FATF

Asia/Pacific Group on Money Laundering

THE WORLD BANK

FATF GUIDANCE

Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion

February 2013

FINANCIAL ACTION TASK FORCE

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

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

www.fatf-gafi.org

Contents

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
APG	Asia-Pacific Group on Money Laundering
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FSRB	FATF-Style Regional Body
GPFI	Global Partnership for Financial Inclusion
IN	Interpretive Note
INR. X	Interpretive Note to Recommendation X
KYC	Know Your Customer
PEP	Politically Exposed Person
RBA	Risk-Based Approach
SIP	Strategic Implementation Planning
STR	Suspicious Transaction Report
LCC	Low Capacity Country

EXECUTIVE SUMMARY

The promotion of formal financial systems and services is central to any effective and comprehensive AML/CFT regime. However, applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the formal financial system. The FATF has therefore defined a Guidance to provide support in designing AML/CFT measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime. The main aims of the document are to develop a common understanding of the FATF Standards[1] that are relevant when promoting financial inclusion and explicit the flexibility that the Standards offer, in particular the risk-based approach (RBA), enabling jurisdictions to craft effective and appropriate controls.

The Guidance paper was initially published in 2011 and was revised following the adoption of the new set of FATF Recommendations in 2012. It is non-binding and does not override the purview of national authorities. It highlights the need to better inform the assessors and the assessed countries of the financial inclusion dimension of the AML/CFT national frameworks.

The Guidance focuses on facilitating access to formal services for financially excluded and underserved groups, including low income, rural sectors and undocumented groups. It extensively explores the initiatives taken in developing countries as it is where the challenge is the greatest. The analysis is based on a number of countries' experiences and initiatives to address financial inclusion within the AML/CFT context.

The Guidance is based on the important assumption that financially excluded and underserved groups, including low income, rural sector and undocumented groups, in both developing and developed countries should not be *automatically* classified as presenting lower risk for ML/TF.

The Guidance gives an overview of the RBA which is a central element of the 2012 Standards. The greater recognition of a risk-sensitive approach to implement AML/CFT measures – including in particular an approach that takes into consideration the risks of financial exclusion and the benefits of bringing people into the formal financial system – will be a key step for countries that wish to build a more inclusive financial system. The application of the RBA will be based on an assessment of risks which will help countries and financial institutions understand, identify and assess risks and apply mitigation and management measures that are risk-sensitive. This may include low risks, which could benefit from an exemption and lower risks, which could be applied simplified AML/CFT measures.

The Guidance reviews the different steps of the AML/CFT process (Customer Due Diligence (CDD), record-keeping requirements, report of suspicious transactions, use of agents, internal controls), and

[1] The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

for each of them presents how the Standards can be read and interpreted to support financial inclusion. In this context:

- For CDD a distinction needs to be made between the pure identification and the verification steps. An RBA can be introduced to carry out the CDD requirements. Examples of lower risk scenarios and of simplified CDD measures are outlined.
- Countries usually define the "reliable, independent source documents" which can be used to verify customers' identity, and financial institutions can also define a risk based approach with verification processes proportionate to ML/TF risk.
- FATF allows for simplified – though neither an absence nor an exemption from - CDD measures where there is a lower risk of ML/TF. Simplified CDD standards can be decided at country level, based on risk or at financial institution level, the principle remaining that each financial institution must know who customers are, what they do, and whether or not they are likely to be engaged in criminal activity or be conduits for proceeds of crime.
- In an RBA it would be acceptable to infer the purpose and intended nature of the business relationship from the type of transaction or business relationship established.
- Ongoing due diligence and business relationship monitoring must be performed through manual or electronic scanning. An RBA is allowed, with the degree of monitoring based on the risks associated with a customer, an account, and products or services used. Regulatory authorities are to be mindful and give due weight to determinations (monetary or other thresholds, to be reviewed regularly) made by financial institutions.
- Monitoring to detect unusual, potential suspicious transactions is required, with any actual suspicion leading to the removal of any threshold or exception. Simplified CDD could be mitigated by closer transaction monitoring, acknowledging however that an absence of sufficient information due to too little CDD could limit the utility of monitoring.
- It is required that financial institutions keep at least the information on identification documents for a minimum of five years. Options available are scanning of documents, or keeping electronic copies, or merely recording reference details.
- An RBA is usually not applicable to suspicious activity reporting. But an RBA could be appropriate for the purpose of identifying suspicious activities. Transactions with vulnerable groups are usually not subject to separate or specific monitoring, but some financial institutions have developed specific indicators to identify suspicious activities.
- Agents may be permitted, in effect or practice, to perform identification and verification obligations, the prevalent rule being that financial institutions hold the business relationship and are accountable for it, and ultimately liable with respect to agents' compliance with AML/CFT requirements. It is recommended to balance regulatory concerns about agents with the financial inclusion objective. Finally, transaction monitoring systems must cover what is performed by agents.

The FATF will continue to work to ensure that financial inclusion and AML/CFT objectives mutually reinforce each other.

INTRODUCTION – BACKGROUND AND CONTEXT

Preliminary remarks

1. The initiative for this Guidance paper was launched under the FATF Presidency of Mexico in 2010, following the interest kindled by the Presidency of the Netherlands. In June 2010, the FATF placed the issue of financial inclusion on its agenda and committed itself to examining potential challenges posed by anti-money laundering and combating the financing of terrorism (AML/CFT) requirements to the goal of achieving financial inclusion[2]. FATF's interest in financial inclusion is driven by its objective of protecting the integrity of the global financial system, which requires covering the largest range of transactions that pose money laundering and terrorist financing risks in the jurisdictions that have committed to the FATF Recommendations. At the occasion of the renewal of the FATF mandate in 2012, FATF Ministers stated that financial exclusion represents a real risk to achieving effective implementation of the FATF Recommendations[3].

2. In addition to the objective of promoting access to formal financial services thus reducing the use of financial mechanisms that are outside of the authorities' scrutiny, FATF has a strong interest in articulating guidance that supports financial inclusion. Many of the countries that are part of the FATF network, especially jurisdictions that can be considered emerging markets, developing countries, or Low Capacity Countries (LCC)[4] have to deal with the challenges of aligning financial inclusion and financial integrity objectives. For developed market and mature economies, ensuring that socially vulnerable categories of the population get access to mainstream financial services is also an important policy concern. The FATF recognises that AML/CFT measures can be implemented in a way that undermines financial inclusion objectives. Regulators and financial service providers would benefit from clear guidelines and examples of implementation of AML/CFT requirements using the flexibility offered by the FATF Recommendations.

3. In response to international calls to consider AML/CFT requirements in the context of financial inclusion, FATF has worked in close coordination with the Asia Pacific Group on Money

[2] On the occasion of the 20th anniversary of the FATF Recommendations in June 2010, the FATF discussed the subject of financial inclusion on the first day of its Plenary meeting. See the FATF website (www.fatf-gafi.org/pages/aboutus/outcomesofmeetings/).

[3] www.fatf-gafi.org/documents/documents/ministersrenewthemandateofthefinancialactiontaskforceuntil2020.html
Although not defined in the Ministerial Declaration, financial exclusion and its risks arise when persons do not have effective access to appropriate and affordable formal financial services and therefore have to seek their financial services from informal providers in the cash economy. The risks include financial crimes committed by informal service providers; threats to the integrity of formal financial services (as due diligence inquiries fail when money trails disappear in the cash economy); social exclusion and continued extreme poverty and consumer protection risks, as informal providers are typically not subject to applicable consumer protection rules and their customers enjoy little if any recourse when transactions fail.
Where "financial exclusion risk" is used in this document, it refers to the risks it poses to ML/FT objectives, unless the context indicates otherwise.

[4] See FATF (2008), pp. 5 and 6, for criteria used to define Low Capacity Countries.

Laundering (APG) and the World Bank to create this Guidance paper. Insights have been sought from FATF members and observers but also more broadly from non-FATF and APG participants (individual jurisdictions and other FATF Style Regional Bodies (FSRBs)) and the private sector, through the FATF Private Sector Consultative Forum and beyond[5]. A first version of the Guidance was adopted in June 2011, based on the 2003 FATF Recommendations.

4. The FATF believes that this Guidance paper greatly contributes to the common objective adopted by the G20 to carry forward work on financial inclusion, including implementation of the *Financial Inclusion Action Plan*[6], endorsed at the G20 2010 Summit in South Korea. The 2010 Summit decided to launch the Global Partnership for Financial Inclusion (GPFI) as the main implementing mechanism. The GPFI is an inclusive platform for G20 countries, non-G20 countries, and relevant stakeholders intended to advance the "Principles for Innovative Financial Inclusion"[7] through multiple channels, including by encouraging standard-setting bodies to take full account of these principles[8]. The White Paper *Global Standard-Setting Bodies and Financial Inclusion for the Poor - Toward Proportionate Standards and Guidance*, adopted by the GPFI in September 2011 notes the steps taken by five international standard-setting bodies, whose activities are relevant to financial inclusion[9], to integrate–financial inclusion into their standards and guidance. It also underscores the critical importance of taking a proportionate approach to regulation that reflects (i) the risks of financial exclusion, (ii) the risks of increasing financial inclusion and (iii) country context in particular, countries that have high levels of financial exclusion and low regulatory capacity[10]. The White Paper welcomed the adoption of the FATF 2011 Guidance paper and highlighted the leading position taken by FATF to facilitate the implementation of its Recommendations whilst taking financial inclusion into account.

5. The present Guidance leverages existing related studies completed by various groups dealing with the broader aspects of financial inclusion, experts' views, consultation with interested parties and stakeholders and gathering jurisdictions' experiences by way of questionnaires.

6. After an extensive consultation with both the public and the private sectors, this updated Guidance paper was adopted by the FATF at its February 2013 Plenary[11].

---

[5] See the list of members of the Project Group as Annex 1

[6] www.g20.utoronto.ca/2010/g20seoul-development.html#inclusion

[7] See Annex 2

[8] One of the three established GPFI subgroups, the "Sub-Group on G20 Principles and Standard Setting Bodies", is devoted to advancing the engagement with standard-setting bodies and to implementing the Principles.

[9] In addition to FATF, the Basel Committee on Banking Supervision, the Committee on Payment and Settlement Systems, the International Association of Deposit Insurers, and the International Association of Insurance Supervisors

[10] Several of the standard-setting bodies discussed in the White Paper have taken steps to incorporate a proportionate approach, including the modification of standards and articulation of guidance that advances financial inclusion.

[11] It is expected that the Guidance paper will be endorsed by APG at its Annual meeting in July 2013.

Scope of the February 2013 Guidance Paper

7. The June 2011 version of the Guidance paper was developed within the framework of the 2003 FATF Recommendations. This 2nd version of the Guidance seeks to reflect the changes brought by the revised set of Recommendations, adopted on 16 February 2012[12].

8. One of the major changes brought by the new Recommendations is the reinforcement of the risk-based approach (RBA) as a general and underlying principle of all AML/CFT systems. This means that both countries and financial institutions are expected to understand, identify and assess their risks, take appropriate actions to mitigate them and allocate their resources efficiently by focusing on higher risk areas. The greater recognition of a risk-sensitive approach to implement AML/CFT measures – including in particular an approach that takes into consideration the risks of financial exclusion and the benefits of bringing people into the formal financial system – will be a key step for countries that wish to build a more inclusive financial system.

9. The Guidance paper examines the existing requirements that are the most relevant when discussing the linkage between AML/CFT policies and the financial inclusion objective. It also refers to other initiatives that the FATF has already launched that have important linkages with financial inclusion[13].

Objectives of the Guidance

10. This Guidance paper provides a general framework to assist jurisdictions in implementing an AML/CFT system that is consistent with the goal of financial inclusion. It is intended to support competent authorities in developing a set of comprehensive and balanced AML/CFT measures based on the ML/TF risk environment in which their financial systems operate. It also aims to promote the development of a common understanding of the FATF Recommendations that are relevant when promoting financial inclusion and clarifying the flexibility they offer, in particular through the risk-based approach. Finally, the paper shares countries' initiatives to address financial inclusion within the AML/CFT context. It has to be noted that those countries' experiences are presented for information only. Most of them have not been assessed against the FATF Recommendations, and their presentation can therefore not amount to an endorsement by FATF.

11. This Guidance paper does not explore how financial inclusion should be integrated into the mutual evaluation methodology and process. However, it highlights the need to better inform the assessors and the assessed countries based on the principle that financial exclusion could undermine the effectiveness of an AML/CFT regime given, among other things, the difficulty of detection (and enforcement of applicable law) in the informal sector[14]. A country's level of financial exclusion is

[12] FATF (2012)

[13] The FATF continues for instance working on the issue of New Payments Methods. FATF (2013b).

[14] The precise nature and impact of financial exclusion risk differs from country to country. The identification and the assessment of the relevant risks depend furthermore on the policy and regulatory objectives that are threatened. Financial inclusion can for example impact on the objectives relating to financial integrity and consumer protection (see footnote 2). While the AML/CFT regulator and the FATF, for example, may focus on

part of the contextual factors or issues to be considered when assessing the effectiveness of a country's AML/CFT regime, particularly its preventive measures.

12. This Guidance focuses on financially excluded and underserved groups, including low income, rural and undocumented persons. It considers experiences in both developed and developing countries, although it focuses more on initiatives taken in developing countries where the challenge is the greatest. Since developing and developed countries differ with regard to the origin and the extent of financial exclusion, as well as possible ways to address the related challenges, this Guidance seeks to address a range of situations that jurisdictions should be able to refer to depending on their level of economic development[15].

Target Audience

13. The Guidance is intended for:

- The public sector, specifically:
  - AML/CFT policymakers, regulators and supervisors tasked with implementing the FATF Recommendations
  - Policymakers, financial regulators and supervisors who are involved in the promotion of financial inclusion
- The private sector, specifically businesses, in particular, financial institutions that provide financial services and products to disadvantaged and other vulnerable groups, including low income and undocumented groups, in both developed and developing jurisdictions.

14. Many aspects of this document may also be useful to a broader audience including organizations providing support to financially excluded and underserved groups[16]; those engaged in providing technical assistance; and other international stakeholders dealing with the subject of financial inclusion.

Status and Content of the Guidance Paper

15. This Guidance is non-binding. It does not review the nature and level of FATF requirements but is consistent with the RBA and the flexibility provided in the FATF Recommendations by the RBA. It is not intended to provide a single model for promoting financial inclusion in the AML/CFT context but seeks to share experiences that jurisdictions and individual businesses may wish to consider. A variety of country experiences exist that address a variety of situations and economic

financial integrity risks, the banking regulator may focus on financial stability risks posed by financial exclusion. See CGAP (2012).

[15] See Annex 3 for examples of countries' actions to support financial inclusion.

[16] Including those that lead financial literacy program and campaigns.

circumstances. Different factors result in the exclusion of various parts of the population from certain financial sectors. Accordingly, different solutions must be adopted to address the specific factors that act as barriers for specific populations to specific financial services/products.

16. Along with the guidance set out in this document and for more specific aspects, jurisdictions should also refer to existing documentation that is available on the subject[17].

[17] See Bibliography and sources.

CHAPTER 1 – STATEMENT OF THE PROBLEM

What is Financial Inclusion?

17. While there is a consensus regarding the importance of financial inclusion, its definition can vary depending on the national context and on the stakeholders involved. From "banking the unbanked" to "branchless banking," a variety of catch phrases are sometimes used as near synonyms for financial inclusion, when in fact they describe specific aspects of a broader concept. In general terms, financial inclusion involves 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 formal financial sector. Financial inclusion also involves making a broader range of financial products and services available to individuals who currently only have access to basic financial products. Financial inclusion can also be defined as ensuring access to appropriate financial products and services at an affordable cost in a fair and transparent manner. For AML/CFT purposes, it is essential that these financial products and services are provided through financial institutions[18] subject to adequate regulation in line with the FATF Recommendations.

State of Financial Inclusion

18. Approximately 2.5 billion adults worldwide lack access to a formal bank account, which amount to 50% of the world's adult population[19]. Most of these people are concentrated in developing economies, where account penetration with a formal financial institution in 2011[20] was 41% on average, but with wide disparities across regions, ranging from 18% in the Middle East and North Africa to 39% in Latin America and Caribbean[21]. Besides, 22% of adults worldwide report having saved at a formal financial institution in 2011, while 9% report having originated a new formal loan[22].

[18] The term "financial institutions" used in this document refers to the definition of the FATF Glossary. Financial institutions are licensed or registered with a supervisory authority and subject to examination or oversight for compliance with domestic AML/CFT laws.

[19] According to the latest available data from the World Bank's *World Development Indicators database*, there are 5.08 billion adults age 15 and above worldwide. World Bank (n.d.)

[20] World Bank (n.d.), Global Findex, Note #1. A formal financial institution is defined by the World Bank's Global Findex to be a bank, credit union, cooperative, post office, or microfinance institution.

[21] World Bank (n.d.). The Global Findex database is based on a 2011 Gallup World Poll survey. The data collection methodology used by Gallup is valuable as it enables comparison across countries. However, the firms categorized as a "formal financial institutions" vary across the 148 countries polled, which may explain some of the inconsistencies between the Global Findex data and other data sources.

[22] World Bank (n.d.)

19. The problem of financial exclusion is greater if focus is on the poor people living on less than USD 2 per day, as their income is not only low but also irregular and they are therefore more vulnerable to external shocks and uncertainties of their cash flows. Among those living on less than USD 2 a day, only 23% have access to a formal account[23]. Nevertheless, studies have demonstrated that a number of poor people in developing countries have developed sophisticated financial lives, transacting through remittance systems outside the formal bank sector, saving and borrowing with an eye to the future and creating complex "financial portfolios" using mainly informal tools[24].

20. As far as remittances are concerned, officially recorded flows to developing countries are estimated to have reached USD 372 billion in 2011, an increase of 12.1% over 2010. The growth is expected to continue at a rate of 7-8% annually to reach USD 467 billion by 2014[25]. However, some experts suggest that if informal and underreported flows were included, the total amount of migrant remittances would be considerably higher – possibly up two to three times higher[26].

The Diversity of the Financially Excluded and Underserved Groups

21. Disadvantaged and other vulnerable groups, including low income households, handicapped persons, individuals in rural communities and undocumented migrants in both developed and developing jurisdictions, are more likely to be excluded from the formal financial sector. The "underserved" are those who currently have access to some financial services, but in a very limited manner. For example, someone may have access to a money or value transfer service provider, but not to a bank. "Underserved" may also mean that an individual or group technically has access, but is not using it because of other barriers, such as problems in meeting the documentary or other requirements, non-awareness, incorrect perceptions, limited knowledge, high cost, etc. Underserved clients represent a very heterogeneous category, with very different risk profiles in different jurisdictions. *As a consequence, they cannot be classified as low risk clients on the sole basis that they are financially excluded*. Appropriate risk management is required to address this diversity.

Challenges of Financial Exclusion

22. There are many reasons why individuals or groups may not take full advantage of mainstream financial service providers. The World Bank recently published a study[27] that shows that globally the most frequently cited reason for not having an account is the lack of enough money to use one. The next most commonly quoted reasons are that banks or accounts are too expensive and that another family member already has access to an account (a response identifying indirect users). The other

[23] World Bank (n.d.)

[24] Collins, D., *et al* (2009)

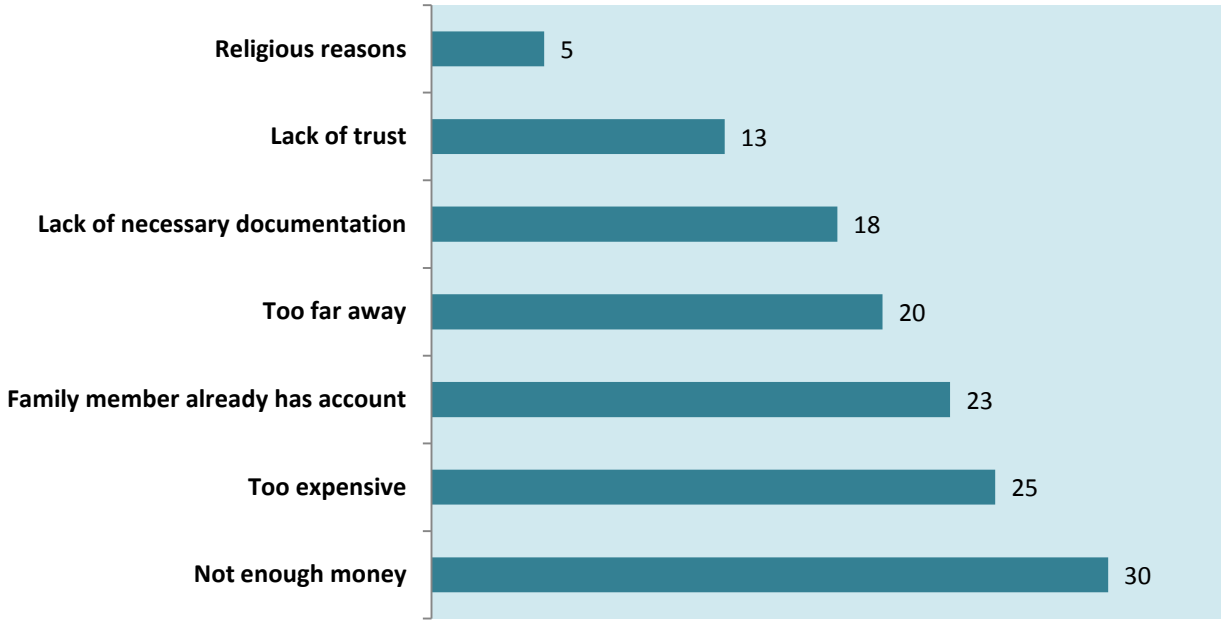
[25] World Bank (2012a)

[26] IFAD (2006)

[27] World Bank (n.d.)

reasons reported include banks being too far away, lack of proper documentation, lack of trust in banks, and religious reasons.

Figure 1. **Self-reported barriers to use of formal accounts**
Non-account-holders reporting barrier as a reason for not having an account (%)



Note: Respondents could choose more than one reason. The data for "not enough money" refer to the percentage of adults who reported only this reason.

Source: Demirguc-Kunt, A., and Klapper, L. (2012)

23. Regarding the lack of proper documentation, the report mentions that strict documentary requirements for opening an account may exclude workers active in rural areas or in the informal economy, who are less likely to have wage slips or formal proof of domicile. In Sub-Saharan Africa, documentation requirements potentially reduce the share of adults with an account by up to 23%.

24. The report concludes that many of the barriers to a formal financial services account could be addressed by public policy, which could pave the way to improve financial access. FATF believes that the present Guidance will contribute to removing existing and perceived obstacles and clarify how to implement AML/CFT requirements, including the documentation requirements, in a financial inclusion context.

25. The World Bank also points out that in most jurisdictions, opening a bank account, receiving a loan, withdrawing money or making a payment still requires going to a bank branch, ATM, or a point-of-sale terminal. However, these access points are usually limited in developing countries and lack of physical access (too far away) is mentioned as an important barrier. The key is finding alternative delivery channels although these may differ, depending on the target audience. Financial inclusion also requires changing financial habits. In that respect, one successful approach is to focus

on changing how government payments, such as wages, pension, and social and medical benefits, are delivered in both developed and developing countries. A number of initiatives have been taken in recent years to channel Government-to-Persons (G2P) payments, especially social protection benefits, through bank accounts[28].

26. There are also new financially excluded groups as a result of the introduction of inappropriate AML/CFT requirements which do not take into account the potential negative impact of such requirements. In some cases, the new AML/CFT requirements meant that services for those existing customers who could not provide the necessary documents had to be terminated[29]. In other instances it may mean that potential customers were not able to enter the formal financial system.

27. Financial inclusion is therefore a multi-dimensional challenge, of which AML/CFT requirements are an important aspect, but only one amongst many others. Solving the AML/CFT issue will not solve the problem of financial exclusion but is a component in an enabling framework. At the same time, one cannot ignore the fact that financial exclusion is an ML/TF risk and that financial inclusion can contribute to a more effective AML/CFT regime.

Balancing AML/CFT Requirements and Financial Inclusion

28. The impact of AML/CFT on the ability of socially and economically vulnerable people to access financial services has been under discussion for many years. In 2005, the World Bank supported a study to consider the impact of AML/CFT in selected developing countries. The report was published in 2008 and concluded that "*Measures that ensure that more clients use formal financial services therefore increase the reach and effectiveness of the AML/CFT controls*"[30]. Other studies, such as that conducted by CGAP in 2009[31], concluded that AML/CFT measures can negatively affect access to, and use of, financial services if those measures are not carefully designed.

29. Promoting formal financial systems and services is consequently central to any effective and comprehensive AML/CFT regime. Financial inclusion and an effective AML/CFT regime can and should be complementary national policy objectives with mutually supportive policy goals. Accordingly, the FATF Recommendations have flexibility, enabling jurisdictions to craft effective and appropriate controls taking into account the relevance of expanding access to financial services as well as the diverse levels and types of risks posed by different products and supply channels. The challenge is finding the right level of protection for a particular financial environment.

---

[28] See countries' experiences in Annex 5, as well as the recently launched *Better than Cash* Alliance http://betterthancash.org/, and World Bank (2012b)

[29] This was for example the case in South Africa in relation to asylum seekers after the Financial Intelligence Centre published a Public Compliance Communication to the effect that the documents that the government issued to asylum-seekers were not appropriate for purposes of account opening.

[30] Bester, H., *et al* (2008).

[31] Isern, J., and De Koker, L. (2009); De Koker, L. (2006).

30. In addition, new financial products and services have been created in the past few years which may contribute to expanding access to new markets and clients[32]. To date, challenges have appeared in how to effectively apply AML/CFT mechanisms to these new products and services. This is particularly evident with branchless and mobile financial services[33].

31. AML/CFT obligations can increase the cost of doing business, which may be borne by financial institutions, reducing potential profits and making it less attractive for the private sector to reach out to the unbanked and provide them with essential financial products and services. The costs may also be-transferred to customers, potentially discouraging some from using the formal financial system, particularly if informal options are cheaper and equally reliable. If a customer lacks a government-issued form of identification, for example, a financial institution may need to use other, more costly methods to verify identification, which could be a disincentive to serve certain customers. For some categories of potential clients, and especially for vulnerable and low-income groups, this creates an additional barrier to financial inclusion[34].

32. A flourishing underground economy that is attractive for clean money is also available for illicit transactions. Alternative or underground providers can thus become a ready conduit for illicit transactions that are difficult for governmental authorities to detect and that undermine AML/CFT efforts. However, through a dialogue with national authorities and the financial industry, and on the basis of the flexibility available under the FATF Recommendations, possible solutions can be found in meeting the needs of the financially excluded in compliance with the FATF requirements. Challenges faced by regulators, financial service providers and ultimately customers in this regard are further analysed in Chapter 2.

[32] see Annex 5 for more details.

[33] see FATF (2013b).

[34] Disproportionate AML/CFT obligations also have negative impact on innovation taking place within the regulated financial services industry. Impact assessments and industry consultations can help to mitigate unintended negative effects.

CHAPTER 2 - GUIDANCE ON ACTION TO SUPPORT FINANCIAL INCLUSION

I. Preliminary Remarks

33. The FATF has identified a series of measures that financial institutions or any other profession subject to AML/CFT requirements must take on the basis of national legislation to prevent money laundering and terrorist financing. These measures, known as "preventive measures", have been designed by the FATF to protect financial institutions from abuse, and help them to adopt adequate controls and procedures. Although these measures create challenging requirements, they have been elaborated with some degree of flexibility in order for countries to build their AML/CFT regimes in a way that is tailored to domestic circumstances. One of the major changes brought by the 2012 FATF Recommendations was to strengthen and emphasise a comprehensive, first order principle of the Risk-Based Approach (RBA) that applies across the FATF Recommendations and provides the overarching framework for their implementation. Countries will therefore be able to build AML/CFT regimes that specifically address their identified higher ML/TF risks while taking into account the importance of financial inclusion, both from an AML/CFT perspective and from a social policy point of view.

34. While the 2003 FATF Recommendations were also intended to encourage countries to apply an RBA, and did impose certain RBA related obligations, a review of the results of countries' assessments carried out between 2005 and 2011 (among the FATF and the FSRBs community) shows that very few countries took full advantage of this flexibility. Rather, most countries have introduced a uniform approach with the same AML/CFT requirements applicable to all financial institutions, clients, products and services. This may have hampered financial inclusion efforts of financial providers. At the customer level, customers who conduct limited and small value (potentially lower risk) financial transactions must often meet the same customer due diligence requirements as higher risk customers who frequently conduct large transactions.

35. In addition to the significant resource capacity and coordination challenges in developing countries, one reason the RBA has not yet been widely embraced is that it might not be well understood. A clearer explanation and understanding of the core elements of the FATF Recommendations and of the RBA can support countries' efforts to tailor their AML/CFT regimes domestically and develop an AML/CFT framework that fosters financial inclusion. This Chapter (i) explains the most relevant elements of the FATF Recommendations and the RBA, (ii) provides possible models of innovative legislation and (iii) gives examples of business practices that can help promote better financial inclusion.

II. Overview of the Risk-Based Approach of the FATF[35]

36. The revised Recommendations make the RBA central in implementing FATF requirements and start with a dedicated Recommendation on the need to understand, identify and assess risks and to apply mitigation and management measures that are risk-sensitive, through an RBA (Recommendation 1).

37. The general principle of a RBA is that where there are higher risks, countries must require financial institutions to take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower (and there is no suspicion of money laundering or terrorist financing) simplified measures may be permitted. This means that countries can and should (in part, to address the consequential risks of financial exclusion) move away from "one size fits all" solutions, and-tailor their AML/CFT regime to their specific national risk context. Under the RBA, the intensity of AML/CFT measures depends on the level and nature of the risks identified. The RBA *requires* countries to take a more enhanced and focused approach in areas where there are higher risks (obligation for countries), *allows* them to take a simplified approach where there are lower risks (option for countries), and creates exemptions from certain requirements if there is proven low risk and other conditions are met[36]. It enables 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.

38. Taking a risk-based approach to AML/CFT safeguards may help countries build a more inclusive financial system by allowing financial institutions to apply certain simplified AML/CFT measures to those who may present a lower ML/TF risk. It will avoid having excessive, disproportionate and unnecessary requirements, including those that may hinder access to appropriate services for under-served groups, as described in Chapter 1. By increasing financial inclusion, a proportionate approach can reduce the scope of transactions conducted through the informal financial system, away from regulatory and supervisory oversight.

39. There are potentially negative consequences if the controls designed for standard risks and higher risks are also applied to situations where the risks are lower[37]. This "over-compliance" approach by regulators and financial institutions could exacerbate financial exclusion risk, thereby increasing overall ML/TF risk. Regulators/supervisors should play a role and provide further

[35] For more information on the risk-based approach (RBA) developed by the FATF, please refer to the RBA Guidance that the FATF has published since 2007 in cooperation with the financial sector and all designated non-financial businesses and professions. The reports are available on the FATF website (www.fatf-gafi.org). These documents are being updated to reflect the changes brought to the new Recommendations.

[36] « Low risk » situations refer to cases that may qualify for an exemption from the FATF Recommendations, while a simplified AML/CFT regime may apply to "lower risks" cases.

[37] De Koker, L. and Symington, J. (2011)

guidance when institutions overestimate ML/TF risks or adopt overly-conservative control measures[38].

Developing a risk assessment – A key step to identifying low risk and lower risk situations

40. The application of the RBA, as outlined in Recommendation 1, requires as a starting point that countries take appropriate steps to understand, identify and assess the ML/TF risks for different market segments, intermediaries, and products on an ongoing basis[39]. This includes supervisors or other authorities assessing specific risks relevant to their functions. Equally, financial institutions are required under Recommendation 1 to understand, identify and assess the ML/TF risks relevant to their activities.

41. Countries can use different means to conduct risk assessments. There is no single or universal methodology for conducting an ML/TF risk assessment. Some countries may use a single approach for money laundering and terrorist financing, others may develop different assessments for the two sets of risks, or specific assessments for different sectors and activities, or on a thematic basis (*e.g.,* proceeds of corruption related ML). There is flexibility about what form these assessments should take. Sectoral, multi-sectoral or thematic risk assessments, which are less resource intensive, might be the starting point for developing countries. What is important is that the assessments are comprehensive in scope, reflect a good understanding of the risks and are coordinated nationally.

42. The FATF *Guidance on National Money Laundering/Terrorist Financing Risk Assessment*[40] defines key concepts and outlines the successive stages required to conduct a national risk assessment:

Box 1. **About the definition of risk**

Risk can be seen as a function of three factors: threat, vulnerability and consequence. Ideally, a risk assessment involves making judgments about all three elements, and their consequences.

- A **threat** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as the past, present and future ML or TF activities. *Threat* is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF risk. For this reason, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment.

[38] Chatain, P.L. *et al* (2009); De Koker, L. and Symington, J. (2011)

[39] This Guidance paper does not examine in detail the challenges a country may face when conducting risk and threat assessments – see FATF (2013). This Guidance paper addresses the challenges that countries face in identifying and assessing the ML/TF risks of certain of their financial institutions or financial activities.

[40] FATF (2013)

In some instances, certain types of threat assessments might serve as a precursor for a ML/TF risk assessment[1].

- The concept of ***vulnerabilities*** as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/FT risk assessment context, looking at *vulnerabilities* as distinct from *threat* means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial products or type of service that make them attractive for ML or TF purposes.
- **Consequence** refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

Note

1. The United Nations Office on Drugs and *Crime* (UNODC) has published *Guidance on the preparation and use of Serious and Organised Crime Assessments* ("The SOCTA Handbook"), which provides useful information on the conduct of certain of national threat assessments.

Box 2. **About the risk assessment process**

The risk assessment process can be divided into a series of activities or stages:

- In general terms, the process of **identification** in the context of an ML/TF risk assessment starts by developing an initial list of potential risks or risk factors[1] countries face when combating ML/TF. Ideally at this stage, the identification process should attempt to be comprehensive; however, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.
- **Analysis** lies at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, the aim of this stage is to gain a holistic understanding of each of the risks – as a combination of threat, vulnerability and consequence in order to work toward assigning some sort of relative value or importance to them. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk and the purpose of the risk assessment, as well as based on the information, data and resources available.
- **Evaluation** in the context of the ML/TF risk assessment process involves taking the risks analysed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. The priorities

can contribute to development of a strategy for their mitigation.

Note

1. The term *risk factors* is used to refer to specific threats or vulnerabilities that are the causes, sources or drivers of ML or TF risks.

43. The national risk assessment will provide useful background information to identify low risk situations which could benefit from an exemption, and lower risk situations for which simplified AML/CFT measures could apply. In the 2012 FATF Recommendations, FATF gives examples of circumstances where the risks of money laundering and terrorism financing could potentially be considered as lower, in relation to particular categories of customers, countries or geographic areas, or products, services, transactions or delivery channels (INR. 10 par. 17)[41]. The lower level of risk is very much determined by the national or local context and the specific environment of the customer. In most cases, a combination of several factors (such as the client's level of income, the business sector in which the client operates, the region's exposure to ML/FT threat etc.), rather than a single element, will be required. The risk assessment should therefore determine the common criteria according to which risks for a given market could be considered as lower.

44. In a financial inclusion context, newly banked and vulnerable groups often conduct a limited number of basic, low value transactions. Hence, they may present a lower ML/TF risk and this could appropriately be recognized as such by the risk assessment. However, it is important to keep in mind that underserved clients represent a very heterogeneous category with very different risk profiles in different jurisdictions. As a consequence, they cannot be classified as lower risk clients solely on the basis that they are low income individuals, who have recently been integrated into the formal financial system. Countries will need to clarify if and under what conditions and for which type of products and transactions low value clients can appropriately be subject to a simplified AML/CFT regime.

45. The Interpretive Note to Recommendation 1 (INR. 1) requires countries to communicate the results of the ML/FT risk assessment to financial institutions, so that they can use the national risk assessment to determine the level and nature of the risk environment in which they operate, and integrate this data into their own risk profiling. This analysis will help financial institutions identify the money laundering and terrorist financing risks that are relevant to their business. Individual financial institutions should also factor in other risk indicators (*e.g.,* their specific operations, the scale of their business, the risks in relation to types of customers, countries or geographic areas, particular products, services, transactions or delivery channels) to determine their own overall risk exposure.

46. It is important to emphasize that there is no requirement, or expectation, that an institution's RBA must involve a complex set of procedures. The particular circumstances of a firm's business, in particular its money laundering/terrorist financing risk will determine how it should implement an RBA: it should design and implement controls to manage and mitigate the risks, monitor and where relevant, improve the effective operation of these controls, and record what measures have been

[41] See par. 69.

implemented and why. The appropriate approach is ultimately a question of judgement by financial institutions, expert staff and senior management. While no set of measures will detect and prevent all money laundering or terrorist financing, an RBA can serve to balance and focus the resources being applied by individual firms with a realistic assessment of the money laundering and terrorist financing threats the firm faces.

47. This risk-mapping and rating will enable financial institutions to determine lower risk scenarios in relation to certain client groups or financial inclusion products[42]. On this basis, a simplified and proportionate AML/CFT regime might apply, subject to the conditions specified by the FATF Recommendations, and whether the country where the financial institution operates allows the application of a simplified regime. A simplified set of CDD requirements, where appropriate, may facilitate access to formal financial services for the unbanked and underserved in a cost-efficient manner for financial institutions, while mitigating financial exclusion risks to national AML/CFT objectives.

48. The APG and the World Bank have developed a national AML/CFT risk assessment template as part of the Strategic Implementation Planning (SIP) Framework to assist jurisdictions in implementing the recommended actions from their mutual evaluation reports[43]. They are in the process of revising the SIP Framework to reflect the 2012 FATF Recommendations. The World Bank and IMF have also respectively developed other risk assessment tools and methodologies. The World Bank tool contains a specific module for the risk assessment of financial products that is designed to facilitate financial inclusion[44].

49. Most countries have not yet attempted to conduct a national risk assessment[45]. For a number of jurisdictions, especially Low Capacity Countries where much of the population is unbanked, this will present major challenges, in light of their capacity and structural constraints and the lack of meaningful data to inform the risk assessment process. FATF recognises that the size and complexity of the country, its ML/TF environment, the maturity and sophistication of the AML/CFT regime, and its overall capacity and structural constraints may influence the development of a full national-level understanding of ML/TF risks. Where the capacity of individual financial institutions, in particular small service providers, is too limited to undertake an institutional risk assessment on their own, the country may consider allowing such institutions to undertake, and rely on, joint sectoral or multi-sectoral risk assessments.

50. The FATF acknowledges that the application of an RBA to terrorist financing has both similarities and differences compared to money laundering. Both require a process for identifying, understanding and assessing risk. However, the characteristics of terrorist financing mean that the risks may be difficult to assess and the implementation strategies may be challenging due to considerations such as the relatively low value of transactions involved in terrorist financing, or the

[42] Data on the criminal abuse of lower risk financial products should be collected and analyzed to determine whether the assessments properly reflected the risks posed. See De Koker, L. (2009)

[43] See Annex 6 I.

[44] See Annex 6. I and II.

[45] See FATF (2013), Annex III, examples from Australia, The Netherlands, Switzerland and the US.

fact that funds can come from legal sources. The FATF *Guidance on National Money Laundering/Terrorist Financing Risk Assessment* includes specific risk indicators with regard to terrorist financing, such as unaddressed history of terrorism financing activity or limited regulation of money or value transfer systems[46]:

III. The flexibility offered by the FATF Recommendations in proven low risk scenarios: the exemptions

51. As permitted by the FATF Recommendations (INR 1. par. 2), a country may take risk into account, and may decide not to apply certain AML/CFT measures to a particular type of financial institution or activity, or Designated Non-Financial Business or Profession (DNFBP), provided that certain conditions are met.

52. The FATF has not prescribed any specific legal way in which countries should introduce these exemptions. Whichever form they take, national implementing regulations should be clear and unequivocal as to the conditions and potential beneficiaries of the exemptions.

53. *Covered financial institutions and activities* - In defining financial institutions[47], the FATF provides a list of financial activities or operations to be covered for AML/CFT purposes.

Box 2. **FATF definition of "financial institutions"**

Financial institutions means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public. [1]
2. Lending.[2]
3. Financial leasing.[3]
4. Money or value transfer services.[4]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:

   (a) money market instruments (cheques, bills, certificates of deposits, derivatives etc.);

   (b) foreign exchange;

   (c) exchange, interest rate and index instruments;

   (d) transferable securities;

[46] See FATF (2013), Annexes 1 and II.

[47] See Glossary of the FATF Recommendations, FATF (2012)

(e) commodity futures trading.

8. Participation in securities issues and the provision of financial services related to such issues.

9. Individual and collective portfolio management.

10. Safekeeping and administration of cash or liquid securities on behalf of other persons.

11. Otherwise investing, administering or managing funds or money on behalf of other persons.

12. Underwriting and placement of life insurance and other investment related insurance.[5].

13. Money and currency changing.

Notes:

1. This also captures private banking.
2. This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).
3. This does not extend to financial leasing arrangements in relation to consumer products.
4. This does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.
5. This applies both to insurance undertakings and to insurance intermediaries (agents and broker)

54. *Conditions for exemption* - INR. 1 par. 6 indicates that there are two separate situations where countries may decide not to apply some of the FATF Recommendations requiring financial institutions to take certain actions:

- there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP;

or

- when a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is low risk of money laundering or terrorist financing.

3. 1. THE "PROVEN LOW RISK" EXEMPTION

55. The FATF Recommendations (INR. 1 par. 6a) allow countries not to apply some of the FATF Recommendations for financial institutions provided that:

- it is based on a proven low risk of money laundering and terrorist financing;
- this occurs in strictly limited and justified circumstances; and
- it relates to a particular type of financial institution or activity, or DNFBP.

56. The main challenges for countries seeking to make use of the proven low risk exemption will be to demonstrate the limited and justified circumstances pertaining to a specific type of financial institution, DNFBP, or activity and provide justification for the view that there is a low risk of ML and

TF. The justification should be based on an appropriate risk assessment[48] and the level of detail will depend on the range and possible impact of the exemption.

57. In most jurisdictions, the current exemptions or limitations on applying AML/CFT requirements to certain financial activities are essentially based on a "perception" of low risk because of the activity's size or nature (*e.g.*, leasing, factoring, life insurance) with little or no evidence to support the risk ranking. Only a few jurisdictions have undertaken risk assessments before exempting a sector. The World Bank has developed a tool to assess ML risk of financial inclusion products that may assist countries to undertake the required risk assessments[49].

3.2. THE *"DE MINIMIS"* EXEMPTION

58. The FATF Recommendations allow countries not to apply AML/CFT obligations when a natural or legal person carries out a financial activity on an occasional or very limited basis (having regard to quantitative and absolute criteria), relative to its other, primary business activities and when there is a low risk of money laundering and terrorist financing. Money or value transfer services cannot benefit from the exemption (INR. 1 par. 6b).

59. While the criterion that financial activity must be carried out "*on an occasional and very limited basis*" leaves room for interpretation, countries that opt to apply the *de minimis* exemption must be able to demonstrate a cause and effect relationship between the very limited and occasional nature of the financial activity and the assessed low level of ML and TF risk. When a country decides to exempt certain natural or legal persons from AML/CFT requirements because they engage in financial activity on an occasional or very limited basis, the onus is on the country to establish that the conditions set out in the FATF Recommendations are met.

60. The European Commission has attempted to define the notion of "financial activity carried out in occasional or very limited basis" in a systematic way in Article 2(2) of the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[50]. It provides a flexibility[51] similar to that set out in the FATF definition of financial institutions. Article 4 of Directive 2006/70/EC[52] which contains implementing measures for Directive 2005/60/EC sets out the technical criteria for simplified customer due diligence

[48] See par. 40 and s.

[49] See Annex 6 II. for details.

[50] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF

[51] "The Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or terrorist financing occurring do not fall within the scope of Article 3(1) or (2)" *i.e.* are not credit or financial institutions as defined by the Directive.

[52] Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_214/l_21420060804en00290034.pdf.

procedures and for exempting a financial activity conducted on an occasional or very limited basis. Using that legal framework and its safeguards, some EU members have opted for such exemptions.

For instance, the Money Laundering Regulations 2007 in the UK foresee such a scenario (Schedule 2):

1. For the purposes of regulation 4(1)(e) and (2), a person is to be considered as engaging in financial activity on an occasional or very limited basis if all the following conditions are fulfilled:

   (a) the person's total annual turnover in respect of the financial activity does not exceed £64,000;

   (b) the financial activity is limited in relation to any customer to no more than one transaction exceeding 1,000 euro, whether the transaction is carried out in a single operation, or a series of operations which appear to be linked;

   (c) the financial activity does not exceed 5% of the person's total annual turnover;

   (d) the financial activity is ancillary and directly related to the person's main activity;

   (e) the financial activity is not the transmission or remittance of money (or any representation of monetary value) by any means;

   (f) the person's main activity is not that of a person falling within regulation 3(1)(a) to (f) or (h)[53];

   (g) the financial activity is provided only to customers of the person's main activity and is not offered to the public.

[53] *I.e.,* the following persons (a) credit institutions; (b) financial institutions; (c) auditors, insolvency practitioners, external accountants and tax advisers; (d) independent legal professionals; (e) trust or company service providers; (f) estate agents; and (h) casinos.

IV. The FATF Recommendations in the light of financial inclusion objectives

4.1. CUSTOMER DUE DILIGENCE (RECOMMENDATION 10)

61. Under the FATF Recommendations, financial institutions must perform customer due diligence (CDD) in order to identify their clients and ascertain information pertinent to doing financial business with them. CDD requirements are intended to ensure that financial institutions can effectively identify[54], verify and monitor their customers and the financial transactions in which they engage, in relation to the money laundering and terrorism financing risks that they pose.

62. The three core elements of "identification", "verification" and "monitoring" are interrelated and closely associated in the FATF Recommendations. They are intended to reinforce each other so that the financial institution builds knowledge of the customer that is crucial from an AML/CFT perspective.

63. The revised FATF Recommendations have not modified the basic CDD requirements. They do, however, clarify how the broad RBA principle relates to the implementation of CDD measures. In particular, and of specific relevance to financial inclusion, the revised FATF Recommendations provide indicators to identify potential lower risks factors (INR.10. par.16 to 18), and examples of simplified due diligence measures that the RBA allows (INR.10. par.21.). These examples are intended as illustrations only, and should not be read as either exhaustive or mandatory.

Circumstances in which CDD must apply

64. Under the FATF Recommendations, all financial institutions that are subject to AML/CFT obligations are required to implement CDD measures, including identifying and verifying the identity of their customers, when:

- establishing business relations[55];
- carrying out occasional transactions above USD/EUR 15 000 or that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

[54] FATF Recommendation 10 does not allow financial institutions to keep anonymous accounts or accounts in obviously fictitious names.

[55] The FATF Recommendations do not define this notion. It is left to countries to decide whether business relations are established.

CDD measures - general

65. Pursuant to these transaction thresholds and other criteria, the institutions, professions and businesses subject to AML/CFT obligations must:

a) Identify the customer and verify that customer's identity, using reliable, independent source documents, data or information.

b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

d) Conduct ongoing due diligence on the business relationship and scrutinize transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer and its business and risk profile, including, where necessary, the source of funds.

66. Applying these CDD measures is challenging for financial service providers, particularly financial institutions dealing with "small" clients and those in Low Capacity Countries. It is essential to distinguish between identifying the customer and verifying identification. Customer identification entails the gathering of information on the (future) customer to identify him/her. At this stage, no identification documentation is collected. In contrast, the verification of the customer identification requires checking reliable, independent source documentation, data or information that confirms the veracity of the identifying information that was obtained during the identification process.

67. Industry feedback highlights a number of practical difficulties regarding identification and verification requirements, most of which arise pursuant to national legislative or regulatory requirements, and not the FATF Recommendations. For instance, in a normal CDD scenario, the FATF Recommendations do not require information to be gathered on matters such as occupation, income or address, which some national AML/CFT regimes mandate, although it may be reasonable in many circumstances to seek some of this information so that effective monitoring for unusual transactions can occur. Similarly, although a majority of countries specify the use of a passport or government-issued identification card as one of the methods that can be used to verify the identity of customers, the FATF Recommendations do allow countries to use other reliable, independent source documents, data or information. This flexibility is particularly relevant for financial inclusion, since low income migrant workers, for example, often lack standard identification documents. Rigid CDD requirements that insist on government-issued identification documents, adopted by some countries or financial institutions, have acted as barriers to these disadvantaged populations obtaining access to the formal financial system.

CDD measures - lower risk scenarios

68. The revised FATF Recommendations allow for simplified CDD measures where there is a lower risk of money laundering and terrorist financing (INR. 1 par.5. and INR 10. par.16 to 18 and par.21). This is an option that is open to all countries. Jurisdictions may consider establishing a simplified CDD regime, for specifically defined lower risk customers and products. Countries may also allow financial institutions to decide to apply simplified CDD measures in lower risk situations, based on their own institutional risk analysis. In any case, simplified CDD measures is not permitted if there is any suspicion of money laundering, or terrorist financing, or where specific higher-risk scenarios apply.

69. *Examples of lower risk situations*. The FATF gives examples of circumstances where the risk of money laundering or terrorist financing might be considered as potentially lower, in relation to particular types of customers, countries or geographic areas, or products, services, transactions or delivery channels (INR. 10 par. 17). The examples are not prescriptive and do not amount to an exhaustive list. The FATF explicitly includes as one lower risk example "*financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes*". This means that it could be reasonable to apply simplified CDD measures for customers of products fulfilling those conditions. For instance, so-called "small bank accounts"[56] for unbanked individuals who lack acceptable identification documents, where the account has caps on overall value, frequency of use, and size of transactions to mitigate the risk of potential for misuse while still providing adequate functionality. This would be particularly relevant for individuals who rely on remittances from family members living and working away from home. Financial institutions still need to monitor lower-risk accounts, but it may be appropriate to do so less frequently and less intensely than with standard-risk accounts, which allows a more efficient allocation of resources, permitting financial institutions to focus their compliance resources on higher risk threats. In all situations of simplified CDD, the lower risk circumstances will have to be confirmed based on a thorough and documented risk assessment, conducted at the national, sectoral or at the financial institution level (INR. 10 par. 16) [57].

70. As the above example makes clear, the FATF Recommendations support the development of entry-level banking or other financial products that will facilitate the integration of financially excluded people into the formal financial sector and mitigate ML/TF risks relating to financial exclusion. Countries will have to specify the different criteria required to benefit from a simplified CDD regime or require financial institutions to do so within their own risk management framework. In general, targeted products may include several specific conditions such as the customer being a natural person, limited transactions in amount (*e.g.,* withdrawals not exceeding X EUR/USD per day or X per month), limited account balance at any time etc.

71. *Application of simplified measures.* Simplified CDD never means a complete exemption or absence of CDD measures. A simplified set of CDD measures may be basic and minimal but must still respond to each of the four CDD components that apply to "standard" customer relationships and

[56] Such accounts lay also be referred to as low-value, simple or no-frills accounts

[57] See par. 40 and s.

transactions[58]. In line with the RBA approach[59], it is the intensity and the extent of customer and transaction information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level. In a lower risk context, fulfilling CDD customer identification, verification and monitoring requirements of Recommendation 10 could for example entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information.

72. INR. 10 par.21 provides a number of examples of possible simplified measures with respect to the timing and verification of customer identity and intensity of transaction monitoring. Again, these examples are proposed for guidance only and should not be considered as prescriptive or exhaustive. They include the possibility of verifying the identity of the customer and the beneficial owner after the establishment of the business relationship, reducing the frequency of customer identification updates or reducing the degree of ongoing monitoring and scrutinising transactions, based on a reasonable monetary threshold[60].

73. Regarding beneficial ownership requirements, in a financial inclusion context the beneficial owner will in most instances be the customer him/herself, or a closely related family member. Situations where suspicions arise that the account holder is used as a strawman, or frontman and is not the real owner,-should not be treated as a lower risk and normal or enhanced measures should be applied (INR. 10 par. 15 a).

74. Countries may consider applying a so called "progressive" or "tiered" KYC/CDD approach whereby low transaction/payment/balance limits could reduce money laundering and terrorism financing vulnerabilities. The stricter the limits that are set for particular types of products, the more likely it would be that the overall ML/TF risk would be reduced and that those products/services could be considered as lower risks. Simplified CDD measures might therefore be appropriate. This approach may provide undocumented (financially excluded) individuals access to accounts or other financial services with very limited functionalities. Access to additional services (*e.g.,* higher transaction limits or account balances, access through diversified delivery channels) should be allowed only if/when the customer provides proof of identity and address. For example, in India, the government amended the AML/CFT regulations to authorize banks to open a "small" or "no frill" savings account for low income customers lacking acceptable forms of identification, using simplified CDD norms. The account is subject to strict limitations on the yearly aggregate of all credits, the monthly aggregate of all withdrawals and transfers, and the balance at any point. It can only be opened at an institution with core banking facilities that can monitor the account and ensure that the transaction and balance limits are observed. The account is operational for 12 months and can only

[58] See par. 65.

[59] See par. 37 and s.

[60] Specific examples of simplified measures which could be envisaged by countries for each step of the CDD process to accommodate the specificities of lower risk financial inclusion products or situations are detailed in the following paragraphs.

be renewed for another 12 months if the account holder provides evidence that he/she has applied for valid identity documents within a year of account opening[61].

CDD measures – customer identification

75. The FATF Recommendations do not specify the exact customer information (referred to by certain countries as "identifiers") that businesses subject to AML/CFT obligations should collect to carry out the identification process properly, for standard business relationships and for occasional transactions above USD/EUR 15 000. Domestic legislation varies, although common customer information tends to consist of name, date of birth, address and an identification number. Other types of information (such as the customer's occupation, income, telephone and e-mail address, etc.) are generally more business and/or anti-fraud driven and do not constitute core CDD information that must be collected as part of standard CDD—although such information could appropriately be part of enhanced CDD for higher risk situations.

76. The FATF Recommendations allow countries' laws or regulations to apply an RBA to the types of customer information that must be collected to start a business relationship. A carefully balanced approach has to be taken, because if identification processes are too lean, monitoring may make a limited contribution to risk mitigation, and manual or electronic scanning of transactions may not be able to identify individual suspicious activity effectively[62]. In some countries, differentiated CDD requirements have been introduced, in relation to certain types of financial products. For instance in Colombia, a 2009 modification of the Finance Superintendence of Colombia (SFC) Basic Banking Circular simplified AML/CFT procedures for low-value electronic accounts and mobile accounts that are opened via agents (who receive and forward the application materials).

CDD measures – verification of customer identification

77. The FATF Recommendations require financial institutions to verify the customer's identity using reliable, independent source documents, data or information. When determining the degree of reliability and independence of such documentation, countries should take into account the potential risks of fraud and counterfeiting in a particular country. It is the responsibility of each country to determine what can constitute "reliable, independent source documents, data or information" under its AML/CFT regime. The general application of the RBA can introduce a degree of flexibility as to the identity verification methods and timing.

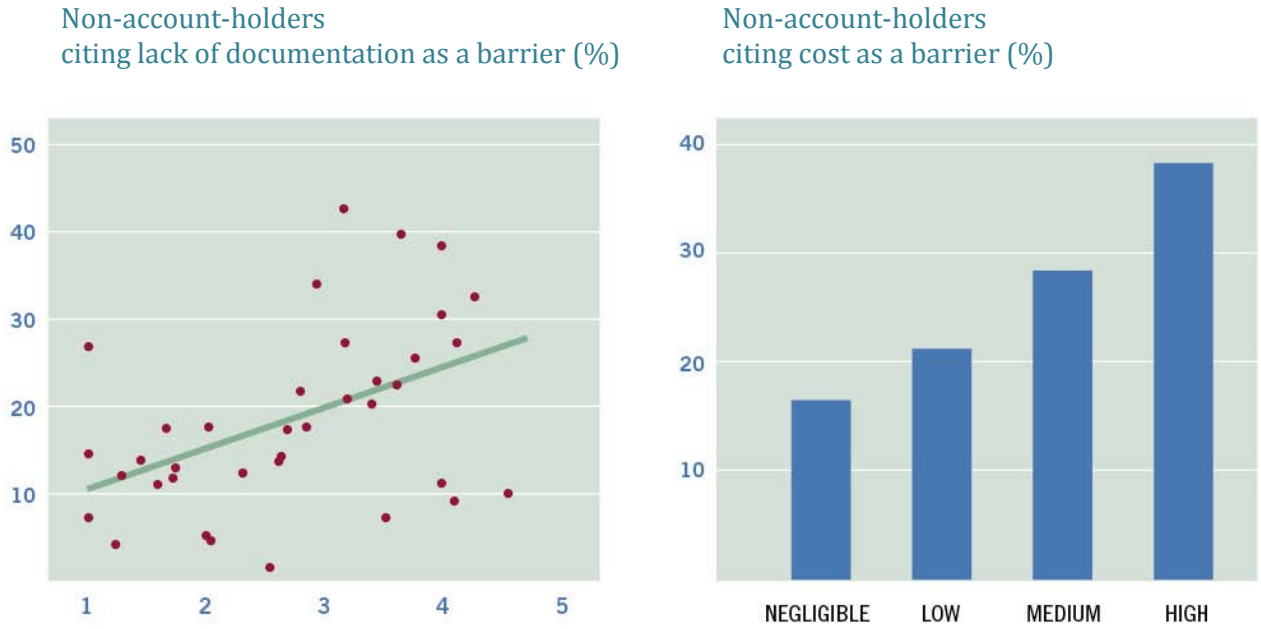
78. According to the industry, the customer identity verification stage is, in all instances, the most difficult and burdensome part of the process. Rigorous verification requirements can act as a disincentive for financial inclusion.

[61] See also experiences from Mexico, Malawi, Brazil, Pakistan as part of Annex 7.

[62] See also par 102.

79. The World Bank has pointed out that respondents to its recent survey often quoted lack of documentation as one of the central reasons for not having an account, especially in countries that require extensive or formal, government-issued documentation[63]:

Figure 2. **Objective data support perceptions of documentation requirements and cost as barriers to use of formal accounts**



Note: Data on number of documents required are for 2005. Data on annual fees are for 2010 and reflect scoring by the national central bank. The sample for the left-hand panel includes 38 economies, and the sample for the right-hand panel 100 economies.

Source: Demirguc-Kunt, A. and Klapper, L. (2012); World Bank, Bank Regulation and Supervision Database; World Bank Payment Systems Database

80. *Relying on a broader range of acceptable identification means*. To address such challenges[64], countries have expanded the range of acceptable IDs for the verification process to include such documentation as expired foreign IDs, consular documents or other records that undocumented people can typically acquire in the host country (bills, tax certificate, healthcare document, etc.). Using an RBA, local authorities have often allowed a broader range of documentation in pre-defined types of business relationships and for specific (financial inclusion) products and accounts, with low balance limits[65]. Countries should take advantage of the RBA to facilitate proportionate

[63] World Bank (n.d.).

[64] This may address the issue of the identification of children since children generally lack IDs and at times do not have guardians.

[65] See experiences from various countries in Annex 5.

requirements with regard to acceptable IDs that will support the provision of relevant services to unserved groups[66].

81. Groups such as community-based financial cooperatives that provide defined financial services to their members only, can have a CDD regime that takes note of their nature. The financial service provider can leverage off the membership process for persons to become members of the cooperative to also meet CDD requirements. This may be considered an alternative form of CDD which reaches the same objective as the normal identification and verification process in retail financial institutions.

82. *Fraud risk relating to alternative acceptable IDs*. Countries should remain mindful that alternative forms of acceptable identification may be more susceptible to fraud and abuse. For instance, whether reliance can appropriately be placed on a letter from a village chief to verify a customer's identity depends on the village chief's integrity and knowledge of the customer. In some reported cases, village chiefs began to demand money for their "verification services". Although such abuse may not be widespread, it is important to remember that like every method of verifying customer identification, alternative identification processes require some basic due diligence and monitoring to ensure integrity and reliability. A proper risk analysis is crucial to support the adoption of verification processes that are proportionate to the level of ML/TF risk.

83. In South Africa, in May 2010, the Financial Intelligence Centre issued an advisory to banks instructing them not to accept documents issued by the South African government to asylum-seekers evidencing their asylum applications as identification documents for the purpose of opening bank accounts. However, following litigation challenging that position, a compromise was reached allowing banks to accept the asylum documentation to verify identity but only after confirming the authenticity of the document with the Department of Home Affairs.

84. *Postponing ID verification*–Amongst the examples of simplified CDD measures in INR. 10 par. 21, the verification of the customer's (and beneficial owner) identity after establishment of the business relationship is envisaged, *i.e.* if account transactions rise above a defined monetary threshold. As part of a tiered CDD approach[67], customers can be provided with limited and basic services, and access to a full or expanded range of services or higher transactions ceilings would only be granted once full identity verification has been conducted.

85. This flexible approach for limited purpose accounts, where verification is postponed but not eliminated, allows clients to get access to basic products with limited functionalities and for low-value transactions. It is very useful in a financial inclusion context since it enables unbanked individuals to get access to the basic formal services they need, and at the same time reduces the costs of small value accounts and increases financial inclusion outreach for financial institutions.

[66] However, the ability to identify individuals reliably is fundamental not only to financial services, but also to distribution of social welfare support and safeguarding national security, so that where it is lacking authorities should prioritise the development of a national system to identify citizens.

[67] See par. 74.

Countries' experiences in dealing with identification and/or identity verification challenges are outlined in Annex 8.

CDD measures - Identification in non face-to-face scenarios[68]

86. The increasing use of technological innovations is a promising channel to expand the provision of financial services to unserved and remote population[69]. In this regard, mobile phone banking and mobile payments have developed significantly over the last years, and have major potential to facilitate access to basic services for unbanked people, especially in developing countries. According to the World Bank, around three quarters of the world's inhabitants now have access to a mobile phone, and the vast majority of mobile subscriptions (five billion) are in developing countries[70]. In Sub-Saharan Africa, the Gallup World Survey poll indicated that 16% of adults reported having used a mobile phone in the prior 12 months to pay bills or send or receive money[71]. Although mobile banking shows potential for financial inclusion purposes, at this stage, it primarily gives access to payment and transfer services. This functionality offers a useful first step to formal financial services but does not in itself provide the benefits of full banking or other financial services.

87. The development of branchless banking channels through non-bank agents (*e.g.,* petrol stations, lottery kiosks, grocery stores etc.), combined or not with mobile phone solutions, also offers significant potential by which financial services can reach the still unbanked or unserved groups[72].

88. In this context, it is important to understand FATF's requirements involving a non face-to-face relationship. INR. 10 par. 15 of the new FATF Recommendations identifies non-face-to-face business relationships or transactions as examples of potentially higher risk scenarios. The new Recommendations also clarify that examples are given for guidance only, and that the risk factors listed may not apply in all situations (INR. 10 par. 14). In a financial inclusion perspective, the risks of identity fraud have to be balanced with the ML/FT risks of newly banked people on a case-by-case basis to decide if it is appropriate to apply enhanced due diligence measures.

89. As far as identification of lower risk customers at the account opening stage is concerned, financial institutions are requested to apply equally effective procedures as for clients with whom they meet. In a number of cases, although there is no direct face-to-face communication with the financial institution, a third party or an agent is involved in the account opening process. In this case, the principles relevant to agent or third party relationships will apply[73]. In most other cases,

[68] See also FATF (2013b).

[69] See G20 Financial Inclusion Experts Group (2010), Annex 3 and FATF (2013b),

[70] World Bank (2012c)

[71] World Bank (n.d.)

[72] See par. 116 and s.

[73] See par. 93 for third party relationships and par. 116 and s. for agents.

financial institutions require customers to send digital copies of their identification documentation, and the whole range of the account facilities are activated once the verification is completed[74].

90. *New products and technologies.* New FATF Recommendation 15 requires that countries and financial institutions identify and assess the specific risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for existing and new products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies, and they should take appropriate measures to manage and mitigate those risks. The initial, pre-launch risk assessment will be refined and adjusted in light of the experience, as part of the requirement that financial institutions regularly review and adapt their RBA measures (INR. 1.8.).

91. Recommendation 15 is part of the section of the new Recommendations requiring additional CDD measures for specific customers and activities. This does not mean, however, that the use of new technologies to develop innovative distribution channels or products automatically calls for additional CDD measures in all cases. While an additional, particularized risk assessment of the new products business practices is required, the specific type of business relationships and transactions involved, the client target groups, the involvement of intermediaries, the sophistication of the technology used are all factors that must be taken into account in evaluating the risks, and determining the appropriate level of CDD that should be applied[75].

92. In the new technology/business practices/financial inclusion context, it is worth noting that the FATF Recommendations (INR. 10 par.11) allow financial institutions in non-face- to-face scenarios to verify the identity of the customer following the establishment of the business relationship (and not before or during the course of establishing a business relationship) when essential to not interrupt the normal conduct of business and provided that the money laundering risks are effectively managed[76].

93. *Reliance on third parties* - Reliance on CDD undertaken by third parties who are not agents of the financial institutions and are not covered by outsourcing agreements is permitted under the FATF Recommendations, provided that certain requirements are met (Recommendation 17). Third party CDD is not permitted in some countries, but when allowed, the ultimate responsibility for customer identification and verification must remain with the delegating financial institution. In a reliance scenario, a financial institution that is accepting a customer relies on a third party to perform some or all of the following elements of the CDD process (a) identifying the customer (and any beneficial owner), (b) verifying the customer's identity, and (c) gathering information on the purpose and intended nature of the business relationship. This information has to be provided immediately to the financial institution. Financial institutions must satisfy themselves that the third party is adequately subject to AML/CFT regulation and supervision by a competent authority and

[74] See countries' experiences in Annex 7.

[75] See countries' experiences in Annex 7.

[76] See FATF (2013b).

has measures in place to comply with the CDD requirements. New Recommendation 17 clearly limits such reliance on third parties to only other financial institutions (INR 17 par. 3). When they belong to the same financial group, the financial institution and the third party may be considered as meeting some of the required conditions as a result of their group-wide AML/CFT programme. In practice, firms develop measures to check the reliability of the third party (especially in a cross-border context) such as the degree of domestic AML/CFT regulation and supervision.

CDD measures - obtaining information on the purpose and intended nature of the business relationship

94. The RBA would allow financial institutions in appropriate circumstances (i.e., with respect to particular types of customers or services/products) to infer the purpose and nature of the business relationship from the type of account established and transactions conducted, instead of collecting specific information and carrying out specific measures intended to satisfy this obligation (INR 10, par. 21 4th bullet point). This means that if an account is obviously opened to enable a poor migrant to send/receive small value transfers to and from his/her country of origin through a safe, affordable and formal channel, this element of the CDD requirements could be considered fulfilled.

CDD measures – enhanced regime if money laundering or terrorist financing is suspected

95. Under INR. 10.21, simplified CDD measures will not be applicable if there is any suspicion of money laundering, or terrorist financing. Neither are they applicable where specific higher-risk scenarios apply. Institutions designing CDD measures for lower risk products should therefore ensure that their institutional measures and systems require employees and agents to implement normal or enhanced CDD measures where such suspicions may be harboured or where higher-risk scenarios are encountered.

CDD measures - conducting ongoing due diligence and monitoring the business relationship

96. Monitoring refers to manual or electronic scanning of transactions. Scanning uses parameters such as the country of origin or destination of the transaction, the value of the transaction and its nature. Client names and beneficiary names are also scanned against national and international sanctions lists. The scanning process may flag a number of transactions for internal investigation, such as transactions with values that exceed the normal value for that type of transaction. Monitoring and internal investigations require capacity and, depending on the method of monitoring, may be time-consuming and expensive. If an outlier transaction is identified, it must be investigated internally. Additional facts must be gathered and considered. The investigator will typically require more information about the client and the transaction before a reasonable conclusion can be drawn that the transaction is above suspicion or that there are reasonable grounds to suspect that the transaction involves ML/FT.

97. The degree and nature of monitoring by a financial institution will depend on the ML/T risks that the institution faces. In applying an RBA to monitoring, financial institutions and their regulatory supervisors must recognize that not all transactions, accounts or customers will be

monitored in the same way. The degree of monitoring will be based on the identified risks associated with the customer, the products or services being used by the customer and the location of the customer and the transactions. The risks a financial institution is willing to accept, either with respect to the customers it serves or the services it offers, need to be consistent with the resources of the financial institution and its ability to monitor and manage its risks effectively. Technology-based service models often offer greater ease of monitoring, and this should be particularly considered by countries in a financial inclusion context.

98. The principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on each financial institution's analysis of its major risks. Regulatory authorities should, therefore, be mindful of and give due weight to the determinations made by financial institutions, provided that these determinations are consistent with any legislative or regulatory requirements, and informed by a credible risk assessment and the mitigating measures are reasonable and adequately documented.

99. Monitoring under an RBA allows a financial institution to create monetary or other thresholds below which an activity will receive reduced or limited monitoring. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. Financial institutions should also assess the adequacy of any systems and processes on a periodic basis. The results of the monitoring should always be documented[77].

100. Some form of monitoring, whether automated or manual, a review of exception reports or a combination of screening criteria, is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk customers, monitoring is needed to verify that transactions match the initial low risk profile and if not, to trigger a process for appropriately revising the customer's risk rating. Risks for some customers may only become evident once the customer has begun transacting either through an account or otherwise in the relationship with the financial institution. This makes appropriate and reasonable monitoring of customer transactions an essential component of a properly designed RBA. Moreover, where there is an actual suspicion of money laundering or terrorist financing, this should be regarded as a higher risk scenario, and enhanced due diligence should be applied regardless of any threshold or exemption.

101. It is also important to note that lower risk circumstances can be limited to specific aspects of a given relationship (INR. 10 par.18). In this situation, the simplified regime may not be applied uniformly to all CDD steps, and the extent of the CDD measures can be differentiated, depending on the risk factors identified for each of the relationship's stages. For example, in the case of a newly banked client benefiting from simplified identification measures, normal levels of ongoing transaction monitoring may be applied in order to make sure that the account facilities are used appropriately and within the agreed limits.

102. As noted above, in some countries, the choice has been made to mitigate the risk introduced by simplified CDD by closely monitoring transactions linked to the relevant products and accounts. However, if little CDD is undertaken, so that the financial institution lacks a sufficient range of

[77] Wolfsberg (2009)

available information, manual or electronic scanning of transactions may not be able to deliver significant benefit.

CDD measures – the specific case of Politically Exposed Persons (PEPs)

103. Products and services targeted at financial inclusion are not expected to normally involve PEPs as customers or beneficial owners, although in a number of cases, financial institutions have to deal with family members of PEPs. Nevertheless, financial institutions must have appropriate risk-management systems to determine whether a customer or the beneficial owner is a foreign PEP, and reasonable measures to make that determination are required in relation to domestic and international PEPs (Recommendation 12). What constitutes an appropriate risk-management system or reasonable measures to identify foreign PEPs could vary, depending on the risk presented by the customer base.

104. When a foreign PEP is identified as a (potential) customer or beneficial owner, financial institutions must apply enhanced CDD, including obtaining senior management approval for establishing (or continuing, for existing customers) such business relationships; taking reasonable measures to establish the source of wealth and source of funds; and conducting enhanced ongoing monitoring of the business relationship.

105. In addition, financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization, and to apply the enhanced due diligence measures described above on a risk-sensitive basis *i.e.,* in cases of a higher risk business relationship with such persons[78].

CDD measures – the specific case of wire transfers

106. Wire transfers are often used for remittances sent for reasons that are linked to financial inclusion issues. In addition to CDD requirements, they are subject to specific rules relating to the customer/originator and beneficiary to ensure full transparency throughout the payment chain (Recommendation 16). Countries may adopt a *de minimis* threshold (no more than USD/EUR 1 000), below which reduced information requirements can be applied (INR 16).

107. CDD requirements apply to occasional wire transfers in the circumstances covered by INR16 (R10 (ii)). This means that, in countries which have adopted the *de minimis* threshold:

- for occasional cross-border wire transfers below USD/EUR 1 000, the reduced requirements of INR16 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. Such information will not have to be verified (INR. 16 5.a).

[78] See Wolfsberg (2008) and FATF (2013a)

- for occasional cross-border wire transfers above USD/EUR 1 000, the information accompanying the transfer should include the elements listed in INR 16.6. : the name of the originator; the originator account number; the originator's address or national identification number of customer identification number or date and place of birth; the name of the beneficiary; and the beneficiary account number. This information need to be verified.

4.2. RECORD-KEEPING REQUIREMENTS (RECOMMENDATION 11)

108. Under Recommendation 11, financial institutions should maintain records of all domestic and cross-border transactions (including occasional transactions) for at least five years, to enable them to comply swiftly with information requests from the competent authorities. The rationale is to facilitate the reconstruction of individual transactions and provide, if necessary, evidence for the prosecution of criminal activity.

109. Recommendation 11 also states that financial institutions should keep all records of the identification data obtained through the customer due diligence process (*e.g.,* copies or records of official identification documents such as passports, identity cards, driver's licenses and similar documents, account files and business correspondence, including the results of any analysis undertaken such as inquiries to establish the background and purpose of complex and unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction. The record keeping requirement is not dependent on risk levels and it is fully applicable to the CDD, transaction and other information collected, whatever the range of this information (INR. 1 6.).

110. Under the FATF Recommendations, the record keeping requirement does not require retention of a photocopy of the identification document(s) presented for verification purposes; it merely requires that the information on that document be stored and kept for five years. A number of countries, such as the United States, Australia and Canada, have considered, but rejected, imposing photocopying obligations on their regulated institutions for a number of reasons: for example, the photocopies could be used to commit identity fraud; their retention may breach privacy laws and they may reveal information about the client that could form the basis of discriminatory practices, such as the refusal of credit facilities[79].

111. Recommendation 11 therefore allows different forms of document retention, including electronic storage. For example, the following record retention techniques are acceptable:

- Scanning the verification material and maintaining the information electronically;
- Keeping electronic copies of the results of any electronic verification checks;
- Merely recording (hand-writing) reference details on identity or transaction documents. This may be particularly useful in the context of mobile banking,

[79] See other countries' experiences in Annex 8.

since mobile money agents are often basic corner shops. The types of details it is advisable to record include:

- Reference numbers on documents or letters,
- Relevant dates, such as issue, expiry or writing,
- Details of the issuer or writer,
- All identity details recorded on the document.

4.3. SUSPICIOUS TRANSACTIONS REPORTING (RECOMMENDATION 20)

112. The reporting of suspicious transactions or activity is critical to a country's ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. All countries should have legal or regulatory requirements that mandate the reporting of suspicious activities. Once a suspicion has been formed, a report must be made and, therefore, an RBA for the reporting of suspicious activity is not applicable.

113. The RBA is, however, appropriate for the purpose of identifying potentially suspicious activity, for example, by directing additional resources at those areas (customers, services, products, locations etc.) that a financial institution has identified as higher risk. As part of an RBA, it is also likely that a financial institution will utilize information (typologies, alerts, guidance) provided by competent authorities to inform its approach for identifying suspicious activity. A financial institution should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions.

114. FATF Recommendation 20 stipulates that if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing, it should be required to report the incident promptly to the country's Financial Intelligence Unit (FIU). This obligation applies to all financial institutions that are subject to AML/CFT obligations, including those that serve disadvantaged and low income people. The implementation of such a requirement requires financial institutions to put in place appropriate internal monitoring systems to identify any unusual behaviour.

115. In most countries, transactions with vulnerable categories of clients are not deemed to be subject to separate or specific monitoring systems to identify suspicious transactions. However, some businesses may have developed indicators. For example, money transfer businesses[80] would focus on the following, in addition to other criteria, such as systematic monitoring:

- A lack of cooperation at the counter when further questions are asked or suspicious behaviour is detected.
- An identified transaction pattern that is not consistent with the status of a financially excluded individual: *e.g.,* consumers who are sending or receiving large amounts of money are typically less likely to have limited access to ID

[80] Based on the experience of Western Union.

documents (from the country of residency or from the country of origin). This disconnect is a source of potential ML/TF risks.

- Any signal that a consumer is engaged in a TF initiative, whatever the amount of money sent.
- Any signal that a consumer tries to bribe / influence the agent or staff at counter or is producing wrong information and recognizes it.

4.4. THE USE OF AGENTS TO CARRY OUT AML/CFT FUNCTIONS

116. *General.* The use of non-bank agents to distribute financial services is part of an increasingly popular model for financial inclusion in many countries. Most of the countries that contributed to this Guidance paper have developed some forms of agent banking options, some of which are referred to as branchless banking, or banking beyond branches. In these countries, banking and payment services are provided through channels such as post offices, mobile phones and small retail outlets, like airtime sellers, groceries, bakeries, etc., with the goal of providing a broader and cheaper access to financial services than the bank branch-based model. The development of these networks of non-bank agents also offers considerable potential to fill the physical distance gap that appears to be one of the major obstacles to financial inclusion[81]. Brazil has developed such a network so that all 5 564 municipalities in the country now have a banking access point, with 25% of the municipalities served only by such mechanisms [82].

Definitions and scope

117. *General.* Customer identification and verification obligations are normally predicated on the basis that these functions are carried out by the officers or employees of the financial institution. However, depending on the jurisdiction, and having regard to the diversity of the financial sectors, there may be occasions when these functions are permitted or are in practice performed by agents[83].

118. *Notion of agent[84].* Although the business models and the terminology may vary significantly from country to country, it is understood that the agent, in any kind of branchless banking model and most mobile money businesses models, works on behalf of a financial institution (INR 17.1.)[85]. The latter has the business relationship with the customer and is accountable for it. The financial institution grants authority for another party, the agent, to act on behalf of and under its control to deal with a client/potential client. For instance, in the mobile money business, the agent can be working on behalf of a mobile network operator who has the license to issue e-money. So the

[81] See par. 22.

[82] www.ifmr.co.in/blog/2010/07/28/correspondent-banking-in-brazil/

[83] See par. 93 for the specific case of the CDD process being undertaken by a third party.

[84] The specific case of Money and Value Transfer Services agents covered by Recommendation 14 is dealt with as part of par. 134 and s.

[85] This can include other account providers such as mobile network operators or payment services providers, see World Bank (2011).

customers tend to view the retailer/agent as a point of access and as a representative of the operator. An agreement creating this relationship may be express or implied, and both the agent and the financial institution may be either an individual or an entity, such as a corporation or partnership.

119. In these branchless banking and mobile money business models, agents are viewed by the FATF as simply an extension of the financial services provider, and consequently, the conduct of CDD by these agents is treated as if conducted by the principal financial institution. The customers themselves generally view the retailer as a point of access and as a representative of the principal financial institution.

120. *Who can be an agent?* Many countries permit a wide range of individuals and legal persons or other entities to be agents for financial institutions. Other countries restrict the list of legally eligible agents[86]. For example, India permits a wide variety of eligible agents, such as certain non-profits, post offices, retired teachers, and most recently, for-profit companies, including mobile network operators. Kenya requires agents to be for-profit actors and disallows non-profit entities. Brazil permits any legal entity to act as an agent, but prevents individuals from doing so. This range of approaches reflects that countries have different regulatory concerns that balance agent eligibility requirements from an AML/CFT perspective with financial inclusion objectives. In some countries the list of eligible agents may be very extensive but under-used by the financial institutions, in which case, countries may wish to explore the reasons underlying the reluctance to engage agents[87].

121. The principle that the financial institution is ultimately liable for compliance with the AML/CFT requirements is required by the FATF Recommendations, and is almost universal amongst jurisdictions, although the extent of liability may differ from one country to another.

122. Finally, countries have adopted different practices regarding licensing or registration of agents and service providers. In Kenya, mobile phone operators are licensed by the communications sector regulator with respect to their provision of traditional communications services but they operate under the oversight of the Central Bank in relation to the provision of any mobile financial services.

AML/CFT functions of the agent and related challenges

123. The fact that agents act as an extension of the principal financial institution means that the processes and documentation, for AML/CFT purposes, are those of the principal financial institution. The main role and duties and how agents have to perform those duties will be determined by the principal financial institution. In this regard, it is essential that these duties are clearly specified in

[86] See CGAP (2011).

[87] CGAP reports that some countries may also restrict the location of agents. For instance, Indian regulators initially required agents to be located within 15 kilometers of a "base branch" of the appointing bank in rural areas, and within 5 kilometers in urban areas. This policy, intended to ensure adequate bank supervision of its agents, limited the use of agents by banks with only a few branches. Consequently, regulators have since expanded the distance to 30 kilometers, and banks can seek exemption from this requirement in areas with underserved populations where a branch would not be viable.

the agency agreement that sets the terms by which the retailer is appointed as an agent of the principal financial institution. In practice, the contracts between the principal financial institution and their agents vary considerably across countries and markets but common clauses generally include the duty to perform specified AML/CFT checks, record-keeping and reporting obligations.

124. In determining the AML/CFT role and duties of the agents, it is crucial that financial institutions and regulators take into account the potential practical limitations faced by retailers acting as agents (often small shops). Retailers generally have only partial knowledge of the transactions conducted by the customer (i.e. the transaction conducted in their particular shops). AML/CFT functions of the principal financial institution and its agents should be seen as complementary and inclusive, keeping in mind that the principal financial institution bears ultimate responsibility for compliance with all applicable AML/CFT requirements.

125. Although the precise role of a retailer agent may differ from business model to model, it generally involves providing cash-in and cash-out services. It may also extend to other customer interface functions such as account opening and customer care. Most regulations permit agents to process cash-in and cash-out transactions.

126. Many countries permit agents to conduct CDD, and agents routinely verify customer identity. In other countries, agents' ability to conduct CDD measures is limited to certain lower risk financial products. The challenges related to the identification of the customer and verification of the identity (as described in section 4.1) will therefore greatly vary from country to country.

127. As indicated above, the FATF requires financial institutions to have appropriate systems and controls to monitor transactions, and report to the FIU any transaction or activity that could be suspected to be related to money laundering or terrorism financing. This monitoring requirement may require some adjustments in principal-agent duties although the models developed across FATF jurisdictions seem very similar.

128. Under Mexico's AML/CFT legal framework for instance, financial institutions are required to establish systems and mechanisms that allow them to receive online all transactions made through an agent, in the same way as those carried out in banking offices. Financial institutions must monitor the operations carried out by the agent and report to the FIU all cases where there is a suspicion of money laundering or terrorism financing. In addition, financial institutions must have automated systems that allow them to monitor client transactions and detect possible unjustified deviations in the client –transactional profile to enable the institution's Communication and Control Committee (consisting of high ranking employees) to analyse them and if appropriate, report them to the FIU. Similar arrangements exist in Malaysia and South Africa. In the Philippines, both principal and agents are covered institutions and are thus required to adhere to AML/CFT laws and regulations on monitoring and reporting suspicious transactions. Principals and agents submit reports (including suspicious transactions reports) to the FIU, separately and independently from each other.

Internal controls applicable to agents

129. As part of the AML/CFT obligations, financial institutions are required to develop internal control programmes against money laundering and terrorist financing (Recommendation 18). The type and extent of measures to be taken for each of the requirements under Recommendation 18 should be appropriate in light of the risk of money laundering and terrorist financing and the size of the business.

130. These programmes generally should include: (1) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees; (2) an ongoing employee training programme; (3) an audit function to test the system. Such internal controls are applicable to agents. They may also be adapted to branchless banking scenarios, in which case agent screening and agent training would be crucial[88].

Oversight of agents

131. Since agents are viewed by FATF as an extension of the principal financial institution[89], it is appropriate for regulatory supervision and oversight to focus primarily on the principal financial institution. Monitoring and supervising thousands of agents would be extremely challenging for most, if not all, countries[90]. The oversight of agents is mainly performed by the principal financial institution, in a similar manner as it monitors employees (see Recommendation 18). It is nevertheless also essential that the regulatory supervisor reviews financial institutions' oversight functions, including by examining the policies, procedures, training and monitoring of agents put in place by the principal financial institutions.

132. Agent monitoring is a very important element in an effective AML/CFT program. While all financial institutions should conduct baseline monitoring of agents to assess and address systemic risks such as inadequate training, new or changing services or products, and poor individual judgment or performance, the application of a risk-based approach will require a higher level of monitoring where there are indications that some agents knowingly or through wilful blindness act in a way that may conceal their customers conduct from the institution's routine transaction monitoring. The degree and nature of agent monitoring will depend on factors such as the transaction volume and values handled by the agent, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to agent monitoring, the degree of monitoring will be based on the identified risks, both external and internal, associated with the agent, such as the products or services provided by the agent, and the agent's location.

---

[88] See par. 140 and s.

[89] Or the principal financial institution**s** in case the agent works with several of them (in a few markets, agents exclusivity for a single Mobile Network Operator is not permitted).

[90] CGAP (2011a).

133. In some countries, agents can act on behalf of multiple principal financial institutions. A particular business such as a convenience store can be an agent for more than one financial institution such as one or more money remitter(s) and one or more retail banks(s), micro lender(s), or micro insurer(s). If the different principal financial institutions do not exercise the same level of monitoring of the agent (or they are not subjected to the same level of oversight in so far as their agent monitoring is concerned), it could lead to arbitrage between the products and services of the different principal financial institutions that can be accessed through the agent. It is therefore important that homogeneous requirements apply to the different financial institutions providing services to low-income clients.

Specific requirements for agents of Money and Transfer Value Service providers[91] (Recommendation 14)

134. Requirements for money or transfer value providers (MVTS) have obvious implications for financial inclusion. For example, poor migrant workers often rely on MVTS providers to send remittances home. Under Recommendation 14, countries should take measures to ensure that natural or legal persons that provide MVTS are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant ML/CFT obligations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

135. The FATF makes explicit reference to the notion of "agent" in the context of Recommendation 14[92]. In relation to this Recommendation, the Glossary defines an agent as "*any natural or legal person providing money or value transfer service on behalf of an MVTS provider, by contract with or under the direction of the MVTS provider.*" As stated earlier, the FATF views that the agent is an extension of the financial institution, with the information and documents held by that agent being immediately available to the institution, and the agent being subject to the control of the institution through their contract.

136. Recommendation 14 requires that any natural or legal person working as an agent of an MVTS provider is either licensed or registered by a competent authority, or alternatively, the MVTS provider (the principal) is required to maintain an updated list of agents which must be made accessible to the designated competent authorities in the countries in which the MVTS provider and its agents operate, when requested. It is important to flag that this requirement on agents only exists in the context of money and value transfer services – and not for other types of financial services covered by the FATF Recommendations.

[91] As defined in the Glossary to the FATF Recommendations, the term "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."

[92] And indirectly in Recommendation 16 on Wire Transfers.

137. Countries have adopted different practices regarding licensing, registration, or listing of agents of MVTS[93]. For example, South Africa, Uganda, and Mongolia require agents to obtain a license. Mexico, Guatemala, and Malaysia require agents to register with a designated competent authority. Where countries require MVTS providers to maintain a list of agents, two approaches have been observed:

1) listing for approval: the MVTS provider must compile a list of agents and obtain approval for them from the designated competent authority. This approach is close to a registration or licensing requirement, and has been adopted by the UK, Jamaica, Nepal, Indonesia, Malawi and Afghanistan.

2) listing for information: the MVTS provider is simply required to maintain a current list of agents and have it available for the designated competent authority when requested. Honduras and the US employ this approach.

138. Recommendation 14 does not require the principal and agent to be in the same jurisdiction. It allows for the possibility that agent in country A could be listed by its principal in country B – provided that authorities in country A and B can obtain the list and the agent follows the AML/CFT requirements applicable to the principal. However, in many countries, if an MVTS agent is operating in a different jurisdiction from where its principal is licensed or registered, the agent is likely to be considered an MVTS[94] provider itself in the jurisdiction in which it is operating, and would have to be licensed or registered itself.

139. Finally, INR. 16 par.22 requires MVTS providers to comply with requirements on wire transfers, regardless of whether conducting transactions directly or through their agents.

4.5. INTERNAL CONTROLS

140. The FATF Recommendations require financial institutions to develop programmes against money laundering and terrorist financing although with some degrees of flexibility considering the ML/TF risk and size of the business (INR. 18). Using this flexibility is crucial, especially for businesses intended to serve the financially excluded or underserved. AML/CFT programmes must include: (i) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees; (ii) an ongoing employee training programme and (iii) an audit function to test the system. Financial institutions must therefore develop an effective internal control structure, including suspicious activity monitoring and reporting and create a culture of compliance, ensuring that staff adheres to the financial institution's policies, procedures and processes designed to limit and control risks. In addition to complying with the requirements of the country in which they are operating, financial institutions should also ensure that their foreign branches and

[93] See Todoroki, E., *et. al.*(forthcoming).

[94] As defined in the Glossary to the FATF Recommendations, the term "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."

subsidiaries comply with the home country AML/CFT requirements. The new Recommendation 18 introduces the requirement that financial groups should have group-wide AML/CFT programmes that include policies on information sharing within the group.

141. The FATF acknowledges that the nature and extent of AML/CFT controls will depend upon a number of factors, including:

- The nature, scale and complexity of a financial institution's business.
- The diversity of a financial institution's operations, including geographical diversity.
- The financial institution's customer, product and activity profile.
- The distribution channels used.
- The volume and size of the transactions.
- The degree of risk associated with each area of the financial institution's operation.
- The extent to which the financial institution is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non-face to face access.

142. The FATF considers that the framework of internal controls should include (the list is not exhaustive):

- Providing increased focus on a financial institution's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.
- Providing for regular review of the risk assessment and management processes, taking into account the environment within which the financial institution operates and the activity in its market place.
- Designate an individual or individuals at management level responsible for managing AML/CFT compliance.
- Provide for an AML/CFT compliance function and review programme.
- Ensuring that adequate controls are in place before new products are offered.
- Implementing risk-based customer due diligence policies, procedures and processes
- Providing for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
- Enabling the timely identification of reportable transactions and ensure accurate filing of required reports.

- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- Providing for appropriate training to be given to all relevant staff.

4.6. OTHER RELEVANT ISSUES

143. Building up an appropriate and balanced AML/CFT regime based on domestic circumstances requires extensive coordination among competent authorities and between public authorities and the private sector. Effective information exchange between the public and private sectors will form an integral part of a country's strategy for combating money laundering and terrorist financing while promoting financial inclusion. To be productive, information exchange between the public and private sector should be accompanied by appropriate exchanges among public authorities. FIUs, financial supervisors and law enforcement agencies should be able to share information and feedback on results and identified vulnerabilities, so that consistent and meaningful inputs can be provided to the private sector.

144. In this regard, the FATF Recommendations promote domestic cooperation mechanisms (Recommendation 2) and encourage public authorities to assist the private sector in adopting adequate and effective AML/CFT measures (Recommendation 34). These principles should guide countries' efforts to implement an effective AML/CFT regime while working towards greater financial inclusion[95].

145. Lastly, the FATF supports increased cooperation among the private sector, and in particular the building of partnerships between different service providers, aimed at delivering innovative financial products that promote financial inclusion. Mobile-based payment services as well as remittance-linked products that promote the replacement of cash payments by bank accounts, payment accounts or stored-value products constitute examples of innovative products that can effectively promote financial inclusion. The FATF acknowledges the importance of promoting the exchange of experience at an international level, in order to help identify best transferrable practices across FATF countries and beyond.

[95] A sample of countries' experiences is provided in Annex 9.

CONCLUSION

146. The FATF acknowledges the importance of financial inclusion and its relevance to the work of the FATF. This Guidance recognises that financial inclusion and AML/CFT are complementary objectives. It provides an important tool to improve guidance to countries, regulators, and supervisors that wish to translate financial inclusion's objectives into real progress on the ground. It believes that the reinforcement of the risk-based approach as a central principle of all AML/CFT regimes will be a key tool to support the development of tailored to–risk-based approach that are available in the AML/CFT Standards.

147. The FATF will continue to work to ensure that financial inclusion and AML/CFT objectives mutually support each other. In that respect, this initiative should not be a one-off effort. The FATF will keep financial inclusion issues in mind as it addresses such issues as the potential lower risks of financial products or services that contribute to increase access to financial services or when reviewing any new financial delivery channel, or business model that can contribute to serve the financially excluded or underserved groups.

148. FATF encourages FATF members, FSRBs and other FATF observers to promote the guidelines provided in this document in order to make sure that throughout the FATF network, balanced AML/CFT regime are developed which protect the integrity of the financial system, while at the same time support and facilitate financial inclusion.

ANNEXES

Countries' experiences are presented for information only. Most of them have not been assessed against the FATF Recommendations, and their presentation can therefore not amount to an endorsement by FATF.

ANNEX 1: MEMBERSHIP OF THE PROJECT GROUP

FATF MEMBERS/OBSERVERS

Australia, India, Italy, Mexico, New-Zealand, South Africa, Switzerland, the United States, the World Bank, ESAAMLG (Kenya), GAFISUD (Peru), GIABA.

APG MEMBERS

The Philippines, Malaysia, Pakistan.

OTHER ORGANISATIONS

Alliance for Financial Inclusion (AFI), Consultative Group to Assist the Poor (CGAP), G20/GPFI.

PRIVATE SECTOR PARTICIPANTS

World Savings Banks Institute/European Savings Banks Group (WSBI/ESBG), World Council of Credit Unions, GSM Association (GSMA), International association of Money transfer networks, International Banking Federation (IBFed), The Money Services Round Table, The Western Union Company, Vodafone Group Services Limited, Russian E-Money association, Lotus Group Ent. Sdn. Bhd, Money Express, Globe Telecom, Banco de Credito BCP (Peru). Barclays Bank (Kenya), Co-op Bank (Kenya), Equity Bank (Kenya), KCB (Kenya), SMJ Teratai Sdn Bhd.

PRIVATE SECTOR OBSERVERS

International Cooperative Banking Association, Orange France Telecom Group, American Express Company, European Microfinance Platform (e-MFP), Placid Express Sdn. Bhd, Prabhu Money Transfer Sdn. Bhd, Mobile money, Arias, Wizzit Bank.

OTHERS

Professor Louis De Koker, School of Law, Faculty of Business and Law, Deakin University, Australia; Universal Postal Union; Bill & Melinda Gates Foundation; UN Secretary General's Special Advocate for Inclusive Finance for Development.

ANNEX 2: G20 PRINCIPLES FOR INNOVATIVE FINANCIAL INCLUSION AND ACTUAL RELEVANCE TO THE FATF

1. PRESENTATION OF THE G20 PRINCIPLES FOR INNOVATIVE FINANCIAL INCLUSION[96]

Innovative financial inclusion means improving access to financial services for poor people through the safe and sound spread of new approaches. The following principles aim to help create an enabling policy and regulatory environment for innovative financial inclusion. The enabling environment will critically determine the speed at which the financial services access gap will close for the more than two billion people currently excluded. These principles for innovative financial inclusion derive from the experiences and lessons learned from policymakers throughout the world, especially leaders from developing countries.

1. **Leadership**: Cultivate a broad-based government commitment to financial inclusion to help alleviate poverty.
2. **Diversity**: Implement policy approaches that promote competition and provide market-based incentives for delivery of sustainable financial access and usage of a broad range of affordable services (savings, credit, payments and transfers, insurance) as well as a diversity of service providers.
3. **Innovation**: Promote technological and institutional innovation as a means to expand financial system access and usage, including by addressing infrastructure weaknesses.
4. **Protection**: Encourage a comprehensive approach to consumer protection that recognises the roles of government, providers and consumers.
5. **Empowerment**: Develop financial literacy and financial capability.
6. **Cooperation**: Create an institutional environment with clear lines of accountability and co-ordination within government; and also encourage partnerships and direct consultation across government, business and other stakeholders.
7. **Knowledge**: Utilize improved data to make evidence based policy, measure progress, and consider an incremental "test and learn" approach acceptable to both regulator and service provider.
8. **Proportionality**: Build a policy and regulatory framework that is proportionate with the risks and benefits involved in such innovative products and services and is based on an understanding of the gaps and barriers in existing regulation.
9. **Framework**: Consider the following in the regulatory framework, reflecting international standards, national circumstances and support for a competitive landscape: an appropriate,

[96] www.g20.utoronto.ca/2010/to-principles.html

flexible, risk-based Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime; conditions for the use of agents as a customer interface; a clear regulatory regime for electronically stored value; and market-based incentives to achieve the long-term goal of broad interoperability and interconnection.

These principles are a reflection of the conditions conducive to spurring innovation for financial inclusion while protecting financial stability and consumers. They are not a rigid set of requirements but are designed to help guide policymakers in the decision making process. They are flexible enough so they can be adapted to different country contexts.

2. RELEVANCE TO THE FATF

There are two principles that are directly related to the FATF: (1) the principle of framework and (2) the principle of proportionality. In addition to these principles, a number of the other principles also have a bearing on the FATF's work. The principle of innovation, for example, requires the promotion of technological and institutional innovation as a means to expand financial system access and usage. This principle is relevant to the application of the FATF framework to new payment methodologies that are vehicles for greater financial inclusion.

ANNEX 3: EXAMPLES OF COUNTRIES' ACTIONS TO SUPPORT FINANCIAL INCLUSION

Countries may develop strategies that aim at enhancing the access, inclusiveness, stability and efficiency of the financial sector. Examples of actions taken to support financial inclusion are provided below:

Stakeholder	Examples of actions to support financial inclusion
Government	■ Becoming a signatory of the June 2012 G20 Los Cabos Declaration on Financial Inclusion, and committing to the G20 Financial Inclusion Peer Learning Programme[97] ■ Include financial inclusion as part of the broader financial sector strategy ■ Develop a market based approach to financial sector development ■ Various regulatory reforms and initiatives that reflect a proportionate approach, including development of legislation to regulate micro-finance, credit unions and e-money and payments ■ Provide greater operational independence for regulators ■ Create space for innovation and stakeholder feedback ■ Support financial education initiatives and consumer protection efforts ■ Conduct the development of relevant and efficient banking and market infrastructure ■ Promote initiatives to gather further information regarding current levels of financial inclusion and barriers to the supply of financial services ■ Implement changes to the distribution of government subsidies in order to promote electronic transfers and financial inclusion
Regulators	■ Proportionate risk-based regulation and supervision of banks and non- financial institutions to ensure the stability of the system and the safety of public deposits, while simultaneously promoting development of products and services appropriate for the

[97] The June 2012 "Los Cabos Declaration on Financial Inclusion" presents the G20 Financial Inclusion Peer Learning Program through which countries commit to setting up a national coordination platform, and strategies for financial inclusion. 17 countries already committed to this initiative. See http://www.g20mexico.org/index.php/en/press-releases/459-evento-de-inclusion-financiera-en-los-cabos.

Stakeholder	Examples of actions to support financial inclusion
	underserved population ■ Ongoing development of capacity to regulate micro-finance activities ■ Create space for stakeholder consultation and feedback and provide regulatory guidance in these areas ■ Support market players' efforts to innovate with a view to extend their outreach – this includes direct engagement with entities outside the traditional financial services industry
Banks, credit unions, micro-finance and other financial institutions	■ Rapid extension of delivery channels ■ Innovation in products, channels and processes in partnership with others, such as mobile phone operators ■ Active participation in discussions on regulatory changes, especially for micro-finance and credit unions

ANNEX 4: EXAMPLES OF GOVERNMENT-TO-PERSONS PAYMENT PROGRAMMES TO SUPPORT FINANCIAL INCLUSION

- In 2011, **Fiji** transferred the payment method of its social welfare benefits from a manual voucher system to an electronic payment system where monthly welfare payments are deposited directly into beneficiaries' bank accounts[98]. Under the old voucher system, recipients had to cash their monthly cash vouchers at their nearest post office and in some cases spent 30%-50% of their benefit on travelling costs to the nearest post office. As a result of the transfer in the welfare payment method, some 22,000 welfare beneficiaries who previously did not have access to the formal banking sector, were able to open bank accounts and access their funds conveniently through nearby ATMs and use their funds via over 800 EFTPOS (Electronic Fund Transfers at Point of Sale) merchants.

- In the **United States**, the federal government is taking additional steps to encourage benefit recipients to accept payments through direct deposit into a federally-insured deposit account. The use of checks is being discontinued and being transitioned to the use of pre-paid cards for those who do not have standard bank accounts, with the goal of simplifying and streamlining the delivery system and simultaneously offering greater protection and security for recipients.

These changes provide public authorities with an opportunity for educating recipients about the benefits of more traditional financial products and services.

- The **Mexican** Federal Government has worked to implement mechanisms to pay social subsidies through electronic transfers. For example, the coverage of the anti-poverty "*Oportunidades*" Program was 35% (2.3 million users) as of December 2010. Two mechanisms have been put in place to pay subsidies: 1) for areas with banking infrastructure, the government transfers resources to a banking account; 2) For areas without banking infrastructure, the government transfers resources to a prepaid card and install Points of Sale in the governmental convenience stores located in these areas[99]. As a result, 4.2 million households benefited from the programme.

[98] http://www.uncdf.org/sites/default/files/Download/PFIP_G2P.pdf

[99] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628874

ANNEX 5: PRODUCTS AND SERVICES THAT TARGET THE FINANCIALLY EXCLUDED AND UNDERSERVED GROUPS

I. TYPES OF SERVICES OFFERED TO THE FINANCIALLY EXCLUDED AND UNDERSERVED GROUPS BY TYPE OF INSTITUTIONS AND DELIVERY MECHANISMS

Service	Institutions	Delivery mechanism
Savings	Banks, Postal Banks, Financial Cooperatives Savings Institutions	In branch Agency Electronic communication
Credit	Banks Micro Finance institutions Financial Cooperatives	In branch Agency
Payment services	Banks Financial Cooperatives Mobile Network Operators and other e-money issuers (and distributors) and payment service providers	Electronic communication
Remittance	Banks Remittance companies Financial Cooperatives Mobile Network Operators and other e-money issuers (and distributors) and payment service providers	In branch Agency Electronic communication
Currency exchange	Banks Money Exchange Businesses Remittance companies	In branch Agency
Cheque cashing	Banks Money services Businesses Financial Cooperatives	In branch Agency
Issuance and/or cashing of traveller's cheques and money orders	Banks Postal Banks Money services Businesses Money Exchange Businesses Financial Cooperatives	In branch Agency
Issuance of stored value products	Banks Mobile Network Operators and other licensed e-money issuers	In branch Agency Electronic communication
Micro insurance	Insurance Companies Micro finance institutions	In branch Agency

	Financial Cooperatives	Electronic communication

II. EXAMPLES OF PRODUCTS OFFERED TO FINANCIAL EXCLUDED AND UNDERSERVED GROUPS

Countries' experiences are presented for information only. Most of them have not been assessed against the FATF Recommendations, and their presentation can therefore not amount to an endorsement by FATF.

Example 1 – products launched to serve the financially excluded and underserved groups in India

Description of the product and financial facilities	Amount/threshold limitation	Customer identification requirements
Savings bank product "small account" that would be opened only in banks to enable financial inclusion	i) the aggregate of all credits in a financial year does not exceed INR 100 000 (equivalent to USD 2 000) **+** ii) the aggregate of all withdrawals and transfers in a month does not exceed INR 10 000 (equivalent to USD 200) **+** iii) the balance at any point of time does not exceed INR 50 000 (equivalent to USD 1 000) Such accounts should be opened only in CBS branches (that is computerized bank servers) to ensure that the limits prescribed are not breached No foreign remittance can be credited to these accounts, and Full customer due diligence to be carried out in case of suspicion of ML/TF.	An individual desirous of opening a "small account" should affix his/her signature or thumb print and produce a self-attested photograph and the designated officer of the bank has to affix his/her signature to indicate that the person opening the bank account and the person as per the photograph are one and the same person, and certify that he/she witnessed the customer affix his/her signature or thumb print. Within 12 months of opening the bank account the account holder has to produce a document to indicate that he/she has already applied for an officially valid document (Passport, Voter's Identity Card, Driving Licence or Income Tax PAN card). Only on production of such a document the bank would allow him/her to continue the account for further 12 months. Therefore, within 24 months of opening small account, the account holder has to produce an officially valid document (Passport, Voter's Identity Card, Driving Licence or Income Tax PAN card), which is the requirement for opening any bank account in India. Therefore, at the initial stage of opening the bank account the person is identified by the designated officer of the bank and then within a specified time period the identification is supported by an official document.

Insurance products

The Government of India constituted in 2003 a consultative group to examine insurance schemes for rural and urban poor with specific reference to reach, pricing, products, servicing and promotion, to examine existing regulations with a view to promote micro insurance organizations, to develop sources of support for micro finance organizations, etc.,

It was decided that it would be more appropriate to have a partnership between an insurer and a social organization like NGO which is already working among the targeted sections to drive micro insurance.

Insurance Regulatory and Development Authority (IRDA) notified Micro Insurance Regulations on 10th November 2005 with features to promote and regulate micro insurance products. The regulations focus on the direction, design and delivery of the products.

In order to be able to meet the requirements of financial inclusion and the AML/CFT requirements, and considering the hardship in complying with the KYC requirement by small value policy holders and possible implications for spread of insurance into rural and low income sectors, especially micro-insurance, the IRDA has provided exemption up to a total annual premium of INR 10 000/- (USD 200) on life insurance policies held by a single individual from the requirement of recent photograph and proof of residence.

In addition to the above, Central and State Governments float various social security schemes extending comprehensive insurance coverage to economically weaker sections/below poverty line unemployed youth of rural and urban areas. Such schemes are generally administered by the Public Sector insurance companies. Typically, major part of premium funding is done by the Central/State Governments.

Example 2 – products launched to serve the financially excluded and underserved groups in Mexico – low risk bank accounts

Regarding the design and implementation of low risk financial products to enhance the levels of financial inclusion authorities have identified risks, based on an assessment of products characteristics and considering their potential vulnerabilities. Based on an evaluation of the latter, coupled with relevant economic and market factors specific to Mexico, which included household income levels´ official subsidies provided by the government to the low income sector, as well as average narcos payroll, adequate thresholds for caps on deposits for low-risk accounts were determined. The resulting thresholds allow low income households to satisfy their basic transactional needs. In parallel, consideration was given as to whether such products could be misused for illicit activities, and a number of additional controls were implemented to mitigate ML/TF risks. In this respect, financial authorities in Mexico identified a significant number of cases where prepaid cards bought in Mexico were then sent for use abroad so as to avoid customs´ cross border cash control system. Furthermore, the authorities also identified wire transfers to accounts

related to drug cartels. As part of this assessment, the authorities took into consideration the typologies provided by FATF for new payment methods[100].

From the above, it was decided to establish updated controls and stricter threshold limits for low risk products, on an increasing basis according to the risk assessment.

Authorities involved in the risk assessment (financial regulators and supervisors), included the Financial Intelligence Unit of the Ministry of Finance and Public Credit and the Central Bank of Mexico.

In 2011, the Ministry of Finance launched a legal reform of the AML/CFT framework in order to include a special regime, with simplified KYC and CDD requirements, for specific banking services, which nature and characteristics represent low risks and lower risks for undertaking money laundering operations.

Based on the above mentioned approach, Mexico implemented a system that divides bank accounts into four levels.

The first level is very restricted. According to Mexico's analysis, there is a proven low risk of money laundering and terrorist financing. An exemption from Recommendation 10 (Costumer Due Diligence), has been applied, pursuant to paragraph 6, a) of the Interpretative Note to Recommendation 1.

The following levels (two, three) have been designed based on the Risk Based Approach principle with simplified Costumer Due Diligence requirements according to the account and customer characteristics (natural or legal person, transactions amounts, transactional restrictions), in accordance to Recommendation 1 and the Interpretative Note to Recommendation 10, paragraphs 16, 17, 18 and 21.

All accounts are monitored and banks have to keep records for at least 10 years. If customer transactions exceed the level threshold, banks must set a higher level and meet the identification requirements that apply.

Description of the product and financial facilities (including whether there is banking arrangement)	Amount/threshold limitation	Customer identification requirements
LEVEL 1 Low risk account that may allow none face to face opening process, but subject to monitoring from financial entities and	Limited to a maximum deposit amount of 750 UDIS[101] per month	Customer identification and ID verification could be exempted – Banks can decide

[100] FATF (2010).

[101] The Mexican Investment Unit (UDI) is a unit of value calculated by the Central Bank of Mexico, which is adjusted on a daily basis to maintain purchasing power of money taking into consideration the changes on the inflationary indicator INPC (Mexican Consumer Price Index). Therefore, any financial and commercial transaction referenced to UDIS is updated automatically.

Description of the product and financial facilities (including whether there is banking arrangement)	Amount/threshold limitation	Customer identification requirements
to enhanced supervision of the financial authorities. Main characteristics: • Restricted use for payment of services and/or products • Maximum amount per transaction established by financial institutions • Only one account per person • Not linked to a mobile phone account (for funds transfers) • Valid only in Mexico • Contracted at banking branches, banking agents, by phone or at the banking institution website • No transfer funds to other accounts or products • Able to receive international funds transfers (not from high-risk and non-cooperative jurisdictions and countries sanctioned by the UN) • Strategic monitoring • If suspicious acts are detected (*e.g.,* when there are several transactions in a short period of time, with the same ATM) financial institutions must send a report to the Financial Intelligence Unit. Also, financial institutions will be able to cancel accounts or block transactions resulting from suspicious acts • Electronic transaction records are retained and made accessible to Law Enforcement Agency upon request. • Managed only by banks.	(around USD 250) per month. Low-value transactions Limited to a non-cumulative maximum balance of 1 000 UDIS (around USD 350)	whether or not to apply the procedure, according to their policies, measures and internal processes.
LEVEL 2 • Lower risk account • Only for natural persons. (no Political Exposed Persons) • Maximum amount per transaction established by financial institutions	Limited to a maximum deposit amount of 3 000 UDIS (around USD 1 050) per month. In the case of	Electronic file requires to include only basic client's data (name, place and date of birth and gender and address). No hard copies

Description of the product and financial facilities (including whether there is banking arrangement)	Amount/threshold limitation	Customer identification requirements
• Managed only by banks • Able to receive international fund transfers (not from high-risk and non-cooperative jurisdictions and countries sanctioned by the UN) • Filing requirements are obtained from basic data of the client and account opening can be outsourced • Two schemes: a) Contracted directly at banking branches and banking agents. b) On a non-face to face scheme, by phone or at the banking institution website, subject to a further ID verification and monitoring by financial entities. The supervisor authority, with opinion from the Ministry of Finance, may authorize processes to validate the data. • May be linked to a mobile phone account. • Financial institutions should validate that the data provided by the client matches with the information of the National Population Registry using an Official Unique ID Code (CURP). The CURP is a countrywide registry that comprises all the inhabitants of Mexico (both foreigners and nationals) as well as Mexicans living abroad • On a non-face to face scheme by phone, financial entities should validate the CURP with the cell phone number. • Electronic transaction records are retained and made accessible to Law Enforcement Agency upon request • May be used for funds transfers	government support funds, the previous limit will increase up to 6 000 UDIS (around USD 2 100)	required. In case of a), the banking institution must obtain complete data of the name, birth date and address, from the customer official ID.
LEVEL 3 • For natural or legal persons	Limited to 10 000 UDIS (around USD 3 500 a	Full data is required (copies are not required)

Description of the product and financial facilities (including whether there is banking arrangement)	Amount/threshold limitation	Customer identification requirements
• Fund transfers are allowed • Accounts opening should be at banking branches or through banking agents	month)	

Example 3 – product launched to serve the financially excluded and underserved groups in South Africa – basic bank accounts

Description of the product and financial facilities (including whether there is banking arrangement)	Amount/threshold limitation	Customer identification requirements
A conditional exemption from some of the identification and verification elements of the relevant anti-money laundering legislation was made to provide for a form of simplified due diligence (Exemption 17). The exemption applies only to: banks, mutual banks, the Postbank, Ithala Development Finance Corporation Ltd and to money remitters (in respect of transactions where both the sending and receiving of funds takes place in South Africa). The products launched under this exemption take on a number of different forms, the most common example being the Mzansi account. This is an inter-operable account which is offered and recognised by a number of different participating banks. Another example is cell-phone banking product offered by a South African bank which allows for the account opening process to be initiated with the use of a cellular phone. The account opening process is completed with an agent of the bank visiting the customer and completing the identification and verification process in a face-to-face meeting. The bank does not operate	A person holding such an account is not able to withdraw or transfer or make payments of an amount exceeding ZAR 5000 (approximately EUR 500, USD 650) per day or exceeding ZAR 25 000 (approximately EUR 2 500, USD 3 270) in a monthly cycle. The balance maintained in the account must not exceed ZAR 25000 (approximately EUR 2500, USD 3 270) at any time. This type of account does not allow the customer to effect a transfer of funds to any destination outside South Africa, except for a transfer as a result of a point of sale payment or a cash withdrawal in a country in the Rand Common Monetary Area (South Africa, Lesotho, Namibia	This product is only available to a natural person; the customer must be a South African citizen or resident. Need to verify the identity information of a customer, that is, the customer's full name, date of birth and identity number-this is verified against a national identity document. There is no need for the verification of residential address- many of the unbanked live in informal settlements where there are no means to confirm physical addresses.

branches of its own and accessing bank accounts and conducting transactions are done by means of a cellular telephone.	and Swaziland). The same person must not simultaneously hold two or more accounts which meet the Exemption 17 criteria with the same institution.	

Example 4 – product launched to serve the financially excluded and underserved groups in South Africa – bank issue pre-paid low value payment product

Description of the product and financial facilities	Amount/threshold limitation	Customer identification requirements
A conditional exemption from the identification and verification elements under of the relevant legislation was made to provide for a pre-paid low value payment product which is issued by banks, the Postbank and mutual banks. A product of this nature can be used as a means of payment for goods and services within the Republic of South Africa only. It cannot facilitate cash withdrawals or remittances of funds to third parties.	A limit on the monthly turn-over of value loaded onto the pre-paid instrument is ZAR 3 000 (EUR 300, USD 390). A limit on the balance on the product is ZAR 1500 (EUR 150, USD 195) at any given time. A limit on the spending on the product is ZAR 200 (EUR 20, USD 26) per transaction.	None. Instead the bank on whose behalf the product is issued to clients by agents has to establish and verify the identities of those agents as it would for customers in terms of the relevant anti-money laundering legislation. In addition the bank on whose behalf the product is issued to clients by agents has to apply enhanced measures over and above its normal procedures, to scrutinise the transaction activity of the agents in relation to the issuing of the prepaid instruments on an ongoing basis with a view to identify and report suspicious and unusual transactions.

Example 5 – product launched to serve the financially excluded and underserved groups in Pakistan - Basic/Entry Level Branchless Banking Accounts

Account Level	Level 0	Level 1
Description	Basic branchless banking Account with low KYC requirements and low transaction limits.	Entry Level account with adequate KYC requirements commensurate with transaction limits.

Account Level	Level 0	Level 1
KYC/Account Opening requirements /conditions	1. Original Computerised National Identity Card (CNIC) of the customer 2. Legible image of customer's original CNIC 3. Digital photo of the customer. 4. Transfer of customer's data electronically to the FI. 5. Copy of Terms & Conditions form to customers 6. Verification of customer's particulars with NADRA (National Database and Registration Authority). 7. Allowing one deposit and one withdrawal transaction during account opening.	1. Original CNIC of the customer 2. Copy of the CNIC or legible image of customer's original CNIC 3. Digital photo of the customer 4. Physical Account Opening Form 5. Confirmation of customer's cell phone number 6. Verification of customer's photo, signature and at least one of the two unique particulars with NADRA record and by follow up with the customer 7. Allowing three deposits and one withdrawal transaction during account opening / activation process.
Account Opening Process	**A) Responsibilities of Agent:** 1. Fill up digital Account Opening Form covering basic personal information of the customer. 2. Check original CNIC and capture its legible image (at least front side) through scanner or digital camera etc. 3. Capture customer's live digital photo at the time of account opening 4. Collect initial deposit for account opening and provide proof of transaction to customer. 5. Provide signed Terms & Conditions form to the customer (with salient features written in Urdu) and obtain a signed acknowledgement receipt from the customer after completing the account opening process. 6. Transfer customer's data electronically to the FI. 7. Financial Institution (FI) may allow Level 0 customer to carry out only one deposit and one withdrawal transaction during	**A) Responsibilities of Agent:** 1. Filling up and signing of physical Account Opening Form including Terms & Conditions by the customer at the agent location. 2. Provide signed copy of Account Opening Form including Terms & Conditions (with salient features written in Urdu) to the customer. 3. Check original CNIC of customer, take copy of CNIC or capture legible image of customer's original CNIC (at least front side) and mark the form —Original CNIC Seen. 4. Capture customer's live digital photo at the time of account opening. 5. Collect initial deposit for account opening and provide proof of transaction to customer. 6. Transfer all data to FIs either through surface mail or electronically (scanned copies). 7. FI may allow a Level 1 customer to carry out only one deposit and one withdrawal transaction during account opening. 8. Two additional deposit transactions

Account Level	Level 0	Level 1
	account opening. **B) Responsibilities of FI:** 1. Verify customer's CNIC particulars and his/her photograph from NADRA. 2. Appropriate action may be taken including blocking of the account if any information of the customer is found incorrect. 3. Further transactions will be allowed after verifications from NADRA and getting confirmation from the customer either through voice call or getting a signed acknowledgement of account opening. 4. Maintain digital record of account opening data, customer photo and verification documents which should be possible to print when required.	may also be allowed to the customer before his/her account is fully activated. **B) Responsibilities of FI:** 1. Verify customer's CNIC particulars from NADRA, including photograph, signature and at least one of the following two fields of unique information not disclosed on CNIC and Account Opening Form: *i. Mother's maiden name OR* *ii. Place of birth etc.* 2. FIs shall confirm either from PTA or the customer that the given cell number of the customer is registered in his/her name. 3. Appropriate action may be taken including blocking of the account if any information of the customer is found incorrect. 4. Further transactions will be allowed after due verifications from NADRA and customer. 5. Maintain physical record of customer account opening data and verification of documents.
Transaction Limits	PKR 15 000 per day (USD 158) PKR 25 000 per month (USD 254) PKR 120 000 per year (USD 1269)	PKR 25 000 per day (USD 254) PKR 60 000 per month (USD 634) PKR 500 000 per year (USD 5 286)

ANNEX 6: EXAMPLES OF RISK ASSESSMENT TOOLS

I. PRESENTATION OF THE RISK ASSESSMENT TEMPLATE IN THE STRATEGIC IMPLEMENTATION PLANNING (SIP) FRAMEWORK

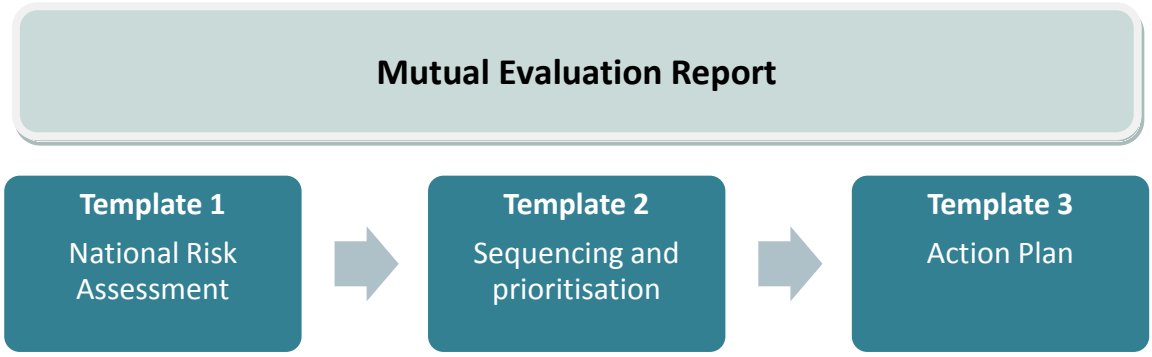
1. The Strategic Implementation Planning (SIP) Framework aims to provide post-mutual evaluation implementation assistance.

2. The SIP Framework aims to use the Mutual Evaluation Report (MER) findings to develop a National Implementation Plan (NIP), concentrating on key areas found to be less than fully compliant. This involves prioritising and sequencing the implementation of MER recommendations on the basis of identified risks/vulnerabilities and the 16 core/Key FATF Recommendations[102], and factoring in resourcing and capacity constraint issues.

3. The tool is ideally used immediately after the adoption of an MER; however, it can be used at any time. In the case of the risk assessment, it should be used prior to a mutual evaluation if possible.

4. Following figure illustrates the SIP framework. The framework is basically built on the MER recommendations. But in addition to MER recommendations it also aims to address the risks that have been identified through Template 1, a detailed spreadsheet that is designed as a self-risk assessment tool.

Figure 3. **SIP framework**



COMPONENT 1: NATIONAL RISK ASSESSMENT (NRA) USING TEMPLATE 1

Background

[102] This will be updated as the FATF discussions evolve on this point.

- Jurisdictions need a basis for prioritising and allocating limited resources to ensure their actions are focused effectively and efficiently.
- For the purpose of prioritisation and more efficient allocation of resources, jurisdictions may consider conducting a risk and vulnerability analysis to identify the relevant areas to focus on when implementing the required AML/CFT measures.
- A national risk assessment should assist jurisdictions to understand sources and methods of ML/TF threats; identify vulnerabilities and risks across various sectors; and evaluate weaknesses in their legal, judicial and institutional systems.
- Template 1 sets out some of the information that jurisdictions may need to collect in order to assess their ML risks, although Template 1 can be modified for TF purposes. (Note: A separate template is being developed for TF risk assessment.)
- A flow-chart describing the SIP Framework is provided below and a detailed description is available at www.apgml.org under Implementation Issues/SIP Framework.

Methodology

- Template 1 utilizes a matrix approach in assessing the ML and TF risks. It focuses on the assessment of threat and vulnerabilities as the main components of the ML/TF risk. Template 1 is an excel file with 5 assessment areas, accompanied by summary findings. Each of the assessment areas contains carefully selected indicators to assess treats and vulnerabilities. Two separate risk assessment is undertaken on ML risk and TF risk, using the symmetric risk assessment structure. The worksheets designed for the ML/TF assessment consists of following sections:

National ML Risk Assessment Template	National ML Risk Assessment Template
Threat Analysis	**Threat Analysis**
1. Prevailing Crime Type	1. TF Threat Analysis
Vulnerability Analysis	**Vulnerability Analysis**
2. Legal/Judicial/Institutional Framework	2. Legal/Judicial/Institutional Framework
3. Economic and Geographical Environment	3. Economic and Geographical Environment
4. Financial Institutions	4. Financial Institutions
5. DNFBPs	5. DNFBPs

- The main difference between ML and TF risk assessment templates is the threat analysis. The objective of ML Threat Analysis is to understand what type of predicate crime poses a ML threat in the jurisdiction, and identify origins (both domestic and foreign) methods of ML. Outcome of this threat analysis will be useful for law enforcement agencies (LEAs) to prioritize their actions. It is also useful for FIU and covered institutions to understand the type

of crimes that generate proceeds and methods of laundering. On the TF risk assessment side, TF threat analysis attempts to capture the statistics and any other information on TF cases and assess the level and sources of TF threats. Vulnerability analysis section consists of four assessment matrices, each of which focuses on vulnerabilities arising from different areas. "Legal/Judicial/Institutional Framework" and "Economic and Geographical Environment" assesses the vulnerabilities arising from the factors at the national level, while "Financial Institutions" and "DNFBPs" focuses on vulnerabilities posed by financial institution and DNFBP categories that are present in assessed jurisdiction. The structure of Financial Institutions and DNFBPs are different from the others, and they are designed to enable assessment and of the inherent vulnerabilities as well as net vulnerabilities (after taking into account the control measures) arising from various sectors, institutions or professions. Vulnerability assessment in ML and TF risk assessment templates are very similar and differ in limited number of indicators.

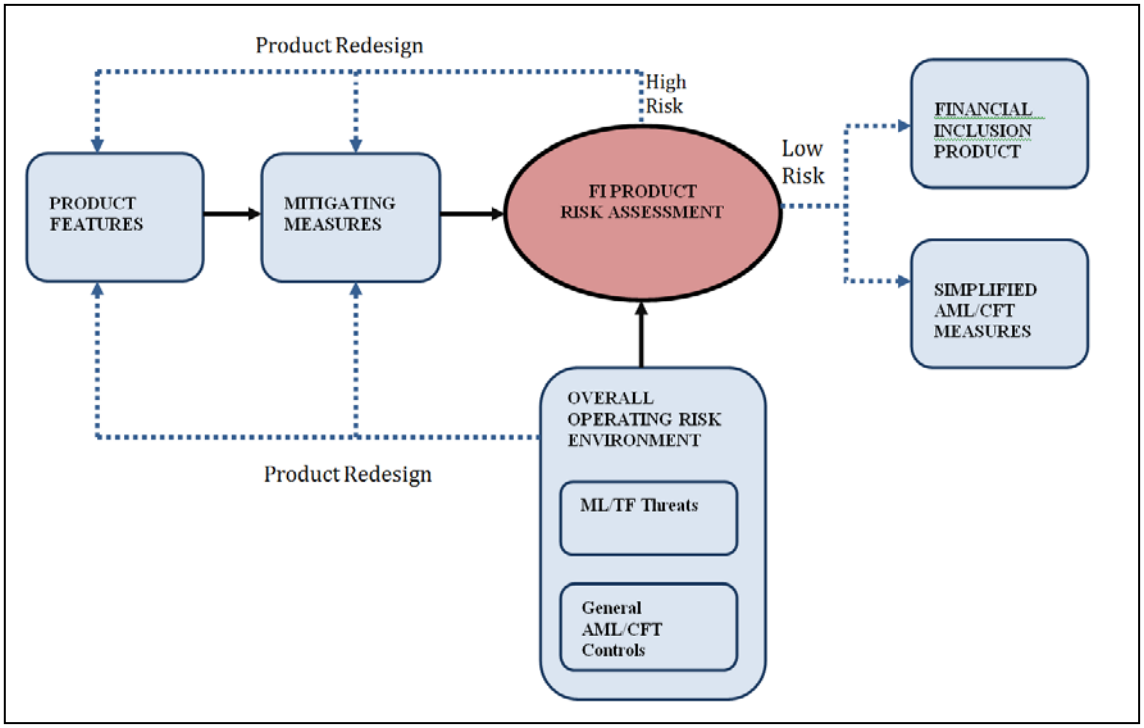
- For each of the indicators in the matrices, a threat, vulnerability or risk level is assessed based on the information and statistics provided. Available information and statistics are filled into designated boxes in the templates. Most of these boxes are designed to capture a short summary of the information/justification. A detailed write up that elaborates the grounds and justification for each assessment, is required in order to ensure the quality and credibility of the assessments.

- The template includes pre-identified and carefully selected indicators to assess the ML/TF risks; however, the template can be customized by adding new indicators or amending existing ones, to reflect each country's unique environment.

II. EXAMPLE OF RISK ASSESSMENT OF FINANCIAL INCLUSION PRODUCTS

World Bank has developed a risk assessment module that focuses specifically on financial inclusion products. The Financial Inclusion Product Risk Assessment Tool aims to assists national authorities with a logical and user-friendly framework to evaluate the money laundering and terrorist financing risks arising from both existing and emerging/new financial inclusion products, in order to effectively facilitate financial inclusion while mitigating potential ML/TF risks. It can be used by regulators to design regulatory framework for financial products or features, or to assess whether an existing financial product can be classified as a low or lower risk. While the tool was developed for use by primarily regulators, it can also be used by the private sector institutions.

The general approach of the risk assessment is provided below.



In the first step, key questions relating to the specific product features of the financial inclusion product will be asked. In the second step, key questions regarding the overall ML and TF risk environment in the specific country will be asked. This includes potential threats of ML/TF in the country and the associated control measures that are in place. The third step is to assess initial ML/TF risk level for each specific product feature, given the information gathered and analysed in step 1 and 2. If the risk level is high or higher than desired, the tool offers guidance on how to mitigate risks arising from the features of the product.

This process is a dynamic process, which enables redesigning of product features and mitigation measures depending on the desired risk levels.

This financial inclusion risk assessment tool is a part of National ML/TF Risk Assessment Tool that the World Bank has developed. It can be used as a stand-alone tool or as part of the NRA exercise.

III. EXAMPLES OF RISK ASSESSMENT METHODOLOGIES DEVELOPED BY THE INDUSTRY

Western Union Risk Methodology

Western Union offers its remittance and other retail payment services across the globe to a broad range of consumers including banked, unbanked, underserved and migrant populations. Consumer value the Company's global reach, reliable service and convenience. The breadth of the Company's reach creates unique challenges in balancing the utility of the services to consumers and mitigating the misuse of services. To assist in this effort Western Union assesses its risk using the traditional FATF risk categories of Agent, Consumer, Geography and Services. The Company uses these categories as a starting point to identify issues and organize its risk assessment efforts. Where relevant, categories are used in various combinations to further tailor Western Union's efforts to its specific risks.

- **Consumer Risk** -Western Union provides value to its consumers through fast, efficient and widely available financial services. Many consumer segments utilize the services throughout the world including those who have access to a variety of financial services as well as those who are underserved and migrant populations who often have no other reliable means of transferring funds, paying bills and accessing other financial opportunities. The utility and broad appeal of Western Union's services means the Company must be diligent in the identification and mitigation of consumer risk. Mitigation efforts include transaction analysis, regulatory reporting, real-time and back-office controls and other techniques. The Company works to identify problematic behaviour, underlying transaction patterns and other indicators of problematic consumer behaviour and take action against it.

- **Agent Risk** - Western Union has Agents located throughout the world to provide its services. Research is done to place Agent locations where Western Union's consumers are located; this includes banked as well as underserved and migrant populations. Agent risk is considered in terms of those Agents unable or unwilling to follow the law and Western Union policies, Agents assisting in problematic behaviour and Agents where problematic behaviour is occurring. To mitigate these risks the Company performs due diligence exercises before an Agent is allowed to conduct business, training before and after activation, transaction review, Agent visits and several other items to provide Agents with the necessary skills to comply with the law and Western Union's policies and to identify those Agents who are not in compliance.

- **Geographic Risk** - Given the Company's global scope there is a need to identify and focus on geographies of higher risk. This is done through the use of relevant publically available information that ranks countries on factors such as stability, financial transparency and other metrics. These statistics are blended with Western Union's own internal data to tailor the third party data to the Company's specific risks. The rankings drive enhanced transaction monitoring efforts in high-risk countries, assist with program prioritization and many other processes.

- **Services Risk** - The Company has created a Services risk model to identify the inherent risks of the services and available controls as well as potential gaps. This assists the Company in scheduling and prioritizing program improvements. Frequently, a service's risk is mitigated through the identification of a consumer or Agent risk pattern which is addressed through consumer or Agent focused controls for a service or group of services. Problematic behaviour can occur across multiple services and the Company will mitigate these risks with solutions that cover all affected services as opposed to the individual service.

- **Risk Category Combination** - Where relevant the Company uses data from the individual risk categories in combination to arrive at more meaningful risk assessments. As mentioned in the Geographic Risk section, a country's risk ranking may influence consumer and Agent efforts in that country. The Company works to identify these opportunities to focus its mitigation efforts to those situations of highest risk.

Source: Western Union, 2011

Risk-Based KYC developed by Globe Telecom in the Philippines

Part of Globe's Risk Based KYC is the development of the Risk Rating Matrix which is composed of risk drivers such as the type of customer and the value of GCASH being transacted. The combination of these risk drivers - serves as the basis for the three types of risk ratings: Low, Medium, and High.

Risk Rating KYC (P5 000 is equivalent to USD 100):

		Amount	
		Below P5K	**P5K and up**
Customer	Known in the Community	**Low**	**Med**
	Not Known in the Community	**Med**	**High**

Full KYC[103] vs. Risk Based KYC:

KYC Process	Full KYC	Risk-Based KYC
Use of forms	Yes	Yes
Presentation of 1 Valid ID	Yes	Yes
Recording of ID details	Yes	Yes
Photocopying of ID:	Yes	No
Known in the community	Yes	**No**
Not known in the community	Yes	**No if amount is less than P 5 000**
		Yes, if amount is P 5 000 and up

GSMA Methodology for Assessing Money Laundering and Terrorist Financing Risk

In relation to mobile money services, the GSMA has developed a Methodology for Assessing Money Laundering and Terrorist Financing Risk[104], that offers–a systematic approach for assessing the

[103] "Full KYC" as understood by Globe Telecom to comply with the relevant regulation in the Phillipines
[104] Solin, M. and Zerzan, A. (2010).

ML/TF risks of mobile money. The GSMA Methodology is based on an understanding of how money launderers and terrorists could exploit the vulnerabilities of the sector, and discusses appropriate and effective tools, including a variety of risk-mitigation processes to address ~~identified~~ risks. Measures that reduce the risk of ML/TF by consumers, for example, include establishing limits on account sizes, transaction frequencies and volumes, and monitoring transaction flows on the system level. By assessing risk before and after such mitigating controls are in place, service providers and regulators can evaluate the effectiveness of such mechanisms. Ongoing risk assessment after controls have been applied becomes an input for adjusting Customer Due Diligence (CDD) requirements on an as-needed basis.

In late 2010, SMART Communications in the Philippines employed the GSMA Methodology to prepare a risk assessment and develop appropriate risk mitigation mechanisms in order to seek approval from the Philippines Central Bank (Bangko Sentral ng Pilipinas, or BSP) to apply reduced KYC requirements to certain customers registering for SMART Money. In early 2011, the BSP issued Circular 706 instructing institutions to "formulate a risk-based and tiered customer identification process that involved reduced CDD for potentially lower-risk clients and enhanced CDD for higher-risk accounts" and describing the requirements for reduced and enhanced CDD[105].

The GSMA has also identified potential vulnerabilities for – risk categories – at each stage of a mobile money transaction:

General risk factors	Sample exploitation of vulnerabilities at each stage		
	Loading	**Transferring**	**Withdrawing**
Anonymity	Multiple accounts can be opened by criminals to hide the true value of deposits	Suspicious names cannot be flagged by system, making it a safe-zone for known criminals and terrorists	Allows for cashing out of illicit or terrorist-linked funds.
Elusiveness	Criminals can smurf proceeds of criminal activity into multiple accounts	Criminals can perform multiple transactions to confuse the money trail and true origin of funds.	Smurfed funds from multiple accounts can be withdrawn at the same time.
Rapidity	Illegal monies can be quickly deposited and transferred out to another account.	Transactions occur in real time, making little time to stop it if suspicion of terrorist financing or laundering.	Criminal money can be moved through the system rapidly and withdrawn from another account.
Lack of oversight	Without proper oversight, services can pose a systemic risk.		

Source: GSMA Risk Assessment Methodology

Other stakeholders may be in a position to inform a country of a given sector's exposure to ML/TF risks. For instance, the 2011 World Bank study on "*Protecting Mobile Money against Financial Crimes, Global Policy Challenges and Solutions*" offers a detailed analysis of the major ML/TF risks faced by the mobile

[105] See Bangko Sentral Ng Philipinas (2011)

money services[106]. Countries may find this risk categorization helpful in informing their domestic risk analysis and developing appropriate risk-management responses.

Type of risk	Observed risks
Anonymity	Acquisition of customers off-branch or not in face-to-face meetings. Use of false identification. Unauthorized use of mobile money services through phone theft, passing a phone, or wireless on network breach.
Elusiveness	Some practices may cover for the true initiator or recipient of a transaction.
Rapidity	Using mobile phones at the layering stage of the ML process (move money across multiple mobile money accounts).
Poor Oversight	Mobile money schemes may fall outside any form of regulations.

Source: Chatain, P-L., *et al* (2011).

[106] Chatain, P-L., *et al* (2011). See also Chatain, P-L. *et al (*2008).

ANNEX 7: COUNTRIES' INITIATIVES TO ADDRESS THE CUSTOMER IDENTIFICATION/IDENTITY VERIFICATION CHALLENGES

USE OF ALTERNATIVE IDENTIFICATION MEANS OR DOCUMENTS

Fiji	■ A "suitable referee" is a person who knows the customer and whom the financial institution can rely on to confirm that the customer is who he or she claims to be and can verify other personal details (occupation, residential address) of the customer. Examples of suitable referees include village headmen, religious leader, current or former employer, and official of the Fiji Sugar Corporation sector office (for sugar cane farmers and labourers). ■ A Certificate/Letter/Confirmation from a suitable referee should include (i) customer's name, address, occupation, (ii) referee's name, address, occupation and contact details (such as phone number), (iii) statement stating how long (period) the referee has known the customer, (iv) statement stating that the referee knows the customer by the stated name, (v) statement stating that the referee confirms the customer's stated address and occupation or nature of self-employment to be true and (vi) signature of the customer and referee with the date the document was signed. ■ The signed declaration (from the suitable referee) must be accompanied by a birth certificate (which all persons must have). Financial institutions cannot rely solely on a signed declaration during the verification process. This is to mitigate any risk of fraud associated with relying on a signed declaration. ■ There is no requirement for a photo of the customer (even with a signed declaration).
Lesotho	■ In Lesotho, the low risk customer threshold below which a reduced CDD procedure is applicable, is defined at national level: individuals with monthly gross turnover less than LSL 4,999.99 (USD 736) are low risk customers. Almost 80% of the portfolio of Lesotho PostBank falls under the low risk category. ■ The Central Bank has approved the following reduced CDD for Lesotho PostBank: ■ - Only an ID (or other formal identification documents) is required to open an account for all customers of Basotho origin or with monthly deposits of less than LSL 4,999.99. No request is done to provide documents for the purpose of address or income verification (the customer is just asked to state them in writing in relevant bank forms – no further verification, unless there is suspicion).

	■ - The ID card for social grant beneficiaries (different than the national official ID) is accepted for KYC exercise for the purpose of social grant payments. ■ The record keeping of transactions and documents can be done in electronic format (documents scanned). ■ The monitoring is done to identify unusual activity of an account.
Malawi	■ Banks accept the following alternative identification documents from low income earners: letters from Traditional Authority, Malawi Electoral Commission Voter Registration Certificate, and Letters from employers, ■ Photograph, biometric identification upon verification of the document
Malaysia	■ The bank accepts *birth certificates, passports* as means of identification for Malaysian citizens and *refugees' cards, student cards, work permits and letters from college/university* for non-citizens. ■ *Employee address* or any other address is accepted to justify a residential address. As for rural areas which do not have any information of residency or address, the bank requires *a postal address*, which is either a *communal post box or neighbour address*.
Mexico	■ Work is in progress to completely implement a scheme for data verification process of non-face to face accounts opened by phone or at the banking institution website. Financial institutions should validate that the data provided by the client matches with the information of the National Population Registry using an Official Unique ID Code (CURP). The CURP is a countrywide registry that comprises all the inhabitants of Mexico (both foreigners and nationals), as well as Mexicans living abroad. ■ In non-face-to-face phone schemes, financial entities should validate the CURP with the cell phone number.
Philippines	■ *Barangay Certification*, a certificate issued by the village master, is accepted as a proof of identification and residence. ■ The bank accepts as other forms of identification: *passport, driver license, student ID, employment ID*, if such documents are *issued by official authorities of the Republic of Philippines, its subdivisions and instrumentalities, government owned and controlled bodies and private entities registered and supervised by the Central Bank (BSP), the Securities and Exchange Commission and the Insurance Commission*.
Switzerland	■ Competent authorities in partnership with the private sector have examined ways to improve access to financial services by foreign illegal migrants who entered or remain in the country illegally, without valid visa/permits or authorizations. Under Swiss anti-money laundering legislation, an official document of any kind is sufficient for the purpose of CDD measures provided it contains the name, date of birth, nationality, address and a photograph.

United States	■ Matricula consular cads for migrant workers or other non US persons, particularly migrant workers from Mexico are allowed to be used as forms of identification.

USE OF INNOVATIVE TECHNOLOGICAL SOLUTIONS

Some countries are using innovative IT solutions to supplement efforts, like biometrics or voice prints. Such market-based solutions have been especially developed in Malawi (see table above) and **New Zealand** where Digicel Pacific Limited, a MNO which operates across the Pacific and is part of Digicel Group (operating in the Caribbean, Central America and the Pacific) has recently introduced in New Zealand a biometric ID system[107], In **Rwanda** and **Kenya**, storing electronic finger prints is permitted and in both countries credit unions have piloted fingerprint identification technology for rural poor customers.

Countries are also developing electronic multi-purpose forms of identification. For instance, in the next few years, Indonesia, along with other countries in Asia, like India, China, Philippines, and Vietnam, will implement an electronic passport (e-passport) technology that uses contactless smart cards. The "Universal Electronic Card will be issued to natural persons upon request as of January 2013, and later to every citizen in Russia.

India is embarking on a project to provide every Indian resident a 12-digit biometric identification number, formerly called the Unique Identity Number (UID) and now called the Aadhaar number, tied to three pieces of biometric data (fingerprints, iris scans, and a facial picture) and limited demographic information. Currently, many of India's poorest citizens do not have any ID cards, bank accounts, or even addresses that they can use to obtain social services. The Aadhaar number is intended to allow individual identification anytime, anywhere in the country through online identity verification from a central database. If successfully implemented, it would be the first biometrically verified unique ID implemented on a national scale and would provide the "identity infrastructure" for financial inclusion, as well as for strengthening AML/CFT implementation, delivery of social services, subsidies and other programs and national security, and anti-corruption efforts.

PROCEDURES SPECIFICALLY APPLIED IN LOWER RISK SCENARIOS

In **India**, special provision has been made under the AML/CFT regulations for low-income customers lacking standard identification documentation to permit them to open "small" or no "frills" accounts[108]. Small accounts can be opened without the customer's producing the normal identification documentation, on the basis of the customer's signature or thumb print and a self-attested photo, provided the account is opened in the presence of a designated bank officer who certifies that he/she witnessed the customer affix his/her signature or thumb print. The account is operational for twelve months but can be renewed for another twelve months if the account holder provides evidence that he/she has applied for valid identity documents within a year of account

[107] PR Newswire (2012)
[108] See Annex 5 for more details

opening. If there is a suspicion of money laundering or terrorist financing or other high risk scenarios, the customer's identity must be confirmed promptly through officially valid documents.

In **Brazil**, for simplified accounts targeted at the low-income market, subject to a monthly transaction limit of US 492 (BRL 1, 000), account opening can proceed without CDD documentation, on the condition that all relevant documents are presented within 6 months of account opening.

In **Mexico**, the current AML/CFT legal provisions for banking institutions establish four levels of accounts specifically designed for low-income groups of the population–and AML safeguards corresponding to their respective exposure to ML/TF risks. Level 1 accounts -low transactional accounts[109]- were implemented under a balanced risk-based approach to increase financial inclusion underpinned by adequate AML/CFT controls.

When **South Africa**n authorities considered developing products designed to serve the financially excluded or underserved[110], they recognised that full CDD, in particular, obtaining and verifying a residential address (as required under South African law) was not feasible given that most people typically did not have residential addresses that could be confirmed by reference to formal documentation. Such a requirement would have precluded most individuals in the intended target market from accessing basic financial products. The authorities revised an existing exemption, Exemption 17 to relieve financial institutions from verification requirements under the money laundering and terrorist financing regulations. Exemption 17 now provides for a form of simplified due diligence for products meeting specific requirements. The exemption applies to banks, mutual banks, the Post Bank, the Ithala Development Finance Corporation Ltd and money remitters (but only for domestic funds transfers) and exempts them from requiring and verifying residential address information as part of the CDD process (many of the financially excluded lived in informal settlements with-no formal addresses). The institutions still must obtain and verify identity information, namely a customer's full name, date of birth and identity number. The exemption applies when the following conditions are met:

- the customer must be a natural person who is a citizen of or resident in South Africa.
- the customer cannot withdraw, transfer or make payments of an amount exceeding R 5000 (approximately USD 564) per day or exceeding R 25,000 (approximately USD 2 824) in a monthly cycle;
- the customer cannot transfer funds to any destination outside South Africa, except for transfer resulting from a point of sale payment or a cash withdrawal in a country in the Rand Common Monetary Area (South Africa, Lesotho, Namibia and Swaziland);
- the balance maintained in the account must not exceed R 25,000 (approximately USD 2 824) at any time and; the same person cannot simultaneously hold 2 or more Exemption 17 accounts with the same institution. Where a customer exceeds the account limits, the

[109] See Annex 5 for more details
[110] See Annex 5 for more details

accountable institution[111] is - required under the exemption to conduct full CDD before completing any additional transactions associated with that customer's account.

Exemption 17 facilitated the launch of several basic banking services including the Mzansi account and the WIZZIT Payments.

- The Mzansi account was developed by the South African banking industry and launched collaboratively by the four largest commercial banks (ABSA, FNB, Nedbank and Standard Bank) together with the state-owned Postbank in October 2004. By December 2008, more than six million Mzansi accounts had been opened[112], and almost two thirds of South African adults were banked, a sizeable increase from just under four years earlier. Currently, at least one in ten South African adults has an Mzansi account and one in six banked people are active Mzansi customers.

- WIZZIT Payments (Pty) Ltd is a provider of basic banking services for the unbanked and under-banked people or enterprises that have no or only limited access to banking services in South Africa. Launched in 2004, WIZZIT is formally a division of the South African Bank of Athens. Its services are based on the use of mobile phones for opening and accessing bank accounts and conducting transactions, in addition to a Maestro debit card that is issued to all customers upon registration. The accounts opened in this way are offered within the parameters of Exemption 17. WIZZIT had an estimated 300,000 customers in South Africa in January 2010.

In 2004, the Financial Intelligence Centre in South Africa published a Guidance Note concerning the client identification – to assist accountable institutions and supervisory bodies with the practical application of the client identification requirements of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act). It describes a risk-based approach to establishing and verifying identity.

The FIC Act and the Money Laundering and Terrorist Financing Control Regulations require that accountable institutions identify all clients with whom they do business unless an exemption applies in a given circumstance. However, institutions are not required to follow a one-size-fits-all approach in the methods they use and the levels of verification they apply to clients.

The Regulations note that accountable institutions must verify certain particulars against information that can reasonably be expected to achieve such verification "and" is obtained by reasonably practical means. This means that an institution must determine what information may be necessary to achieve verification of the particulars in question and by what means this verifying information can be obtained. In doing so, the institution should balance the accuracy of the verification required and the level of effort invested to obtain such verification so that its verification process is commensurate with the nature of the risk involved in a given business relationship or transaction.

[111] Financial institutions covered by the Financial Intelligence Centre Act, 2001 (FIC Act) are called "accountable institutions" in South Africa.

[112] This is a measure of accounts opened and does not reflect the current status of the accounts (i.e., it includes active, dormant, closed and even opened-but-never-funded/activated).

- Applying a risk-based approach to the verification of the relevant particulars implies that an accountable institution can accurately assess the risk involved. It also implies that an accountable institution can take an informed decision on the basis of its risk assessment as to the appropriate methods and levels of verification that should be applied in a given circumstance. An accountable institution should therefore always have grounds on which it can base its justification for a decision that the appropriate balance, referred to above, was struck in a given circumstance.

- Accurately assessing the relevant risk means determining, firstly, how the reasonable manager in a similar institution would rate the risk involved with regard to a particular client, a particular product and a particular transaction, and secondly, what likelihood, danger or possibility can be foreseen of money laundering occurring with the client profile, product type or transaction in question. It is imperative that the money laundering risk in any given circumstance be determined on a holistic basis. In other words, the ultimate risk rating accorded to a particular business relationship or transaction **must be a function of all factors which may be relevant to the combination of a particular client profile, product type and transaction**.

- The assessment of these risk factors should best be done by means of a systematic approach to determining different risk classes and identify criteria to characterise clients and products. In order to achieve this, an accountable institution would need to **document and make use of a risk framework**.

- Once a proper risk assessment is done an institution must put in place measures to isolate the different risk classes and to ensure that procedures which are appropriate only for lower risk classes are not applied in relation to higher risk classes. Due regard needs to be paid to the practicability of segregating different risk categories. As with all risk management, an institution's risk framework **needs to be regularly updated** and **supported with documentation** to enable and ensure compliance within each institution.

(Source: General Guidance Note Concerning Identification of Clients, South Africa, April 2004)

PROCEDURES APPLIED IN NON FACE-TO-FACE SCENARIOS

In 2011, the State Bank of **Pakistan** (SBP) revised the branchless banking regulations introduced in 2008 and applicable to all financial institutions (commercial, Islamic and microfinance banks) [113]. With a view to expanding the outreach of branchless banking operations in the country, SBP introduced level '0 branchless bank accounts to bring the low income earning segment of society into the formal financial sector. Under the amended regulation, branchless banking agents are allowed to send the digital account opening form, the customers' digital photo and an image of the customer's Computerized National Identity Card (CNIC) to the financial institution–electronically, instead of sending the physical account opening forms and copies of customers' CNICs to the financial institution for further processing. The new category of level '0 branchless banking accounts will provide flexibility to agents and financial institutions for opening basic branchless banking

[113] State Bank of Pakistan (2011)

accounts, while rationalizing the KYC requirements in line with the account transaction limits, which are: daily limit USD 165 (PKR 15 000), monthly limit USD 275 (PKR 25 000), annual limit USD 1 316 (PKR 120 000) and maximum balance limit USD 1 097 (PKR 100 000).

In **South Africa**, a bank offering a mobile-payment service is required to obtain a name and a national ID number from the client and cross-reference these against an acceptable third-party database and then undertake additional electronic CDD measures, including cross-referencing the customers' information with third-party databases that source identity information from the Department of Home Affairs' population register and controls that prevent a customer from having more than one such an account with the bank[114]. However, since the regulator has determined that this service model introduces higher ML risk, clients who use the non-face to face registration process can– transact against their accounts in a total amount of no more than approximately US$120 (ZAR1,000) a day. The regulator thus chose to limit the functionality of the account rather than to prohibit the business model. The control measures also allow for flexibility: clients who wish to transact for larger amounts can be released from the restrictions after submitting to regular face-to-face CDD procedures[115].

In **Malawi**, a "fast track" account was introduced, which accepts minimal KYC measures. The characteristic of the account are as follows:

- It is a savings account which is sold by Direct Sales Agents (DSA), not bank staff members;
- The DSAs report to a team leader of a branch or agency who are responsible for day to day supervision;
- Upon opening of the account, customers are issued with a starter pack which contains an ATM Card (none personalised), PIN Mailer, Manual on the Fast Account and Mobile;
- The customer pays a sum of K900 (USD3.2) - K500 (USD1.84) for ATM Card Fee and K400 (USD1.48) for initial deposit;
- The initial deposit is deposited by the DSA at the branch together with the rest of the customer details by close of business of the date of transaction;
- The account is activated at the regional processing hub after ensuring that all forms have been completed and the supporting documents are attached;
- The only registration that requires the customer to go to a branch is when he/she wants to have the mobile facility;

[114] Registrar of Banks' Guidance note 6 of 2008.

[115] Isern, J. and De Koker, L. (2009), p 8.

- The product targets low income earners and maximum limit of withdrawals per month is K 50 000 (USD184.50)[116].

RISK FACTORS AND POSSIBLE APPROACHES TO VALIDATE CUSTOMERS' IDENTITY

In **the UK**, the Guidance issued by the Joint Money Laundering Steering Group[117] identifies risk factors and designs some possible combined approaches to validate customers' identity:

Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on so-called 'identity documents', such as passports and photocard driving licences, and these are often the easiest way of being reasonably satisfied as to someone's identity. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of confirmation, including, in appropriate circumstances, written assurances from persons or organisations that have dealt with the customer for some time.

How much identity information or evidence to ask for, and what to verify, in order to be reasonably satisfied as to a customer's identity, are matters for the judgement of the firm, which must be exercised on a risk-based approach, taking into account factors such as:

- the nature of the product or service sought by the customer (and any other products or services to which they can migrate without further identity verification);
- the nature and length of any existing or previous relationship between the customer and the firm;
- the nature and extent of any assurances from other regulated firms that may be relied on; and
- whether the customer is physically present.

Evidence of identity can be in documentary or electronic form. An appropriate record of the steps taken, and copies of, or references to, the evidence obtained, to identify the customer must be kept.

Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the ML Regulations, or to equivalent legislation; then
- those issued by other organisations.

Firms should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, firms should take whatever practical and proportionate steps are

[116] However, this was about USD285 before devaluation. The regulator is yet to revise the simplified measures limits.

[117] The JMLSG is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations.

available to establish whether the document offered has been reported as lost or stolen. In their procedures, therefore, firms will in many situations need to be prepared to accept a range of documents, and they may wish also to employ electronic checks, either on their own or in tandem with documentary evidence.
(*Source: JMLSG*)

ANNEX 8: COUNTRIES' INITIATIVES TO ADDRESS THE RECORD KEEPING REQUIREMENTS CHALLENGES

In **South-Africa**, legislation allows for electronic capturing and storage record information, including in relation to documents of which copies must be retained.

In **Mexico**, in an effort to expand efficient and secure financial services to people living in rural, marginalized areas, the World Council of Credit Unions (WOCCU) has teamed with Caja Morelia Valladolid, one of Mexico's largest credit unions, in a pilot project to utilize personal digital assistants (PDAs) to perform financial transactions during field visits to their members. Field officers previously recorded transactions manually in Caja Morelia's accounting books and in members' passbooks then took the records back to the credit union to process. Through PDA, technology handheld printers immediately produce receipts while member accounts are updated in real time. PDA applications shorten transaction times which reduces the length of waiting time for members and enable credit union representatives to serve more people during field visits. This new technology offers an interesting alternative retention technique for transactions information.

ANNEX 9: COUNTRIES' EXAMPLES OF DOMESTIC COOPERATION TO PROMOTE FINANCIAL INCLUSION

DOMESTIC COOPERATION IN BRAZIL

Aligned with the Principles for innovative financial inclusion from the G20, various authorities related to the issue of financial inclusion in Brazil have been working in an integrated and coordinated manner. In this sense, the Central Bank has established several technical cooperation agreements with different government agencies.

In the area of financial education, it was established in 2007, at the federal level, a working group comprised of representatives from the Central Bank, the Brazilian Securities Commission (CVM), the National Superintendency of Pension Funds (Previc), and the Superintendency of Private Insurance (Susep), with the main goal of developing the National Strategy for Financial Education proposal (ENEF), which should promote a national inventory of actions and projects for Financial Education in the country, in addition to conducting research aimed at showing the degree of financial education of the population.

As for actions related directly to the appropriate financial inclusion of the population, the Central Bank has established institutional partnerships. One example of partnership with government representatives is its partnership with the Ministry of Agrarian Development (MDA), established in 2004 to promote the credit union directed to family farmers and agrarian reform settlers, seeking the democratization of financial services in Brazil, especially in rural areas, which still concentrates the highest level of poverty in Brazil. In 2009, a partnership with the Ministry of Work and Employment (MTE) was established in order to conduct studies for systematic monitoring of the development of social currency in Brazil.

In 2010, the Central signed three important agreements:

- The first was signed with the Ministry of Justice (through the Secretariat of Economic Law and the Department of Consumer Protection and Defense - DPCD), aimed at "improving the delivery of products and provision of services to customers and consumer users of financial institutions, consortium management, and other institutions authorized to operate by the BCB";
- The second was signed with the Ministry of Environment (MMA), through technical agreement, aimed at combining efforts to strengthen the agenda of monitoring of actions to promote social-environmental responsibility engaged by financial institutions in the country;
- The third was signed with the Ministry of Social Development and Fight against Hunger (MDS) for the implementation of financial inclusion actions and improvement of life quality for members of the program Family Allowance.

Other partnerships with private entities also extend and expand the network of financial inclusion. In 2004 the Central Bank signed an agreement with the Brazilian Service of Support for Micro and Small Enterprises (Sebrae), aiming the development of microfinance, particularly credit unions. In 2010, the Central Bank established a deal with the Brazilian Credit Union Organization (OCB), aimed at developing, strengthening and promoting socio-economic efficiency and effectiveness of the Brazilian credit unions.

The ultimate goal is to form a network that can work/apply efforts in coordination, stimulating the results.

Also, it is worth mentioning that in 2010 it was established a specific component within the Financial System Regulation Department on the Central Bank, with the objective of linking internal and external initiatives. Just as an example, 15 different departments of the Central Bank were at some point involved in the preparation of the "I Financial Inclusion Report".

DOMESTIC COOPERATION IN THE PHILIPPINES

Relevant government institutions, including the regulators are increasingly consulting and collaborating with each other, thus fostering synergy in terms of financial inclusion objectives/initiatives. Presently, some government institutions are undertaking their own financial inclusion initiatives within their jurisdiction and as their legal mandate allows. For example, the finance ministry (Department of Finance), which spearheaded credit policy reforms and the formulation of the National Strategy and Regulatory Framework for Microfinance, together with the Insurance Commission are working on establishing an enabling environment for micro-insurance to address the need of the low income segments for adequate risk protection. Another example is the Philippine ministry of foreign affairs (Department of Foreign Affairs), which advocates microfinance and financial inclusion in international fora like the APEC. To ensure compatibility of objectives and complementarity of initiatives, the BSP aims to advocate the establishment of a national financial inclusion strategy.

BIBLIOGRAPHY AND SOURCES

BIBLIOGRAPHY

- Bangko Sentral Ng Philipinas (2011), Updated Anti-money laundering rules and regulations, Office of the Governor, circular No 706, www.bsp.gov.ph/downloads/regulations/attachments/2011/c706.pdf
- Bester, H., *et al* (2008), Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines. The FIRST Initiative. The World Bank, Washington, DC www.cenfri.org/documents/AML/AML_CFT%20and%20Financial%20Inclusion.pdf.
- CGAP (2011), "Regulating Banking Agents", Focus Note 68 www.cgap.org/sites/default/files/CGAP-Focus-Note-Regulating-Banking-Agents-Mar-2011.pdf
- CGAP (2011a), "Bank Agents: Risk Management, Mitigation and Supervision", Focus Note 75 www.cgap.org/sites/default/files/Focus-Note-Bank-Agents-Risk-Management-Mitigation-and-Supervision-Dec-2011.pdf
- Chatain, P-L., *et al* (2009), Preventing Money Laundering and Terrorist Financing: A Practical Guide for Bank Supervisors, The World Bank, Washington, DC http://lnweb90.worldbank.org/ext/epic.nsf/ImportDocs/823A21EF2A4AA930752575DD00351A9B?opendocument&query=PH
- Chatain, P-L., *et al* (2011), Protecting Mobile Money Against Financial Crime: Global Policy Challenges and Solutions. The World Bank, Washington, DC http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2011/03/10/000333037_20110310000727/Rendered/PDF/600600PUB0ID181Mobile09780821386699.pdf
- Chatain, P-L., *et al* (2008), "Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing", Working Paper 146. The World Bank, Washington, DC http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf.
- Collins, D., *et al* (2009), Portfolios of the Poor: How the World's Poor Live on $2 a Day, www.portfoliosofthepoor.com/index.asp
- Consultative Group to Assist the Poor (CGAP). 2009. Financial Access 2009: Measuring Access to Financial Services around the World. CGAP, Washington, DC, www.cgap.org/gm/document-1.9.38735/FA2009.pdf
- De Koker, L. (2006), "Money laundering control and suppression of financing of terrorism: some thoughts on the impact of customer due diligence measures on financial exclusion", *Journal of Financial Crime*, vol 13(1). Emerald. pp. 26-50.

- De Koker , L. (2009) "Identifying and Managing Low Money Laundering Risk: Perspectives on FATF's Risk-Based Guidance", *Journal of Financial Crime,* vol 16(4), pp. 334-352, www.emeraldinsight.com/journals.htm?articleid=1816893
- De Koker, L. (2009a) "The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa: Findings and Guidelines", *2009 Journal of Money Laundering Control,* vol 12(4), pp. 323-339, www.emeraldinsight.com/journals.htm?articleid=1817094
- De Koker, L. and Symington, J. (2011), Conservative compliance behaviour: drivers of conservative compliance responses in the South African financial services industry, Centre for Financial Regulation and Inclusion (CENFRI), www.gpfi.org/knowledge-bank/case-studies/global-standard-setting-bodies-and-financial-inclusion
- Demirguc-Kunt A. and Klapper, L.(2012), "Measuring Financial Inclusion: the Global Findex", *World Bank Policy Research*, WP 6025 http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTRESEARCH/EXTPROGRAMS/EXTFINRES/EXTGLOBALFIN/0,,contentMDK:23147627~pagePK:64168176~piPK:64168140~theSitePK:8519639,00.html
- G20 Financial Inclusion Experts Group (2010), Principles for Innovative Financial Inclusion, www.g20.utoronto.ca/2010/to-principles.html
- IFAD (2006), Remittances strategic and operational considerations, www.ifad.org/ruralfinance/pub/remittances.pdf
- Isern, J., and L. de Koker. (2009). "AML/CFT: Strengthening Financial Inclusion and Integrity." Focus Note 56. CGAP, Washington, DC http://www.cgap.org/publications/amlcft-strengthening-financial-inclusion-and-integrity
- PR Newswire (2012), "Digicel Launches World's First Biometric Identification System For International Money Transfers" http://betanews.com/newswire/2012/06/19/digicel-launches-worlds-first-biometric-identification-system-for-international-money-transfers/
- Solin, M., and Zerzan, A. (2010) "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks", *GSMA Discussion Paper*, GSMA, London
- State Bank of Pakistan (2011), "Branchless Banking Regulations for Financial Institutions", *Banking Policy and Regulation Department (BPRD) circulars,* No 09 of 2011, www.sbp.org.pk/bprd/2011/C9.htm
- Todoroki, E., Vaccani, M. and Noor, W. (2009), "The Canada-Caribbean Remittance Corridor: Fostering Formal Remittances to Haiti and Jamaica through Effective Regulation", *World Bank Working Paper,* No 163,The World Bank, Washington, DC http://publications.worldbank.org/index.php?main_page=product_info&products_id=23110
- Todoroki, E., *et al* (forthcoming), Evolving Remittance Markets: Lessons Learned from Regulating and Supervising Remittance Service Providers, World Bank, Washington, DC

- Wolfsberg (2008), Wolfsberg Frequently Asked Questions ("FAQs") on Politically Exposed Persons ("PEPs"), www.wolfsberg-principles.com/pdf/Wolfsberg_PEP_FAQs_(2008).pdf
- Wolfsberg (2009), Statement on AML Screening, Monitoring and Searching, www.wolfsberg-principles.com/pdf/Wolfsberg_Monitoring_Screening_Searching_Paper_(2009).pdf
- World Bank, Outlook for Remittance Flows 2012-14, Migration and **Development** Brief 17, December 2011, http://siteresources.worldbank.org/TOPICS/Resources/214970-1288877981391/MigrationandDevelopmentBrief17.pdf
- World Bank (2012), *World Development Indicators database,* World Bank Washington.
- World Bank (2012a), *Migration and Development Brief*, Nr. 18, World Bank, Washington
- World Bank (2012b), *General guidelines for the development of Government Payment Programs*, World Bank Washington, http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/282044-1323805522895/WB_2012_Guidelines_10_11_12.pdf
- World Bank (2012c), 2012 Information and Communications for Development, Maximizing Mobile, World Bank, Washington, http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTSDNET/0,,contentMDK:23241724~menuPK:64885113~pagePK:7278667~piPK:64911824~theSitePK:5929282,00.html
- World Bank (*n.d.*), *Global Financial Inclusion (Global Findex) Database,* World Bank Washington, http://go.worldbank.org/1F2V9ZK8C0, accessed December 2012.
- World Savings Banks Institute (2009), Anti Money Laundering and Combat Financing Terrorism Rules and the Challenge of Financial Inclusion: WSBI Experience and Proposals to FATF, WSBI, Brussels www.wsbi.org/uploadedFiles/Position_papers/0565%20updated.pdf

RELEVANT FATF DOCUMENTATION:

- FATF Guidance on the Risk-Based Approach to Combat Money Laundering and Terrorist Financing – High Level Principles and Procedures (series of Guidance published between June 2007 and October 2009 by the FATF in collaboration with the professions that are subject to AML/CFT obligations under the international Standards, see www.fatf-gafi.org); www.fatf-gafi.org/documents/riskbasedapproach/
- FATF (2008), Guidance on Capacity Building for Mutual Evaluations and Implementation of the FATF Standards within Low Capacity Countries, FATF, Paris. www.fatf-gafi.org/documents/documents/guidanceoncapacitybuildingformutualevaluationsandimplementationofthefatfstandardswithinlowcapacitycountries.html
- FATF (2010), FATF Report on Money Laundering Using New Payment Methods, FATF, Paris, www.fatf-gafi.org/documents/documents/moneylaunderingusingnewpaymentmethods.html
- FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, www.fatf-gafi.org/recommendations.

- FATF (2013), National Money Laundering/Terrorist Financing Risk Assessment, FATF, Paris.
- FATF (2013a), Guidance on PEPs, FATF, Paris, forthcoming.
- FATF (2013b), Guidance on New Payment Products and Services, FATF, Paris, forthcoming.

OTHER USEFUL SOURCES:

- Boston University (*n.d.*), Financial inclusion Guide, www.bu.edu/bucflp/initiatives/financial-inclusion-guide/, accessed November 2012.
- CGAP (2010), Notes on Regulation of Branchless Banking in the Philippines, CGAP, Washington, DC, www.cgap.org/gm/document-1.9.42402/Updated_Notes_On_Regulating_Branchless_Banking_Philippines.pdf
- CGAP (2012), Financial inclusion and the linkages to stability, integrity and protection: insights from the South African experience, CGAP, Washington, DC www.cgap.org/sites/default/files/I-SIP%20Report_1.pdf
- Basel Committee on Banking Supervision (2001), Customer Due Diligence for Banks. Basel Committee on Banking Supervision, BCBS, Basel www.bis.org/publ/bcbs85.htm
- Basel Committee on Banking Supervision (2010), Microfinance activities and the Core Principles for Effective Banking Supervision, Bank for International Settlements, BCBS, Basel www.bis.org/publ/bcbs175.pdf

