.).

- Customer whose transaction patterns appear consistent with generation of criminal proceeds; *e.g.* illegal drug growing season, drug trafficking, illegal immigration and human trafficking, corruption etc.; based on information available with the MVTS provider.

Product/Transactions/Service Risk

48. An overall risk assessment should also include determining the potential risks presented by products and services offered by a MVTS provider. A MVTS provider should be mindful of the risks associated with new or innovative products or services not specifically offered by the MVTS provider, but that make use of the MVTS provider's systems to deliver the product or service. The FATF 2013 NPPS Guidance determines the risks involved in the provision of NPPS, including through consideration of any relevant risk factors and risk mitigation measures. Determining the risks of products and services could include a consideration of their attributes as well as any risk mitigation measures put in place in respect thereof and could include factors such as:

- Products or services that may inherently favour anonymity or products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone.
- Products or services that have a very high or no transaction limit.
- The global reach of the product or service offered.
- The complexity of the product or service offered.
- Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.

49. The risk associated with the transaction may also vary depending on whether the MVTS provider is sending or receiving the transaction. An overall risk assessment should include a review of transactions as a whole. This should include a consideration of such factors as:

a) Transactions sent or attempted:

- Customer's behaviour at point of origination:
  - Customer structures transaction in an apparent attempt to break up amounts to stay under any applicable CDD threshold- avoiding reporting or record keeping.
  - Transaction is unnecessarily complex with no apparent business or lawful purpose.
  - Number or value of transactions is inconsistent with financial standing or occupation, or is outside the normal course of business of the customer in light of the information provided by the customer when

conducting the transaction or during subsequent contact (such as an interview, discussion or based on information provided to tax authorities and made available to the MVTS provider etc.)

- Customer offers a bribe or a tip other than where a tip is customary or is willing to pay unusual fees to have transactions conducted.
- Customer has vague knowledge about amount of money involved in the transaction.
- Customer makes unusual inquiries, threatens or tries to convince staff to avoid reporting.
- Customer sends money internationally and then expects to receive an equal incoming transfer or vice versa.
- Customer wires money to illegal online gambling sites. Email addresses containing gambling references or transfers to countries with large numbers of internet gambling sites.
- Customer wires money to higher-risk jurisdiction/country/corridor.
- Customer attempts a transaction, but given he or she would likely be subject to the CDD monitoring, cancels transaction to avoid reporting or other requirements.
- Customer transfers money to claim lottery or prize winnings or to someone he or she met only online. Transfer towards credit card or loan fee or for employment opportunity or mystery shopping opportunity. All indicators of potential consumer fraud.
- Senders appear to have no familial relationship with the receiver and no explanation forthcoming for the transfer.

- Activity detected during monitoring (in many of these scenarios the customer's activity may be apparent both during point-of-sale interaction and during back-end transaction monitoring):
  - Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
  - Unusually large aggregate wire transfers or high volume or frequency of transactions with no logical or apparent reason.
  - Customer uses aliases, nominees or a variety of different addresses.
  - Customers whose concentration ratio of transfers made to a jurisdiction is notably higher than what is to be expected considering overall customer base.
  - Customer transfers/receives funds from persons involved in criminal activities as per the information available.

- A network of customers using shared contact information, such as address, telephone or e-mail, where such sharing is not normal or reasonable explicable.
- Transfers to HOSSPs in destinations where such transactions are known to the MVTS provider to be considered illegal.

b) Transactions received:

- Concerning the implementation of R16 on wire transfers, MVTS providers should pay special attention:
  - To transactions that are not accompanied by the required originator or beneficiary information.
  - When additional customer or transactional information has been requested from an ordering MVTS provider, but has not been received.
- Large number of transactions received at once or over a certain period of time which do not seem to match the recipient's usual past pattern (e.g. during illicit drug production seasons, towards migrant smuggling etc.).

Distribution Channels Risk, namely Agent Risk

50. An overall risk assessment should analyse specific factors which arise from the use of agents as a business model to facilitate the delivery of MVTS. In some cases these agents may also use the products and services themselves. It is important for MVTS providers to ensure that they understand who the agent is, and that they are not criminals or criminal associates. Assessing agent risk is more complex for MVTS providers with an international presence due to varying jurisdictional requirements and potential risk of non-compliance by agents of the applicable local AML/CFT regulations and the logistics of agent oversight. This agent risk analysis should include such factors as the following based on the extent that these are relevant to the MVTS providers' business model:

- Agents representing more than one MVTS provider.
- Agents located in a higher-risk jurisdiction/country or serving high-risk customers or transactions.
- Agents determined to have "politically exposed person" status.
- Agents conducting an unusually high number of transactions with another agent location, particularly with an agent in a high risk geographic area or corridor.
- The transaction volume of the agent is inconsistent with either overall or relative to typical past transaction volume.
- Transaction pattern indicating value of transactions just beneath any applicable CDD threshold.

- Agents that have been the subject of negative attention from credible media or law enforcement sanctions.
- Agents that have failed to attend or complete the training programs.
- Agents that operate sub-standard compliance programs, i.e. programs that do not effectively manage compliance with internal policies, monetary limits, external regulation, etc.
- Agents with a history of regulatory non-compliance and that are unwilling to follow compliance program review recommendations, and therefore subject to probation, suspension or termination.
- Agents who fail to provide required originator information upon request.
- Agents whose data collection or record keeping is lax, sloppy or inconsistent.
- Agents willing to accept false identification or identification records that contain false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers.
- Agents with a send-to-receive ratio that is not balanced, consistent with other agents in the locale, or whose transactions and activities indicate potential complicity in criminal activity.
- Agents whose seasonal business fluctuation is not consistent with their incomes or with other agents in the locale or is consistent with patterns of criminal proceeds.
- Agents whose ratio of questionable or anomalous customers to customers who are not in such groups is out of the norm for comparable locations.

B. CUSTOMER DUE DILIGENCE AND WIRE TRANSFERS

51. CDD processes should be designed to meet the FATF standards and national legal requirements. The CDD process should help MVTS providers assess the ML/TF risk associated with a proposed business relationship or occasional transaction above the threshold. The initial CDD comprises identifying the customer and, where applicable, the customer's beneficial owner and verifying the customer's identity on a risk basis on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework. It also includes understanding the purpose and intended nature of the business relationship (where relevant) and, in higher risk situations, obtaining further information.

52. Non-banking institution providing MVTS typically carry out occasional transactions and generally do not open or maintain accounts. However, MVTS providers sometimes may also introduce customer loyalty schemes and relationship management tools, which coupled with an agreement between the MVTS providers and customers, indicate that a business relationship has been formed. The MVTS providers should have procedures, which are effectively implemented and

used to identify and verify, on a risk basis, the identity of a customer (a) when establishing business relations with that customer; (b) when carrying out occasional transactions above the applicable designated threshold[36]; (c) where they have suspicions of ML/TF regardless of any exemption or thresholds; and (d) where they have doubts about the veracity or adequacy of previously obtained identification data.

53. The legal frameworks of some countries go further than Recommendation 10 requires[37] by requiring full CDD for all transactions performed by MVTS providers, including those which are de facto occasional transactions below the USD/EUR 15 000 threshold. Such an approach may be consistent with the risk-based approach, as set out in Recommendation 1, provided that it is justified on the basis of the country's assessment of risks (e.g. through the identification of higher risks). One factor which should be taken into account is whether this would increase the risk of driving transactions to unregulated sectors.

54. Recommendation 16 establishes the requirements for countries with respect to wire transfers. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers.[38] MVTS providers must include relevant originator and beneficiary information on wire transfers and ensure that the information remains with the wire transfer throughout the payment chain as set out in the Interpretive Note to Recommendation 16. It is important to note, that countries may adopt a *de minimis* threshold for cross-border wire transfers, below which verification of the customer, and beneficiary information need not be required unless there is an ML/TF suspicion.[39] That is, for occasional cross-border wire transfers below USD/EUR 1 000, the requirements of the Interpretive Note to Recommendation 16 apply and the name of the originator and of the beneficiary will be requested, as well as an account number for each or a unique transaction reference number; however such information will not have to be verified unless there are suspicious circumstances related to ML/TF, in which case information pertaining to customer should be verified.

55. The MVTS provider should adopt effective risk-based policies and procedures for determining when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information and the appropriate follow-up action.[40]

56. Based on a holistic view of the information obtained in the context of their application of CDD measures, MVTS providers should be able to prepare a customer risk profile in appropriate cases. This will determine the level and type of ongoing monitoring and support the MVTS providers' decision whether to enter into, continue or terminate the business relationship. Risk profiles can apply at the individual customer level or, where a cluster of customers displays homogenous characteristics (for example, clients conducting similar types of transactions or with the same economic activity), at the cluster level. MVTS providers should periodically update customer risk

36 The FATF Recommendations require that any national threshold is no higher than USD/EUR 15 000 for occasional transactions (other than wire transfers), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked. See INR. 10.

37 Recommendation 10 required CDD measures to be undertaken.

38 INR. 16 at paragraph 3.

39 INR. 16 at paragraph 5.

40 INR. 16 at paragraph 18 and 22.

profiles[41] of business relationships, which serve to help MVTS providers apply the appropriate level of CDD. In addition, MVTS providers should take measures to comply with international sanctions lists issued by the UN and with national AML/CFT lists issued by the competent national authorities (e.g. national lists of designated persons and organisations for TF) by screening the customer's and beneficial owner's as well as beneficiary's names against such lists. Smaller MVTS providers may consider joining industry groups to have access to sanctions screening services, wherever appropriate.

57. The extent of CDD measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk, if any, associated with the individual business relationship as discussed above under Risk Assessment. This means that the amount or type of information obtained, or the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher. It may also be simplified where the risk associated with the business relationship is lower. It should, however be noted that the ability to apply simplified CDD or an exemption from other preventive measures, simply on the basis that MVTS is being carried out by natural or legal persons on an occasional or very limited basis is not to be applied (INR. 1.6(b)). Also SDD measures are not acceptable whenever there is a suspicion of ML or TF, or where specific higher-risk scenarios apply.

Box 3. **Examples of Enhanced Due Diligence/Simplified Due Diligence measures**
(see also INR 10)

- Enhanced Due Diligence
  - obtaining and corroborating additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk profiling
  - carrying out additional searches (e.g. verifiable adverse internet searches) to better inform the individual customer risk profiling
  -
  - where appropriate, undertaking further verification procedures on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may be involved in criminal activity
  - verifying the source of funds or wealth involved in the transaction or business relationship to be satisfied that they do not constitute the proceeds from crime
  - evaluating the information provided with regard to the destination of funds and the reasons for transaction
  - seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship

41 Based on the MVTS provider's own risk assessment and taking into account risk factors such as those outlined in the FATF standards, e.g. in INR 10 and Recommendations/INR 12-16.

- Simplified Due Diligence
  - obtaining fewer elements of customer identification data, seeking less robust verification of the customer's identity
  - not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established
  - verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if transaction values rise above a defined monetary threshold)
  - reducing the frequency of customer identification updates in case of business relationship
  - reducing the degree and extent of on-going monitoring and scrutiny of transactions, based on a reasonable monetary threshold

58. Where MVTS providers cannot apply the appropriate level of CDD, Recommendation 10 requires the MVTS provider to not enter into a business relationship or carry out an occasional transaction or to terminate an already-existing business relationship; and considering making a suspicious transaction report in relation to the customer.

Ongoing CDD and Monitoring

59. Ongoing monitoring on a risk basis means the scrutiny of transactions to determine whether those transactions are consistent with the MVTS provider's information about the customer and the nature and purpose of the business relationship, wherever appropriate. Monitoring also involves identifying changes to the customer profile (for example, their behaviour, use of products and the amount of money involved), and keeping it up to date, which may require the application of enhanced CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may be potentially suspicious.

60. Monitoring should be carried out on a continuous basis and may also be triggered by specific transactions. It need not require electronic systems, although for some types of MVTS activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, MVTS providers should understand their operating rules, verify their integrity on a regular basis and check that they take account of the identified ML/TF risks.

61. MVTS providers should adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for higher risk situations. The adequacy of monitoring systems and the factors leading

MVTS providers to adjust the level of monitoring should be reviewed regularly for continued relevance to the MVTS provider's AML/CFT risk programme. Transactions performed/triggered by agents must be subject to regular monitoring under the same conditions as transactions of MVTS provider itself. The monitoring should be conducted by the MVTS provider itself or in collaboration with the agent, based on appropriate agreement and under the MVTS provider's controls.

62. Monitoring under a risk-based approach allows MVTS providers to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. MVTS providers should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be transparent.

63. To this end, MVTS providers should properly document, retain and communicate to the relevant personnel the results of their monitoring as well as any queries raised and resolved.

Suspicious Transaction Monitoring and Reporting

64. Recommendation 20 requires all financial institutions including MVTS providers that suspect, or have reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, to report their suspicions promptly to the relevant FIU. MVTS providers should have the ability to flag unusual movements of funds or transactions for further analysis. MVTS providers should have appropriate systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether the funds or transaction are suspicious.

65. Funds or transactions that are suspicious should be promptly reported to the FIU and in the manner specified by competent authorities. The processes MVTS providers put in place to escalate suspicions and ultimately report to the FIU should reflect this. While the policies and processes leading MVTS providers to form a suspicion can be applied on a risk-sensitive basis, a MVTS provider should report once ML/TF suspicion has been formed.

66. MVTS providers should comply with applicable STR requirements when established through a network of agents in different host jurisdictions. The territorial approach requires the STR and any other information to be submitted, on behalf of the MVTS provider, to the FIU in the country in which the agent is established.

67. Consistent with paragraph 22 of the INR 16, MVTS providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a funds transfer, the MVTS provider: (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether this gives rise to suspicion; and (b) where necessary should file an STR with the appropriate FIU, and make relevant transaction information available to the FIU.

68. The lack of required originator or beneficiary information should be considered as a factor in assessing whether an electronic funds or wire transfer is suspicious and whether it is thus required to be reported to the FIU.

C. INTERNAL CONTROLS AND COMPLIANCE

Internal Controls and Governance

69. Adequate internal controls are a prerequisite to an effective implementation of policies and processes to mitigate ML/TF risk. Internal controls include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated, controls to monitor the integrity of staff and agents, which are implemented in accordance with the applicable local legislation. MVTS providers should consider national or sectoral risk assessments and controls to validate that their policies and processes are effective tools for identifying, assessing, and monitoring ML/TF risk in the region. It is appropriate that MVTS providers modify their internal controls according to relevant changes in their size, operational complexity, or risk exposure. Accordingly, MVTS providers should maintain systems that are adequate to manage and mitigate their risks. Where the risks are low (see for example Annex 5 for indicators of lower risk), less sophisticated systems will suffice.

70. For MVTS providers which work through agent networks, they should include these networks in their AML/CFT internal control processes and monitor them for compliance with their AML/CFT programs.

71. The successful implementation and effective operation of a RBA to AML/CFT depends on strong senior management leadership, which includes oversight of the development and implementation of the RBA across the MVTS provider.

72. Senior management should consider various ways to support AML/CFT initiatives:

- create a culture of compliance and promote compliance as a core value of the MVTS provider by sending a clear message that the MVTS provider will develop processes to ensure that:
- ML/TF risks can be managed before entering into, or maintaining, business relationships or offering services that are associated with excessive ML/TF risks;
- business relationships are not established when the ML/TF risks cannot be mitigated and managed.
- Senior management, together with the company board of directors, are responsible for setting up robust risk management governance and controls mechanisms that:
- reflect the company's established risk policy;
- implement adequate internal communication processes appropriate for the actual or potential ML/TF risks faced by the MVTS provider. These mechanisms should link (where applicable) the board of directors, the AML/CFT chief officer, any relevant or specialised committee within the MVTS provider (e.g. the risks or the ethics/compliance committee), the IT division and where applicable, each of the business areas;

- helps decide on the measures needed to mitigate the ML/TF risks identified and on the extent of residual risk the MVTS provider is prepared to accept; and
- adequately resource the MVTS provider's AML/CFT function.

73. This implies that senior management should not only know about the ML/TF risks to which the MVTS provider is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. This would require that senior management:

- understands the regulatory and supervisory requirements where the MVTS provider operates;
- receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the MVTS provider is exposed through its activities and individual business relationships;
- receives sufficient and objective information to understand whether the MVTS provider's AML/CFT controls are effective;
- receives updates on government communications or enforcement actions related to the AML/CFT obligations of MVTS providers and ML/TF risks;
- ensures that processes are in place to escalate important decisions that directly impact the ability of the MVTS provider to address and control risks.

74. Responsibility for the consistency and effectiveness of AML/CFT controls should be clearly allocated to an individual of sufficient seniority within the MVTS provider to signal the importance of ML/TF risk management and compliance, and that ML/TF issues are brought to senior management's attention. This includes the appointment of a skilled compliance officer at management level.[42] The compliance officer should have the necessary independence, authority, seniority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including across lines of business, and foreign branches, subsidiaries and agents). Where an MVTS provider is situated via one or more agents in various host countries, an individual with functions of compliance officer may be appointed in each host country to ensure compliance with the local AML/CFT requirements (CDD, record keeping, STR and any other reporting obligation to the host FIU among others).

75. Recommendation 18 requires countries to require financial institutions to have an independent audit function to test the AML/CFT programme with a view to establishing the effectiveness of its AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. Senior management will need to have a means of independently validating the development and operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based methodology reflects the risk profile of

42 INR 18.

the MVTS provider. This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, specialist consultants or other qualified parties who are not involved in the implementation or operation of the MVTS provider's AML/CFT compliance programme. The testing should be risk-based, taking into account the risk profile of the MVTS provider; should evaluate the adequacy of the MVTS provider's overall AML/CFT policies and programme, the quality of risk management for the MVTS provider's operations, departments and subsidiaries; should include comprehensive procedures and testing; and should cover all activities.

76. Both the compliance and audit functions should base their assessment on all information relevant to their task including, where relevant and appropriate, information obtained confidentially through relevant internal mechanisms or whistleblowing hotlines. Other sources of information can include training pass rates, compliance process or control failures or analysis of questions received from staff.

Internal Mechanisms to Ensure Compliance

77. A MVTS provider's internal control environment should be conducive to assuring the integrity, competence and compliance of staff with relevant policies and procedures. The measures relevant to AML/CFT controls should be consistent with the broader set of controls in place to address business, financial and operating risks generally.

78. The nature and extent of AML/CFT controls will depend upon a number of factors, including the nature, scale and complexity of a MVTS provider's business, the diversity of its operations, including geographical diversity, its customer base, product and activity profile, the degree of risk associated with each area of its operations and distribution channels, i.e. the extent to which the MVTS provider is dealing directly with the customer or is dealing through intermediaries, agents, third parties, or in a non-face-to-face setting without appropriate mitigating measures.

79. The framework of AML/CFT compliance function and internal controls should:

- Place priority on the MVTS provider's operations (products, services, customers and geographic locations) that are more vulnerable to abuse.
- Provide for regular review of the risk assessment and risk management processes, taking into account the environment within which the MVTS provider operates and the activity in its market place.
- Provide for an AML/CFT compliance function and review programme.
- Ensure that adequate risk assessment and controls are in place before new products are offered.
- Inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed.
- Provide for programme continuity despite changes in management or employee composition or structure.

- Focus on meeting all appropriate regulatory record keeping and reporting requirements and for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- Provide for adequate controls for higher risk customers, transactions and products, agents, as necessary, such as transaction limits or management approvals.
- Enable the timely identification and filing of reportable transactions.
- Provide for adequate management and oversight of its agents, including initial agent due diligence, AML/CFT training, and ongoing risk-based monitoring.
- Provide for adequate supervision of employees who handle transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the business's AML/CFT programme.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- Provide for appropriate initial and refresher training to be given to all relevant staff.
- Provide for appropriate initial and refresher training for agents at appropriate intervals.

Vetting and recruitment

80. MVTS providers should recruit through background checks and satisfy themselves that the staff they employ have integrity, are adequately skilled and possess the knowledge and expertise necessary to carry out their function, in particular where staff are responsible for implementing AML/CFT controls, whether in compliance or in front-line function.

81. The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

Training and Awareness

82. The effective application of AML/CFT policies and procedures depends on staff within MVTS providers understanding not only the processes they are required to follow but also the risks these processes are designed to mitigate, as well as the possible consequences of those risks. It is therefore important that staff receive AML/CFT training, which should be:

- Relevant to the MVTS provider's ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls;
- Obligatory for all relevant staff;

- Tailored to particular lines of business within the MVTS provider, equipping staff with a sound understanding of specialised ML/TF risks they are likely to face and their obligations in relation to those risks;
- Effective: training should have the desired effect, and this can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the MVTS provider's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected;
- Ongoing: in line with INR 18, AML/CFT training should be regular, relevant, and not be a one-off exercise when staff are hired;
- Complemented by AML/CFT information and updates that are disseminated to relevant staff as appropriate.

83. Overall, the training should also seek to build up a working culture where compliance is embedded in the activities and decisions of the entire MVTS provider's staff.

D. AGENTS OF MVTS PROVIDERS

Agent Due Diligence

84. Agent Due Diligence is intended to enable a MVTS provider to ensure that it knows the legal and ownership structure of its agents and that it will be forming business relationships with legitimate and viable agents that will reliably implement or adhere to (depending on local regulations) AML/CFT requirements, program responsibilities, policies, and procedures. The MVTS provider's procedures must take into considerations such factors as:

- Upon application, identify the agent and perform the necessary background checks and due diligence, such as a recent change from current relationship with other product/service providers, whether the agent is representing more than one MVTS provider or is licensed/registered by the relevant national supervisory authority to provide payment services, length of time in business, ownership structure, creditworthiness, financial viability, class of trade or industry, licensing and regulatory structure and other regulatory licensing or registration to which the agent may be subject.
- Obtain appropriate additional information to understand the applicant's business, such as offering other MVTS services, the agent's past record of legal and regulatory compliance, expected nature and level of transactions and customer base, and geographical exposure.
- Upon approval, conduct new agent AML/CFT training encompassing applicable AML/CFT requirements, AML compliance program responsibilities, and MVTS internal policies and procedures. Provide AML/CFT compliance materials, tools, and training to agents on an ongoing and regular basis.

- Provide guidelines and assistance to the agent to assess its own compliance program regime and to develop its own risk assessment based upon its unique risk profile for its products and services, customers, geography, and subagents or outlets (if applicable).
- Ensure compliance regime adherence to internal policies and external regulation, such as reporting suspicious or attempted suspicious activities, large transactions, monitoring the risk behaviours described above, reporting and record keeping, through periodic AML compliance program reviews.
- Provide prompt attention and remediation of risk behaviours by onsite or offsite contact with the agent, which may result in further training, or probation, suspension or termination of the agent.

Training and Awareness of Agents

85. As a preventive measure, MVTS providers should check the agent's integrity before and during the business relationship, in order to avoid the abuse of their services. Agents must have appropriate training with regard to AML/CFT either provided by the MVTS providers or by themselves. Putting in place and maintaining effective controls relies on both training and awareness. This requires an enterprise-wide effort to provide all relevant employees and agents with appropriate information on AML/CFT laws, regulations and internal policies.

86. Applying a risk-based approach to the various methods available for training gives each MVTS provider additional flexibility regarding the frequency, delivery mechanisms and focus of such training. Agent training should be documented and training records should be maintained according to applicable record keeping requirements. A MVTS provider should review its agent base and available resources and implement training programmes that provide appropriate AML/CFT information that is at the appropriate level of detail.

87. Agent training may include onsite or offsite initial training (*i.e.* upon activation), and ongoing training via web-based programmes, periodic mailings or newsletters, websites or pop-up messages at point of origination. In conjunction with or in addition to such training, the MVTS provider may provide periodic compliance program reviews involving a comprehensive assessment of the agent's compliance with internal and external AML regulatory requirements.

Monitoring of Agents

88. Agent monitoring is a very important element for an effective MVTS provider's AML/CFT program. All agents require monitoring to assess and address systemic risks such as inadequate training, new or changing services or products, and poor individual judgment or performance. The degree and nature of agent monitoring will depend on the transaction volume of the agent, the monitoring method being utilised (manual, automated or some combination), countries where the funds are sent, outcomes of previous monitoring mechanisms (where relevant), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, the degree of monitoring will be based on the perceived risks, both external and internal, associated with the agent, such as

the products or services being provided by the agent, the location of the agent and the nature of the activity. Prompt attention and remediation of risk behaviours should be addressed by appropriate means, such as enhanced examination of the agent's transaction history and data integrity, obtaining and evaluating the agent's explanation of these behaviours, confidential sampling of the questioned aspects of the agent's services, or onsite or offsite contact with the agent, which may result in further training, or probation, suspension or termination.

89. Agent monitoring under a risk-based approach allows a MVTS provider to create monetary or other thresholds or specific red flags to determine which agent activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. MVTS providers should also assess the adequacy and integrity of any systems and processes on a periodic basis.

90. Competent authorities and MVTS providers (as well their industry associations) may consider collaborating to address and mitigate the specific risks emanating from certain agent behaviour. Some of the measures that can be implemented in this regard may include:

- an industry-held register of high-risk agents (or the so-called "bad agents"), through which MVTS providers can share alerts with each other about potential bad actors.
- requiring application of enhanced CDD measures in appropriate cases.
- applying thresholds on cash transactions.
- providing specific training sessions on STR indicators to MVTS providers in order to enhance their understanding and improve reporting standards, with the expectation that the MVTS provider would then train its agents or alternatively training to both the MVTS providers and their agents.

SECTION III – GUIDANCE FOR SUPERVISORS

A. THE RISK-BASED APPROACH TO SUPERVISION AND/OR MONITORING

91. The RBA to AML/CFT aims to develop prevention or mitigation measures which are commensurate with the ML/TF risks identified. In the case of supervision, this applies to the way supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that is conducive to the application of RBA by MVTS providers.

92. Recommendation 26 requires countries to subject MVTS providers to effective systems for AML/CFT supervision and/or monitoring. INR 26 requires supervisors to allocate greater supervisory resources to areas of higher ML/TF risk, on the basis that supervisors understand the ML/TF risk in their country and have on-site and off-site access to all information relevant to determining a MVTS provider's risk profile.

Box 4. **Recommendation 26: Regulation and Supervision of Financial Institutions**

[.....]

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

[.....]

Understanding ML/TF Risks

93. An effective risk-based regime reflects a country's policy, legal and regulatory approach. The national policy, legal and regulatory framework should also reflect the broader context of financial sector policy objectives that the country is pursuing. These would include financial inclusion, financial stability, financial integrity and financial consumer protection and include considerations such as competition. The extent to which the national framework allows MVTS to apply a risk-based approach should also reflect the nature, diversity and maturity of the MVTS sector, and its risk profile as well the ML/TF risks associated with individual MVTS providers.

94. Supervisors should also develop a deep understanding of the MVTS market, its structure and role in the financial system and the country's economy to better inform risk assessment of the sector. Supervisors should draw on a variety of sources to identify and assess ML/TF risks. This will include but not limited to jurisdiction's national or sectoral risk assessments, domestic or international typologies and supervisory expertise, as well as FIU feedback. Where competent authorities do not adequately understand the MVTS environment operating in the country, it may be appropriate for competent authorities to consider undertaking a more targeted sectoral risk assessment in relation to the MVTS sector to develop a national level understanding of the relevant ML/TF risks and to also inform the institutional assessments to be undertaken by the MVTS providers.[43]

95. Access to information about ML/TF risks is fundamental for an effective RBA. INR 1.3 requires countries to take appropriate steps to identify and assess ML/TF risks for the country, on an ongoing basis in order to make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs. In situations where some parts of the MVTS sector have potentially limited capacity to identify ML/TF risks, countries should particularly work with the sector to understand their risks. Depending on their capacity, general information or more granular information and support may be required.

[43] FATF (2013a), paragraphs 17-19.

96. For individual MVTS providers, supervisors should take into account the level of risk associated with the MVTS providers' products and services, business model, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location, countries of operation and the level of compliance with the AML/CFT measures. Supervisors should also look at the controls in place, including the quality of the risk management policy, the functioning of the internal oversight functions etc. Other information, which may be relevant in the AML/CFT context, includes the fitness and propriety of the management and the compliance function.

97. Some of this information can be obtained through prudential supervision in countries where MVTS providers are subject to prudential regulation. This involves appropriate information-sharing and collaboration between prudential and AML/CFT supervisors, especially when the responsibilities belong to two separate agencies. In other regulatory models, such as those focusing on licensing/registration at the national level, but with shared oversight and enforcement at the state level and/or with SRBs, information sharing should include the sharing of examination findings.

98. Where relevant, information from other stakeholders such as other supervisors (including overseas supervisors, and supervisors of payment systems and instruments), the FIU and law enforcement agencies may also be helpful in determining the extent to which a MVTS provider is able to effectively manage the ML/TF risk to which it is exposed. Some regimes, such as those only requiring registration (without extensive background testing) may still enable law enforcement and regulators to be aware of the existence of the institution, its lines of business, or controlling interests.

99. Supervisors should review their assessment of both the sector's and MVTS providers' ML/TF risk profiles periodically and in any case when MVTS providers' circumstances change materially or relevant new threats emerge.

100. Examples of different ways MVTS supervisors assess ML/TF risk in the MVTS sector and in individual MVTS providers can be found in *Annex 2.*

Mitigating ML/TF risk

101. The *FATF Recommendations* require supervisors to allocate and prioritize more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risk to which the sector and individual MVTS providers are exposed. Supervisors should give priority to the areas of higher risk, either in the individual MVTS provider or to MVTS providers operating in a particular sector. If a jurisdiction chooses to classify an entire sector as higher risk, it should be possible to get some granularity for the appropriate categorisation of individual MVTS providers within the sector based on their customer base, countries they deal with and applicable AML/CFT controls etc.

102. It is also important that competent authorities acknowledge that in a risk-based regime, not all MVTS providers will adopt identical AML/CFT controls and that single, unwitting and isolated incidents involving the transfer or exchange of illicit proceeds do not necessarily invalidate the

integrity of a MVTS provider's AML/CFT controls. On the other hand, MVTS providers should understand that a flexible RBA does not exempt them from applying effective AML/CFT controls.

103. Examples of ways in which supervisors can adjust their approach include:

a) Adjusting the type of AML/CFT supervision or monitoring: supervisors should always have both off-site and on-site access to all relevant risk and compliance information. However, to the extent permitted by their regime, supervisors can determine the correct mix of off-site and on-site supervision or monitoring of MVTS providers. Off-site supervision alone may not be appropriate in higher risk situations. However, where supervisory findings in previous examination (either off-site or on-site) suggest a low risk for ML/TF, resources can be allocated to focus on higher risk MVTS providers. In that case lower risk MVTS providers could be supervised off-site, for example through transaction analysis and questionnaires.

b) Adjusting the frequency and nature of ongoing AML/CFT supervision or monitoring: supervisors should adjust the frequency of AML/CFT examination in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge, e.g. as a result of whistleblowing, information from law enforcement, analysis of financial reporting or other supervisory findings. Other risk-based approaches to supervision could consider geographic location, customer base, cash intensity, number of accounts, the nature and number of agents, revenue, prior history of non-compliance, significant changes in management, and/or acquisitions.

c) Adjusting the intensity of AML/CFT supervision or monitoring: supervisors should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of MVTS providers' policies and procedures that are designed to prevent them from being abused. Examples of more intensive supervision could include: detailed testing of systems and files to verify the implementation and adequacy of the MVTS providers' risk assessment, reporting and record keeping policies and processes, internal auditing, interviews with operational staff, senior management and the Board of directors and AML/CFT risk assessment in particular lines of business.

104. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and AML/CFT rules and guidance remains adequate. Whenever appropriate, and in compliance with relevant confidentiality requirements, these findings should be communicated to MVTS providers to enable them to enhance the quality of their RBA.

105. Under *FATF Recommendation* 27 and 35, supervisors should have the power to impose adequate sanctions on MVTS providers when they fail to comply with regulatory requirements. Supervisors should use proportionate actions, which may include a range of supervisory interventions, including corrective actions to ensure proper and timely correction of identified deficiencies as well as punitive sanctions for more egregious non-compliance, taking into account that identified weaknesses can have wider consequences. Generally, systemic breakdowns or significantly inadequate controls will result in a more severe supervisory response.

B. SUPERVISION OF THE RISK-BASED APPROACH

Licensing or Registration

106. *FATF Recommendations* 14 and 26 require countries to ensure that MVTS providers are licensed or registered by a competent authority, including the requirement to ensure that agents of MVTS providers are licensed or registered, or that the MVTS provider maintains a current list of its agents accessible by competent authorities in the countries in which the provider and its agents operate. These requirements should take into account the benefits of bringing MVTS providers into the regulatory framework.

General approach

107. Supervisors should understand the ML/TF risks faced by the sector and by a MVTS provider. They should have a comprehensive understanding of higher, standard as well as lower risk lines of business, with a particularly thorough understanding of the higher risk lines, leading to a sound judgment about the proportionality and adequacy of AML/CFT controls. As part of their exam procedures, supervisors should communicate findings and their views about the individual MVTS provider's AML/CFT controls. It is important to understand why institutions may decline to adopt proportionate controls. Where this is due to a lack of understanding of the flexibility available, supervisors should be able to provide appropriate guidance. Equally supervisors should understand the reasons why an institution engages in instances which go beyond the law (also called conservative or over-compliance) and provide further guidance, where considered appropriate.

108. It is important that supervisors discharge their functions in a way that takes into consideration the adoption of a RBA by MVTS providers. This means that supervisors should ensure that their staff are equipped to assess whether a MVTS provider's policies, procedures and controls are appropriate and proportional in view of the MVTS provider's risk assessment and risk management procedures. Supervisors should satisfy themselves that the MVTS provider adheres to its own policies, procedures and controls, and makes sound decisions. It is also important that supervisors should articulate and communicate clearly their expectations of the measures needed for MVTS providers to comply with the applicable legal and regulatory framework.

109. To support supervisors' understanding of the overall strength of measures in the MVTS sector, comparative analysis between MVTS providers' AML/CFT programs could be considered as a means to inform their judgment of the quality of an individual MVTS provider's controls. Supervisors should, however, note that under the RBA, there may be valid reasons why MVTS providers' controls differ.

110. In the context of the RBA, the primary focus for supervisors should be to assess whether the MVTS provider, in its own risk assessment, has reasonably and fairly gauged the risk to the business. In doing so, the supervisors should take into account the individual business circumstances; in addition to the overall sector risk. Supervisors should also determine whether or not the MVTS provider's AML/CFT compliance and risk management program is adequate to a) meet the regulatory requirements, and b) appropriately and effectively mitigate and manage the risks. The effective application of the RBA means that risk is assessed by institution and customer, not to an entire category of financial institutions or customer groups. In the case an MVTS provider

operates across different jurisdictions on the basis of a single licence or registration, the home supervisor (that licences or registers the entity) should take into consideration the risk the entity is exposed to and the extent to which those risks are adequately mitigated.

Guidance

111. Supervisors should communicate their expectations of MVTS providers' compliance with their legal and regulatory obligations, and may consider engaging in a consultative process, where appropriate with relevant stakeholders. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based obligations, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied.

112. Guidance for the MVTS sector is essential and is a requirement under *FATF Recommendation* 34. Some MVTS providers may have limited experience in, or ability to, identify relevant ML/TF risk factors. In particular, for MVTS providers with lower capacity, the guidance provided would need to be more detailed than that provided for other MVTS, and could include extensive information on conducting a risk assessment and implementing a RBA. The guidance could include tools that enable small MVTS providers with lower capacity to undertake assessments and develop risk mitigation and compliance management systems to meet their legal obligations. Supporting ongoing and effective communication between supervisors and MVTS providers is an essential prerequisite for the successful implementation of a RBA.

113. Supervisors should also consider liaising with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of the legal obligations and to promote a level playing field, including overseers of payment systems and instruments. This is particularly important where more than one supervisor is responsible for supervision (for example, where the prudential supervisor and the AML/CFT supervisors are in different agencies, or in separate divisions of the same agency or when the MVTS provider has agents in several jurisdictions). Multiple sources of guidance should not create opportunities for regulatory arbitrage, loopholes or unnecessary confusion among MVTS providers. When possible, relevant regulatory and supervisory authorities within a jurisdiction should consider preparing joint guidance.

Training

114. Training is important for supervision staff to understand the MVTS sector and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of a MVTS provider's ML/TF risk assessments and to consider the adequacy, proportionality, effectiveness, and efficiency of the MVTS provider's AML/CFT policies, procedures and internal controls in light of its risk assessment.

115. Training should allow supervisory staff to form sound judgments about the quality of the MVTS provider's risk assessment and the adequacy and proportionality of a MVTS provider's AML/CFT controls. It should also aim at achieving consistency in the supervisory approach at a national level, in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

Information exchange

116. Information exchange between the public and private sector is of importance in the MVTS sector and may form an integral part of a country's strategy for combating ML/TF. In situations where MVTS providers do not have experience, or have limited capacity for an effective assessment of ML/TF risk, it will be important for public authorities to share risk information to better help inform the risk assessments of MVTS providers.

117. The type of information that could be shared between the public and private sectors include:

- ML/TF risk assessments;
- Typologies of how money launderers or terrorist financers have misused MVTS;
- General feedback on STRs and other relevant reports;
- Targeted unclassified intelligence. In specific circumstances, and subject to appropriate safeguards such as confidentiality agreements, it may also be appropriate for authorities to share targeted confidential information with MVTS providers as a class or individually; and
- Countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by *FATF Recommendation* 6.

118. Domestic cooperation and information exchange between the supervisors of the banking sector and the MVTS sector, central bank and MVTS supervisors for monitoring and feedback of the remittance flows, among law enforcement, intelligence, FIU and MVTS supervisors and between the FIU and supervisor of the MVTS sector is also of vital importance for effective monitoring/supervision of the sector.

119. Cross border information sharing of authorities and private sector with their international counterparts is of importance in the MVTS sector, taking into account the multi-jurisdictional reach of many MVTS providers.

Supervision or monitoring of agent networks

120. Some MVTS providers operate through a network of agents, sometimes in different jurisdictions. The use of agents can create vulnerabilities where an agent may not itself be a financial service professional. In all cases, MVTS providers that use agents should be required to include them in their AML/CFT programs and MVTS providers should monitor them for compliance with applicable AML/CFT legislation and regulation.[44]

121. Recommendation 14 requires that agents of MVTS providers should either be licensed/ registered, as is the case for their provider, or countries could also choose another option, which is requiring the MVTS provider to maintain a current list of agents that is accessible by competent authorities. Countries should carefully consider the risks involved in each approach, the practical

[44] R.14

feasibility, and the resources required before making a final decision on whether to license/ register, or require the MVTS provider to maintain a current list of agents. In all cases, countries should ensure that under their legal framework, the MVTS provider remains responsible for its AML/CFT obligations and is accountable for the actions of its agents consistent with established principles of agency law. Supervisors that license MVTS providers to operate outside of their own jurisdiction should consider the risks such activities represent to those host jurisdictions, and should ensure that the obliged entity mitigates risks adequately.

122. Countries should determine on a risk-sensitive basis whether the supervision of agents is undertaken indirectly through the MVTS providers or through direct contact with the agents, to ensure that supervision or monitoring is proportionate and commensurate with the level of ML/TF risk. In line with the risk-based approach, countries may consider imposing AML/CFT regulation on MVTS agents, as well as the MVTS providers. Under this approach, the agents would themselves be subject to AML/CFT obligations and be directly supervised for compliance with these obligations by the relevant supervisory authority. This approach may be beneficial in situations where the MVTS provider is located in another country which creates difficulties in effectively supervising that entity. Countries could consider supervisory mechanisms such as central contact points or home/host supervisory cooperation between relevant AML supervisors of the sector, in order to ensure effective supervision and monitoring of compliance with the applicable AML/CFT obligations and to facilitate information exchange.

123. In establishing the supervisory framework, countries should clearly establish the competent authority that is responsible for the AML/CFT supervision or monitoring of MVTS providers. When a MVTS provider is a multinational entity or operates through a network of agents in different jurisdictions, the cooperation between supervisors in these jurisdictions becomes even more important. It is necessary to clarify the responsibilities of the supervisors, to ensure mechanisms and arrangements (such as protocol on cooperation in AML/CFT supervision) for effective cooperation, exchange of information about agents and the MVTS provider and to clarify the regulatory position.

SECTION IV – ACCESS OF MVTS TO BANKING SERVICES[45]

This section should be read in conjunction with the *2014 FATF RBA Guidance for the banking sector.*

A. AML/CFT REQUIREMENTS AND BANKING MVTS PROVIDERS

Regulatory Expectations

124. As a financial institution subject to FATF requirements, a MVTS provider is subject to the full range of AML/CFT controls with which it has to comply vis-à-vis its customers, such as: CDD, wire transfer rules and ongoing monitoring mechanisms apart from record keeping, suspicious transactions reporting etc. (Section II). The review of the AML/CFT measures and programme put in

45 All reference to access of MVTS providers to banking service in this section and elsewhere in the paper includes access to non-banking financial institutions, which may hold payment accounts of MVTS providers as customers.

place by the MVTS provider will often be part of the overall MVTS customer risk assessment conducted by the bank before on-boarding the MVTS provider as a customer.

125. As stated earlier, MVTS agents should either be licensed or registered with a competent authority or be part of a list maintained by the MVTS provider and accessible by competent authorities in the country where they operate. As a starting point, the MVTS provider should provide evidence or confirmation that it has conducted the relevant agent due diligence, that its AML/CFT program includes its agents and that compliance is monitored. When they are themselves MVTS providers, agents are required to establish AML/CFT programs and comply with due diligence, record keeping and other AML/CFT requirements.

B. BANKS' RISK-BASED APPROACH TO MVTS PROVIDERS

MVTS Risk Assessment

126. It should also be noted that in many cases, MVTS providers are reliant on access to the banking system in order to commence or continue their operations. It is important that banks apply the RBA properly and do not resort to the wholesale termination or exclusion of customer relationships within the MVTS sector without being informed by a proper risk assessment.

127. Where banks propose to enter into a business relationship with a MVTS provider, they should evaluate the ML/TF risk of the business relationship and assess whether those risks can be appropriately mitigated and managed. This should include control measures to mitigate the risks of the MVTS provider as a customer currently assessed as low, medium or high risk, and a process for escalation to deal with MVTS providers or particular aspects of their business, which become higher risk in the course of the business relationship.

128. When assessing the risks associated with MVTS providers, different risk factors (types of products and services offered, types of customers, distribution channels, and jurisdictions they are exposed to, experience of the provider, purpose of the account, anticipated account activity etc.) should be weighed; as MVTS providers will not present the same levels of ML/TF risk. While some will pose a higher risk, there are others that will not. An effective risk assessment should be a composite of multiple factors, and important elements in the case of MVTS will include the scope of markets served (domestic or international), the purpose of the bank account and the anticipated account activity, the regulatory oversight effectiveness in the countries of operation, and the effectiveness of the MVTS's risk management and compliance programs.

129. Depending upon the circumstances, certain factors may be weighed more heavily than others. For example, one of the elements which could act as a risk mitigant is the fact that MVTS providers are regulated financial institutions that are subject to the full range of AML/CFT obligations, supervision and monitoring. Factors which could potentially increase the ML/TF risks are the geographic coverage (especially countries with weaknesses in their AML/CFT framework), bulk transfers (where the transfer represents a collection of underlying transactions), third party payments, inadequate supervisory framework in its home jurisdiction, or the fact that the provider is a new business without an established operating history. Factors that may decrease the risk are geographic coverage (for example, where a money remitter offers services only domestically or to countries which are largely compliant with the FATF standards or present a relatively low ML/TF

risk); that the business operator has an established operating history etc. Other factors that may be relevant include whether transactions are small remittances for family members, or where there are high levels of transparency of payment information (e.g. purpose of sending funds is clearly explained, MVTS provider has visibility into both sender and recipient, all parties are adequately identified including beneficial ownership and it involves a direct transaction without any further intermediation).

130. The bank may consider, on a risk-sensitive basis whether the MVTS provider acts as a principal or is an agent of another provider. In this case, the way in which the principal monitors and controls compliance by its agents needs to be considered as an element of risk. Thus agents' due diligence procedures and adequacy and effectiveness of their supervision/monitoring by MVTS providers may be considered by banks and factored in when assessing the overall ML/TF risks being posed by such MVTS providers to banks as their customers. Where the MVTS provider itself is not a bank's customer but the MVTS agent is a customer, bank may also consider obtaining information/reference from the MVTS provider; in order to assist in its understanding of the MVTS agent's business and source of funds.

Risk-based AML/CFT Obligations for Banking MVTS Providers

MVTS Provider Due Diligence

131. Based on AML/CFT requirements applicable to banks, proper due diligence associated with opening and maintaining accounts for MVTS providers is required, in relation to the customer, the beneficial owner(s), and the business relationship (i.e. determine the structure and ownership of the MVTS provider, the nature of its business and operations including the target market, the purpose of the relationship and the expected account activity). In all cases, the level and extent of due diligence applied will be dictated by the risks associated with the particular MVTS customer provider.

132. Depending on the level and nature of risk identified, and the size and sophistication of the particular MVTS provider, banks may pursue different types of action as part of an appropriate due diligence process. When identified risks are higher, enhanced due diligence should be applied, which can include reviewing the AML/CFT (group-wide) programmes, their internal or external audit and other expert's reports, review of the list of agents and their monitoring, management and screening practices. A visit to the place of business and/or informative statements sent to third parties to verify the alignment with operating history, where appropriate, may prove helpful to check the existence and activities of the provider. Bank may also rely and/or verify from publicly available information (such as licensed or registered person lists with competent authorities) in such cases. If a bank becomes aware of changes in the profile of a MVTS provider to which services are being provided, additional steps or enhanced due diligence may be necessary.

Ongoing Monitoring of MVTS Accounts

133. Risk-based monitoring of accounts maintained for all customers, including MVTS providers, is a key element of an effective system to identify and, where appropriate, report violations and suspicious transactions. The level and frequency of such monitoring will depend, among other things, on the bank's risk assessment and the activity across the MVTS provider's accounts (including reconciling the activities of the MVTS providers together with the MVTS agents in order

to ascertain the full risk exposure where both the MVTS provider and its agents are bank's customers). Risk-based review of transactions should be conducted to detect any significant unexplained variations in transaction size, nature or frequency through the account which could reveal potentially suspicious operations.

MVTS Suspicious Transaction Reporting

134. While the policies and processes leading banks to form a suspicion can be applied on a risk-sensitive basis, a bank should report once a suspicion of ML/TF has formed. Banks should have the ability to flag unusual movements of funds or transactions conducted by MVTS providers for further analysis. They should also have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether they are suspicious. Similarly, if a bank is aware that an MVTS provider is breaching the applicable licensing or registration requirements, it should not accept the MVTS provider as a customer and should file a STR, if appropriate, in such cases.

C. GUIDANCE FOR THE SUPERVISION OF BANKS WITH MVTS PROVIDERS AS CUSTOMERS

General approach

135. Banks' considerations before providing services to MVTS providers are varied, including ML/TF risks, the compliance costs to effectively mitigate those risks, profitability, reputational risk and requirements imposed by international correspondent banks. There may also be some circumstances in which a bank may choose not to provide financial services to some or any MVTS providers for reasons including limited product lines that do not include MVTS related service, adequacy of supervision over MVTS, cross-border information-sharing barriers, the risks associated with specific jurisdictions which it deems unmanageable.

136. While the decision to accept or maintain a business relationship is ultimately a commercial one for the bank, supervisors need to ensure that they understand the drivers of and reasons for those commercial decisions and they communicate the importance of banks following the risk-based approach to managing the risks of individual accountholders. It is possible that financial institutions go beyond the requirements of relevant laws and regulations (also called conservative or over-compliance) for example, by deciding not to implement simplified due diligence measures, where allowed, in relation to lower risk products or by refusing or closing accounts due to lack of understanding of the law, lack of compliance expertise or on account of business factors that are not compliance related.[46] Where decision to restrict or terminate relationship with MVTS is due to a lack of understanding of the flexibility of the risk-based approach, supervisors will be able to provide appropriate guidance as to what the RBA entails.

137. Banks should identify, assess, manage and mitigate the risks posed by their customers, sectors in which those customers operate and the products and services offered. Banks themselves are best placed to assess and manage the risks posed by their customers and the products and services offered. Effective supervision can assist banks to understand the implementation of the RBA, thereby avoiding wholesale termination of customer relationships. Systematic termination of

46 De Koker, Louis and Symington, John (2014).

business relationships and refusal to on-board MVTS clients without proper risk assessment and mitigation measures, could, drive remittance flows to unregistered and unregulated channels. This may exacerbate the AML/CFT risk rather than address it. In any case, the wholesale cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risks or risk mitigation measures for individual customers within a particular sector, cannot be considered as being in line with FATF standards. In addition to increasing ML/TF risks, such action may give rise to reputational and legal risks for banks, amongst others relating to unfair discrimination, competition and consumer protection.

Guidance

138. All supervisors should sufficiently and consistently clarify their MVTS related supervisory expectations over the RBA as part of their day-to day supervision and when wholesale de-risking occurs as a result of misinterpreting the RBA. Supervisors may take the opportunity to clarify that the intention of a RBA is not to eliminate risk by refusing services to any particular sector, but to manage risk effectively. Supervisors should provide meaningful and actionable guidance on the effective implementation of the RBA to both the banking sector and supervisory staff. With appropriate systems and controls in place, banks should be able to manage and mitigate the potential ML/TF risks posed by some MVTS providers. Other relevant FATF guidance on the supervision of banks can be found in the FATF RBA Guidance for the banking sector and the FATF Guidance on the Risk-Based Approach for Effective Supervision and Enforcement.

139. Supervisors could emphasise the varying degrees of risks in the MVTS sector and encourage banks to take into account risk mitigating factors, such as AML/CFT procedures and controls, which are put in place by MVTS providers to manage their ML/TF risks. Often, supervisors of banking and non-banking MVTS providers are different (e.g. central bank/financial regulator *vis-à-vis* FIU, non-banking supervisors/different departments within the bank/supervisors etc.). Supervisory compliance expectations and tolerance for risk in these cases are also often inconsistent. Thus, stress should be given to coordination among different supervisors so that all MVTS providers and banks could have similar expectations and similar approaches to RBA.

140. Supervisors could clarify the expectations on banks concerning the assessment of CDD policies and procedures implemented by a MVTS provider. Supervisors could inform bank decisions by providing examples of CDD practices that they deem adequate for small, lower risk MVTS providers.

141. Supervisors could encourage banks to engage with the MVTS sector on the measures that the sector could take immediately and in the longer term to meet the banks' risk standards which would enable a continuation or start of the business relationship. Such encouragement will be more meaningful when accompanied by supervisory statements on risk tolerance.

ANNEX 1. UNAUTHORISED MVTS PROVIDERS

Recommendation 14 requires countries to take action to identify natural or legal persons that carry out MVTS without a licence or registration, and to apply appropriate sanctions. Countries should take a systematic and pro-active approach by identifying and taking action against unauthorised providers on a regular basis. For many jurisdictions, proactive identification of informal MVT services and awareness-raising is an integral element of establishing and maintaining an effective registration / licensing regime.

Countries should ensure that a competent authority has the responsibility for the identification and sanctioning of unauthorised MVT providers. Depending on the institutional framework in a country, the authority may be, for example, the supervisor, the FIU, the law enforcement agencies or another agency with regulatory authority over the financial sector. Countries should consider which competent authority is best placed to be responsible for this issue, which will differ between countries depending on the circumstances and institutional structure. When determining the responsible authority, counties should consider a range of factors including the powers and capacity of competent authorities, the level of interaction with MVTS providers, and the information available to competent authorities to support this function.

There is a range of information sources which may indicate MVT activity and could be useful to identify unauthorised MVTS providers, for example:

- Applications for licencing or registration, including those that were unsuccessful or historical applications which were not renewed or where licenses or registrations have been withdrawn;
- Marketing by MVTS providers, including advertisements in the various media outlets;
- Suspicious transaction reports;
- Data by MVTS organisations, reporting those entities which do not form part of their organisation or association;
- Information provided by whistle blowers;
- Policing and intelligence reports; and
- Reports of international funds transfers or cross-border movements of funds (if applicable in a country)

Whichever authority is responsible, coordination between various authorities is important as they may hold information relating to unauthorised providers. Countries should be aware of the information that is available in their jurisdiction and ensure information is shared as appropriate to support the identification and sanctioning of unauthorised MVTS providers.

There can be a number of ways for awareness raising campaigns in respect of unauthorised MVTS. This should be done on a risk basis, i.e. not all countries should conduct awareness raising campaigns with the same intensity. Some of these examples include:

- Ensuring that the competent authorities responsible for overseeing and/or registering or licensing unauthorised MVTS providers know how to detect those services that have not registered or been licensed and are adequately resourced to do so.
- Making unauthorised MVTS providers aware of their obligations to license or register, as well as any other obligations with which they may have to comply. Using education and compliance programs, including visits to advise businesses which may be operating unauthorised MVTS of licensing or registration and reporting obligations, as opportunities to seek information about others in their industry. Using these outreach efforts by law enforcement and regulatory agencies to enhance their understanding about the operations, record keeping functions and customer bases of unauthorised MVTS operations. Extending outreach campaigns to businesses typically servicing unauthorised MVTS providers (such as shipping services, courier services and trading companies). Placing in trade journals, newspapers, web-pages or other publications of general distribution notices of the need for unauthorised MVTS providers to register or license and comply with other relevant requirements.
- Ensuring that law enforcement is aware of the compliance requirements for MVTS providers in addition to the methods by which those services are used for illicit purposes. Ensuring that the full range of training, awareness opportunities and other forms of education are provided to investigators with information about MVTS operations, their obligations under the regulatory regime and ways in which their services can be used for ML/TF. This information can be provided through training courses, presentations at seminars and conferences, articles in policing journals and other publications.
- Publishing guidelines to encourage licensing or registration and compliance with other relevant requirements. Additionally, issuing material to ensure financial institutions currently subject to STR requirements (e.g. banking sector) develop an understanding of MVTS. Informing potential customers about the risks of utilising illegal MVTS and their role in ML/TF.
- Requiring entities to display their registration/license to customers once they are registered/licensed. Legitimate clients will likely have a higher degree of confidence in using registered/licensed operators and may therefore seek out those operators displaying such documentation.
- Making a comprehensive and up-to-date list of all licensed or registered persons that provide MVTS publicly available.

The FATF has identified a number of effective practices in the area of identification strategies for unauthorised MVTS, which include[47]:

- Increasing and strengthening communication between supervisory authorities including self-regulatory bodies, MVTS organisations and the general public, in order to identify those institutions which have lost their licenses or registrations, specifically due to not complying with AML/CFT provisions.
- Examining the full range of media to detect advertising conducted by unauthorised MVTS providers and informing operators of their registration/licensing obligations. This includes national, local and community newspapers, radio and the internet; giving particular attention to the printed media in various communities; and monitoring activities in neighbourhoods or areas where unauthorised MVTS providers may be operating.
- Passing on, to the competent authorities, information about unauthorised MVTS providers uncovered during investigations effective practices include encouraging investigators to pay particular attention to ledgers of business that may be associated with unauthorised MVTS; encouraging enforcement agencies to look for patterns of activity that might indicate involvement of unauthorised MVTS; and, where possible, encouraging enforcement agencies to consider using undercover techniques or other specific investigative techniques to detect MVTS that may be operating illegally.
- Consulting with of registered / licensed MVTS providers and banks for potential leads on MVTS providers that are unregistered or unlicensed.
- Being aware that unauthorised MVTS are often utilised where there is bulk currency moved internationally, particularly when couriers are involved. Paying particular attention to the origin and owners of any such currency. Coordinating with border control agencies to identify instances of cross-border currency movement via couriers. Couriers could provide insights for the identification and potential prosecution of illegal operators with whom the couriers are associated, especially when potential violations by couriers are linked back to the source of the unauthorised MVTS operation.
- Paying particular attention to domestic suspicious transaction or unusual activity reporting, as well as to domestic and international large value cash reporting, where applicable, to identify possible links to unauthorised MVTS operations.
- Assisting banks and other financial institutions in developing an understanding of what activities/indicators are suggestive of unauthorised MVTS operations and using this to identify them. Many unauthorised MVTS

47 See FATF (2003).

providers maintain bank accounts and conduct transactions in the formal financial sector as part of other business operations. Giving banks the authority to crosscheck particular accounts against a register of these operators and notify the relevant regulatory authority as appropriate. These registers can also be made available online for easy access and search and may be updated at frequent intervals.

- Once unauthorised MVTS operations are identified, international exchange of information and intelligence on these entities between the relevant agencies can be facilitated. Consideration could be given to sharing domestic registers with international counterparts. This strategy would also assist jurisdictions to identify local operators not previously known.

Where unauthorised MVTS providers are identified, it is important to consider the reasons why they conducted their business without authorisation. If this is due to a lack of information, improved communication of the need for authorisation may be required. If operators do not register because they are concerned about their ability to meet compliance requirements, it is important to understand the concerns and to consider whether these can be addressed, for example by providing appropriate guidance.

EXAMPLES OF ACTION TAKEN BY AUTHORITIES AGAINST UNAUTHORISED MVTS PROVIDERS.

Mexico

According to Mexican Law (Article 101 of General Law of Auxiliary Credit Organizations and Activities), the provision of those services of the Mexican entity analogous to the MVTS (the "*transmisor de dinero*" or "money remitter") by someone who has not been registered for those purposes by the National Banking And Securities Commission, is a crime punished with prison from 3 to 15 years, and a fine of up to 100 000 days of wage (article 101 of the General Law of Auxiliary Credit Organizations and Activities).

The National Banking and Securities Commission (CNBV) has broad faculties to investigate and sanction natural and/or legal persons who are carrying out financial activities without authorisation. Thus, the CNBV imposes the suspension of activities to those offenders, among others effective, proportionate and dissuasive sanctions.

Moreover, in order to ensure that users and financial institutions are able to know which entities are authorised as MVTS, the CNBV website publishes a list of the registered MSBs and MVTS. Likewise, money remitters should indicate in any kind of advertisement their registration number and its issuance date. Additionally, the CNBV website has a mechanism in which people can report any MVTS without registration.

Netherlands

In the Netherlands, De Nederlandsche Bank N.V. (DNB) is authorised to supervise MVTS. Transferring money to and from foreign countries without prior authorisation by DNB is considered to be a violation of the Financial Supervision Act.

DNB is authorised to impose fines (max. EUR 4 million) and to issue a cease and desist order to stop the illegal activities. These activities also constitute a criminal offence, which is liable to proceedings by the Public Prosecutor.

In the autumn of 2014, DNB conducted several examinations into people and offices suspected of transferring money to and from foreign countries without prior authorisation by DNB. The goal of this project was to make a stand against illegal practices and to show the authorised payment institutions that illegal activities are not acceptable. These examinations involved an on-site inspection supported by the police. The on-site inspections revealed that several violations of the Dutch Financial Supervision Act had been committed. DNB has therefore imposed fines in several cases. DNB has also issued a press release on this subject in which the general public as well as the authorised MVTS providers were incited to report illegal MVTS activities to DNB. In addition, DNB used social media to get across its message[48].

Singapore:

Singapore has the following mechanism to deal with the issue:

- Physical surveillance: police look out for illegal remittance operators when patrolling areas where they are more likely to be active, such as places where migrant workers congregate.
- Public database of licensed operators: A public database of the names and addresses of licensed remittance businesses allows the public to cross-check remittance businesses and alert authorities to unlicensed activities.
- Outreach to likely users of unlicensed services: Target groups, such as migrant workers, are educated on the risks of using unlicensed remittance operators and directed towards the licensed operators. Siting licenced remittance services in convenient locations, such as foreign worker dormitories/ recreation centres.

48 Eenheid Rotterdam (5 January 2015), “Underground Banking”, www.youtube.com/watch?v=ThgVR6jM6kI

ANNEX 2. EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH TO THE MVTS SECTOR

Argentina

Law 25246, as amended, in its Section 20, subsection 2, establishes as legally bound reporting parties "the institutions governed by Law 18924, as amended, and natural or artificial persons authorized by the Central Bank of the Argentine Republic to operate in the purchase and sale of foreign currency in the form of cash money or cheques drawn in foreign currency, or by means of credit or debit cards or in the transfer of funds within the national territory and abroad".

FIU Resolution 66/2012 regulates the measures and procedures that shall be observed by fund remitters, in order to prevent, detect and report facts, acts, transactions or omissions that may constitute crimes of Money Laundering and Terrorist Financing.

Section 3 of this Resolution establishes the prevention policy for the purposes of correctly complying with the obligations arising from Law 25246. Among other aspects, said policy shall include the development of records of analysis and risk management about Money Laundering and Financing of Terrorism of detected unusual transactions and those that have been considered suspicious and thus have been reported.

As legally bound reporting parties, fund remitters shall adopt risk analysis policies. Section 18, subsection l) of this Resolution indicates that: Said risk analysis policies shall be gradual; enhanced measures shall be performed over higher risk customers and updates and analysis of information on the customer's economic, assets, financial and tax situation and corporate and control structure shall be conducted more frequently.

A regards to supervision, during 2014, the overall supervisory system has been strengthened to ensure correct implementation of AML/CFT prevention measures on part of the legally bound reporting parties, among which fund remitters are included. Verification procedure, both on-site and off-site, is performed based on a risk approach, according to FIU Resolution 229/2014. With respect to sanctions, in 2014, administrative summaries were applied to two fund remitters for non-compliance of the current AML/CFT obligations.

In addition, twice a year, the FIU coordinates intensified cross-border control of currency and negotiable instruments with the participation of country members of GAFILAT

Canada

Example of Guidance on the RBA:

FINTRAC provides guidance to reporting entities on operationalizing a risk-based approach to combatting money laundering and terrorist financing. This guidance is designed to help reporting entities to:

1) Consider business-wide elements or factors that may impact ML/TF risk and apply controls and measures to mitigate the risks, addressing:

- Products, services and delivery channels;
- The business' geography; and
- Other factors relevant to the business' specific activities (e.g. legal, environmental, etc.)

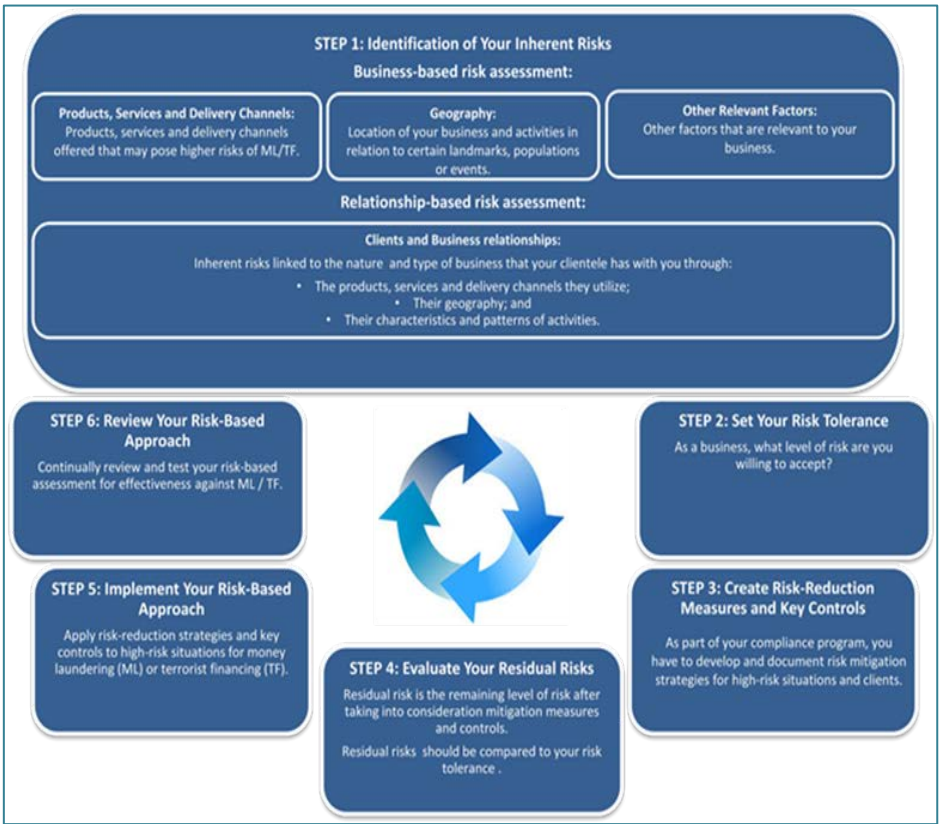
2) Evaluate the risks associated with the clients and business relationships by looking at:
   - The products, services and delivery channels they utilize;
   - The geography related to the clients (their location, links to high-risk countries, where they conduct their business and transactions, etc.); and
   - Their activities, transaction patterns, characteristics, etc.

   This specific assessment will allow reporting entities to identify high-risk business relationships and apply the prescribed special measures.

3) Identify and validate controls to mitigate high-risk activities and business relationships, including prescribed special measures; and

4) Review and assess the status of the business' compliance regime with Canada's laws as well as the adequacy of your current controls to mitigate the identified high risks.

This guidance accomplishes these four tasks through the following six step approach:



This document was prepared generally for all of Canada's FIs and DNFBPs and can be found at www.fintrac-canafe.gc.ca/publications/rba/rba-eng.asp. FINTRAC is aware that all sectors require more specific information to operationalize a meaningful risk-based assessment to combat ML/TF. To accommodate this need, FINTRAC is preparing sector specific workbooks to aid reporting entities in operationalizing their risk-based approach.

Italy

Money Transfer Proceeding ("Money River" Operation) - December 2014

As a result of systematic criminal behaviour committed by the suspects, eighteen (18) money transfer operators based in Rome were addressed by custody order on 17 December 2014 (10 out of 18 in prison and 8 under house arrest). Money transfer plays a significant role within Rome's economy and is almost exclusively consisting of foreign countries operators. The investigated operators illegally transferred abroad approx. EUR 1 billion, as a result of several predicate offences: import and sale of counterfeit goods, market fraud, sales of industrial products with false or misleading trademarks and tax evasion.

In particular, a huge sum of money was transferred abroad through a large number of illicit transfers of cash amounts (approx. EUR 785 000) below the threshold set by law, and illegally, since the operations were fictitious, performed without customer identification and with no indications of the nature of the underlying relationships. None of the requirements set by the Italian AML legislation was fulfilled.

Transfer operations were always made below the threshold – i.e. whereby the threshold for cash transactions was set at EUR 5 000 (up to 12 August 2011), operations then amounted to EUR 4 999 each; whereby the threshold was EUR 2 500 (up to 5 December 2011), operations then amounted to EUR2 499; and, most recently, with the threshold set at EUR 1 000, transactions amounted to EUR 999.

"*The money was transferred without any tax trace in Italy*" (as reported by the Judge in the mentioned custody order).

The convicted individuals were accused of: transnational criminal association and money-laundering arising from the related predicate offences (ascribed to the economic operators who made use of the activity carried out by money-launderers). In compliance with the law regulating legal persons' liability, the offences related to the crimes committed by their managers were also notified.

The case involved multiple criminal associations operating through the Rome-based Italian branch of the *XYZ* payment institution (i.e. a multinational company specialised in worldwide money transfers based in a foreign country), as well as 7 Rome-based money transfer agencies operating in the circuit headed by the mentioned Payment Institution.

The association members include the branch leaders and the representative in charge of AML checks, as well as a number of operators that violated laws on money transfer in order to carry out the above transactions.

Preliminary investigations lasted for about two years and were performed by the *Nucleo di Polizia Valutaria* of the *Guardia di Finanza* (*GdF*) through a wide array of investigative tools: wiretaps, video surveillance services, searches, seizures, watching and shadowing services, AML inspections and documentation analysis.

The investigations were inspired by the AML inspection into a Rome-based money transfer agency carried out by GdF upon own initiative. The inspection revealed abnormal operations involving a considerable amount of money transfer operations almost exclusively requested by non EU-citizens and addressed to their respective countries of origin.

Investigations (subsequently extended to another 6 Rome-based agencies of the Italian branch of the Payment Institution and numerous foreign traders) enabled shedding light on a widespread criminal network which – by making use of the services provided by the money transfer circuit headed by the Payment Institution, and taking advantage of systematic violation of AML legislation – managed to transfer huge cash flows by laundering the proceeds of tax evasion and unlawful activities related to trade of counterfeit products.

The cash was delivered to money transfer agencies or by their representatives who used to pick it up directly at the premises of the persons ordering the transfer operations.
The names used to perform the operations were invented, or belonged to deceased persons, or even to unsuspecting customers already registered in the Payment Institution management database and made accessible to the agencies operating within the circuit.

The fictitious character of the operations resulted from multiple sources:

- Documentation obtained;
- Wiretaps;
- Uneconomic character of operations compared to larger bank transfers (expressly chosen as they guaranteed anonymity, tax evasion, money-laundering and large profits to the money transfer operators, thus favouring combined economic and criminal interests for those committing predicate offences and money-launderers);
- Video surveillance agencies (few customers entering but huge volumes of transactions recorded);

Following inspections carried out by GdF at the premises of money transfer agencies, operators decided to resort to pick-up of the funds to be transferred directly from the premises of the subjects ordering the operations.

The subjects requesting money transfer operations were foreign entrepreneurs and traders operating in Italy (especially in Rome), with criminal records for committing crimes of various kinds (smuggling, counterfeiting, tax evasion).

The illegal transfer was managed and directed by persons who held important positions within the Payment Institution and enacted systems aimed at "circumventing" proper tracking of the origin of the sums. Among those addressed by restrictive measures: the temporary regional director, the AML supervisor, the sales department manager, and the head of unsettled debts office of the Italian branch. GdF executed the seizure of assets worth over EUR 13 million, equivalent to the profits

made by the Payment Institution and money transfer agencies through the illicit transactions performed.

Mexico

Ministry of Finance:

The Mexican Ministry of Finance modified the administrative rules so that the professional organisations of MVTS are able to draft the AML/CFT internal compliance manuals. This reduces costs due to scale economies, while taking into consideration the differences of specific sectors of MVTS and, ultimately, fostering AML/CFT compliance.

National Banking and Securities Commission (CNBV):

Several questionnaires have been conducted to Money Transmitters to deepen operability mechanisms, which is used to determine the risk degree of Money Transmitter. The questionnaire enables to know the geographical areas of increased operation, the number of related agents, the number of specific operations, parameters or amounts, among other data. This allows updating information on supervisory requirements based on major elements of risk and not just random or geographical information.

The Money Transmitters must inform the CNBV the name of related agents having a contractual relationship, as well as other parties that operate with their related agents; with this information corridors can be known.

Whenever an inspection is conducted, information of the entities is requested to the FIU regarding the behaviour that have generated them concern based on information analysis of relevant, unusual and internal reports and such reports sent to that authority.

The CNBV counts with a risk matrix that qualifies the risk to which every Money Transmitter is exposed; this matrix integrates information from geographic areas of major transactions, the number of branches and related agents to each society, the average number of employees, specific transactions, parameters or amounts, as well as the mitigating measures implemented by these. Based on such matrix, and concerns of the FIU, CNBV implements the Annual Inspection Visits Program with tasks that will be reviewed during the inspection visits.

Every time a Money Transmitter is cancelled because it did not complied correctly with its AML/CFT obligations, the CNBV monitors if it still sends any kind of operational report and, if it does, an specific area visits the cancelled entity and if it is still operating starts the corresponding administrative or criminal procedure to sanction the illegal entity.

Netherlands

In the Netherlands, De Nederlandsche Bank N.V. (DNB) is responsible for the supervision of MVTS. In addition to supervising MVTS authorised in the Netherlands, DNB also supervises Dutch-based agents of foreign MVTS, by virtue of the Anti-Money Laundering and Anti-Terrorist Financing Act *(Wet ter voorkoming van witwassen en het financieren van terrorisme – Wwft)*.

Each quarter, DNB analyses all money transfers made in the Netherlands and performs a network analysis on these transfers. Based on this network analysis, DNB is able to detect potentially unusual transaction patterns and take direct action by arranging on-site inspections. This working method allows DNB to perform her supervisory tasks effectively and efficiently. At present, DNB leverages this technique to supervise around a thousand locations in the Netherlands. Over the past year, DNB has imposed several formal measures as a result of this supervisory practice and made one report to the Public Prosecutor's Office with respect to a suspected case of money laundering.

Singapore

To balance the need to focus on the higher risk MVTS operators, while not being blind-sided by the broader population, supervisors could augment their resources by engaging external auditors/consultants to assist in performing periodic reviews of lower-risk entities. The MVTS sector may be more suited for such an approach where its operations and business model are generally less complex than banks.

Spain

At the end of 2009, SEPBLAC, in its FIU capacity, detected a fresh money laundering operation, carried out by criminals who, taking up the position of agents of payment institutions, were splitting amounts of cash into numerous remittances, which were attributed to fictitious identities and transferred to China. These funds were associated with payments for smuggled goods, tax fraud and other criminal activities.

SEPBLAC received suspicious activity reports with respect to this pattern of operation not only from payment institutions, but also from banking institutions in which certain agents had opened accounts, from which they were sending funds to be transferred to the MVTS. SEPBLAC examined the STRs and concluded that the suspicious activity reported did not refer to end-customer transactions, but rather that it was the agents themselves who were connected with ML/FT activities, and not the alleged customers, who were in reality inexistent.

Following a scrutiny of such reports, the relevant financial intelligence reports were sent by SEPBLAC to law enforcement agencies and Customs authorities. In October 2012, Spanish media revealed the results of this investigation, known as "*Operacion Emperador*". This large ML network is currently being prosecuted in Spain. A total of 110 people are being prosecuted in Spain, Germany and Italy and EUR 11.6 million in cash and EUR 11 million in bank accounts have been seized. The case involved laundering the proceeds of numerous predicate offences, including smuggling (undeclared or undervalued goods imported) and fiscal crimes.

At the same time, this problem was reported to SEPBLAC's Supervision Area which decided to undertake measures of a general nature applicable to the entire sector, as well as specific measures in relation to certain institutions.

1) General measures:

- Requirement for the payment institutions to send monthly statistical information broken-down by country and agent. This requirement expanded the statistical information which the Bank of Spain had been

collecting and which was accessible by SEPBLAC and it enabled SEPBLAC Supervision Area to conduct a strategic analysis on the money remittance sector. The findings of this strategic analysis were used to implement additional risk-based supervisory measures, selecting the targets according to the level of risk detected in the analysis and to adapt SEPBLAC's operational analysis to be more useful for competent authorities.

- Training and awareness-raising of institutions with respect to the need to control the activity of their agents, in order to comply with the obligation expressly contained in AML/CFT legislation. This objective was achieved by means of circulars sent to the representatives of the payment institutions and the organisation of specific meetings with the sector, where the problems posed by the laundering of money through agents and the ways to detect it and curtail it were explained.

2) Specific measures:

- SEPBLAC's Supervision Area decided to undertake extensive on-site inspections of certain money remitters in order to verify the nature of the phenomenon, its extent and how it was being managed by the various institutions. The outcome of these inspections caused, in the first place, the opening of several sanctioning case files against a number of institutions and, as a consequence thereof, there was a very significant increase in STRs filed by money remitters in relation to their agents. The result of these new STRs was incorporated by the police authorities into investigations already in progress, which made it possible to finally compile the information for initiating criminal proceedings.

Moreover, from the point of view of the activity of these companies, the outcome of this entire process has led to:

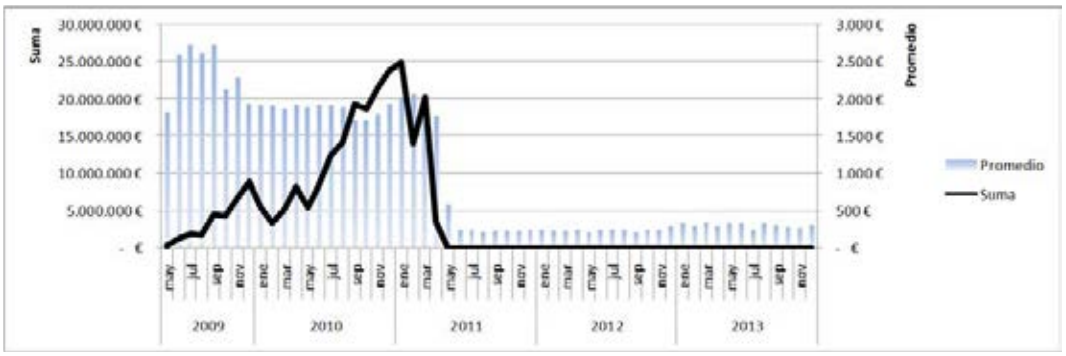
1) A "purging" process of the MVT sector, with the disappearance of several institutions and a general improvement in the controls existing among those remaining. A particularly significant development among the latter measures was the creation by the association of MVTs of a database of agents whose activity has been the subject of an STR. Money remitters are thus able to know immediately whether the person or company they are intending to contract as an agent, or which they have already engaged, has been the subject of an STR by another money remitter.

2) A reduction in the flows of illegal money channelled through money remitters, due to the improvements introduced into their AML/CFT systems and to the measures put into place by the sector overall. In 2013, SEPBLAC measured the impact of the decisions and measures taken as a result of its strategic analysis, and established that the total amount of high risk transactions in the money remittance sector has considerably decreased as revealed by graphs below:

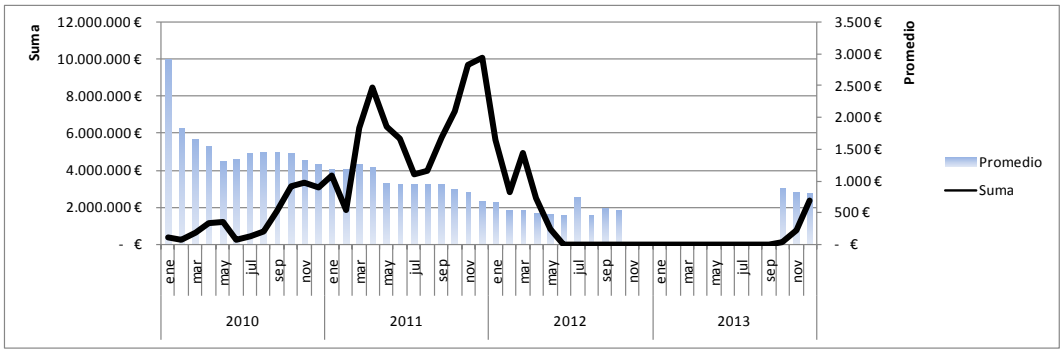
China

Remittances to China

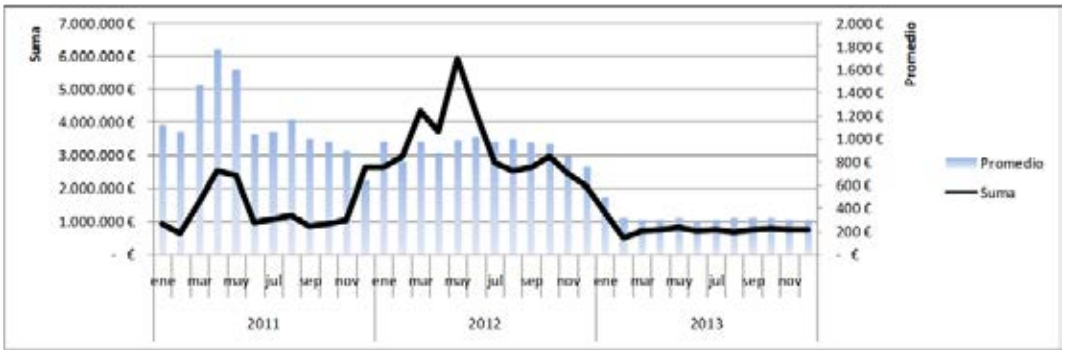
Institution A (2009 – 2013)



Institution B. (2010 – 2013)



Institution C. (2011 – 2013)



United States

Supervisory Guidance on Risk Management Associated with MVTS

- The office of the comptroller of the currency (OCC), a US banking supervisor, issued a "statement on risk management associated with money services businesses" to provide clarification to national banks, federal savings associations, and federal branches and agencies of foreign banks (collectively, banks) on the agency's supervisory expectations with

regard to offering banking services to money services businesses (MSB). Available at www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-58.html

- Joint guidance – FIU and supervisor. In 2005, the US FIU (FinCEN), together with all the US. Banking supervisors collectively called the "federal banking agencies", jointly issued a statement to address expectations regarding banking institutions' obligations under the Bank Secrecy Act for money services businesses, such as check cashers and money transmitters. Available at www.fincen.gov/news_room/nr/html/20050330.html

ANNEX 3. EXAMPLES OF COUNTRIES' SUPERVISORY PRACTICES FOR THE IMPLEMENTATION OF THE RISK-BASED APPROACH TO THE BANKING SECTOR WITH MVTS PROVIDERS AS CUSTOMERS

Mexico

National Banking and Securities Commission (CNBV)

The CNBV published on its website a compliance chart with the levels of legal compliance on AML/CFT matters, including Money Transmitters, among others. The chart aims to increase financial transparency and build trust between the supervised entities and users of financial services.

The CNBV has practiced visits to the main FIs that send their customers' resources through concentration accounts, as well as to such banks that have opened concentration accounts of brokerage firms, it has been recommended since 2009, to this sector, to implement the following measures:

Privilege:

a) The use of a referenced number for those accounts being used in concentration and dispersion of resources.

b) The use of electronic transfers to concentrate resources on these kinds of accounts, since it allows the identification of the resource's origin.

Implement:

a) Special monitoring to identify the source of the received funds by means of transfers.

b) Random special monitoring in order to identify the origin of the resources received through documents (checks).

c) Prohibition of receiving cash deposits through concentration accounts.

d) Information exchange with FIs where concentration accounts are opened.

As a result of the financial reform published in the Official Journal of the Federation (DOF -for its acronym in Spanish-) on January 10th 2014, the CNBV will certify professionals, compliance officers and independent external auditors who provide services to entities and persons subject to supervision by the CNBV on AML/CFT matters. This certification will provide the FIs and supervised subjects with confidence and will foster stability of the Mexican financial system. On October 2nd 2014, was published in the DOF the general provisions for certification of independent, external auditors, compliance officers and other professionals in the prevention of transactions with illegal proceeds and terrorist financing; and on March 13th 2015, was published through the same means the Agreement by which it is disclosed the Calendar to start the certification process of independent external auditors, compliance officers and other professionals in the prevention of operations with resources illegal proceeds and terrorist financing.

According to this calendar the certification program will start with the banking sector, followed by brokerage firms and regulated multiple purpose financial companies (Sofoms) before the end of 2015.

ANNEX 4. EXAMPLES OF PRIVATE SECTOR PRACTICES IN APPLICATION OF RBA

Canada

Example of private sector effective practices for Agent Risk

a.) When onboarding agents, conduct beneficial ownership assessment, criminal background check, media scan for negative press, check of compliance credentials.

b) In dealing with agents on an ongoing basis, conduct an ongoing risk assessment of their business and provide training, outreach, and transaction monitoring in accordance with their risk. Conduct mystery shopping and compliance testing internally.

c) Having a clear and defined process for resolving customer complaints and de-registering agents.

d) Sharing information on de-marketed agents and customers with other industry participants.

Example of private sector effective practices for Customer Risk

e) When on-boarding clients, checking beneficial ownership, criminal background, and media scan of clientele.

Example of private sector effective practices for Internal Controls

f) Dedicated compliance staff that are not compensated in accordance with transactions, business relationships or on-boarding agents.

Japan

One MVTS provider has been voluntarily setting maximum fund transfer amount from JPY 100 000 to JPY 500 000 yen per one day according to the beneficiary countries' risk situations, and also the fund transfer has been limited to two transactions in maximum per one day (fund transfer from different business locations is not permitted).These measures have been taken due to the increasing illegal fund transfer case using money mule in Japan.

The Netherlands

In the Netherlands, the Dutch Association of Money Transfer Companies has developed a code of conduct. This code of conduct applies to all members of the Dutch Association of Money Transfer Offices (NVGTK) and is intended to set minimum requirements for risk management and compliance with regard to money laundering and other criminal activities. This code of conduct strives to implement these requirements based on the following themes: compliance, customer agreement, risk criteria, customer due diligence, monitoring, reporting unusual transactions, payment service agent due diligence, training and knowledge level, retaining evidence, and complaints procedure. (www.nvgtk.nl/actueel/gedragscode--code-of-conduct)

Spain

As a consequence of the awareness-raising process developed with this sector regarding the risks of agents, the main association of MVTS providers has created a database of "bad agents".

This is an industry-held register of high risk agents (or the so-called "bad agents"), through which MVTS providers can share alerts with each other about those agents whose transactions(not singular transactions, but the whole business managed by that agent) have been reported to the FIU and business relationships terminated. Usually, these decisions are based on the suspicious that these agents are splitting amounts of cash into numerous remittances, which are attributed to fictitious identities and transferred to third countries.

Making use of that database, every time a MVTS provider is going to initiate business relationships with a new agent, they can check whether his/her transactions have been reported to the FIU as suspicious or not.

ANNEX 5. EXAMPLE OF COMPLIANCE PRACTICES OF AND IN RELATION TO A LOW RISK MVTS

This Annex is intended to support supervisors and banks to identify lower risk MVTS providers. This Annex can assist in bridging the gap between the current guidance and supervisory and compliance practices in relation to lower risk MVTS providers.

Characteristics that may factor into lower risk MVTS may be as follows:

- Registered/Licensed with annual audits and regulatory exams.
- Publicly-traded or well capitalized.
- Stable track history with substantial infrastructure.
- Established AML/CFT program.
- Ability to quickly and accurately provide customer specific information (i.e. transaction logs).
- Direct interaction with consumers (as opposed to nested wholesalers or large commercial transactions).
- Low dollar, domestic consumer-based transactions (non-cross border).
- Low dollar, cross-border consumer remittances.
- Licensed agents monitored by licensed parent.
- Established and transparent network of counterparties (foreign).
- A small number of known, regular customers with a pattern of repeat micro-transactions often linked to a pay or salary cycle and with senders and recipients normally linked by family ties.

REFERENCES AND BIBLIOGRAPHY

Chatain *et al* (2011), *Protecting Mobile Money Against Financial Crimes*, World Bank, Washington, D.C., http://dx.doi.org/10.1596/978-0-8213-8669-9

De Koker, Louis and Symington, John (2014), "Conservative corporate compliance: Reflections on a study of compliance responses by South African banks" in *Law in Context*, Volume 30, 2014: 228-256

FATF (2015a), *Guidance for a risk-based approach: effective supervision and enforcement by AML/CFT supervisors of the financial sector and law enforcement*, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-effective-supervision-and-enforcement.html

FATF (2015b), *Guidance for a risk-based approach to virtual currencies*, FATF, Paris, www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

FATF (2015c), *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html

FATF (2015d), *Emerging Terrorist Financing Risks*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

FATF (2014), *Guidance for a risk-based approach for the banking sector*, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html

FATF (2013a), *National money laundering and terrorist financing risk assessment*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

FATF (2013b), *The role of Hawala and other similar service providers in money laundering and terrorist financing*, FATF, Paris, www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html

FATF (2013c), *Politically exposed persons (Recommendations 12 and 22)*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/peps-r12-r22.html

FATF (2013d), *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, FATF, Paris, www.fatf-gafi.org/publications/financialinclusion/documents/revisedguidanceonamlcftandfinancialinclusion.html

FATF (2013e), *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html

FATF (2013f), *Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems,* FATF, Paris, www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (the "FATF Recommendations"), FATF, Paris, www.fatf-gafi.org/recommendations

FATF and MONEYVAL (2010), *Money laundering through money remittance and currency exchange providers*, FATF, Paris and MONEYVAL, Strasbourg, www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingthroughmoneyremittanceandcurrencyexchangeproviders.html

FATF (2003), *Combating the abuse of alternative remittance systems*, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/internationalbestpracticescombatingtheabuseofalternativeremittancesystemssrvi.html

FATF

GUIDANCE FOR A RISK-BASED APPROACH
MONEY OR VALUE TRANSFER SERVICES

Money or Value Transfer Services (MVTS) providers play an important role in the international financial system, in particular for the migrant communities around the world.

This guidance will assist countries and their competent authorities, as well as the practitioners in the MTVS sector and in the banking sector that have or are considering MVTS providers as customers, to apply the risk-based approach to the development of measures to combat money laundering and terrorist financing for the MVTS sector.

The risk-based approach, the cornerstone of the FATF Standards, requires that measures to combat money laundering and terrorist financing are commensurate with the risks.

www.fatf-gafi.org | February 2016