ASIA/PACIFIC GROUP ON MONEY LAUNDERING

WORLD BANK

FINANCIAL ACTION TASK FORCE

*FATF Guidance*

# Anti-money laundering and terrorist financing measures

and

# Financial Inclusion

*June 2011*


# THE FINANCIAL ACTION TASK FORCE (FATF)

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 and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. 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

# Executive summary

The promotion of well regulated 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 financial system. The FATF has therefore prepared a Guidance paper to provide support to countries and their financial institutions 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 that are relevant when promoting financial inclusion and to lay out the flexibility that the Standards offer, in particular regarding the risk-based approach (RBA), thus enabling jurisdictions to craft effective and appropriate controls.

The Guidance paper has been developed within the framework of the 2003 version of the FATF Standards. It is non-binding and does not override the measures applied by national authorities.

There are many reasons (unrelated to AML/CFT measures) why financially excluded and underserved groups may not be able to take advantage of mainstream financial service providers. This Guidance paper focuses on ensuring that AML/CFT controls do not inhibit access to well regulated financial services for financially excluded and underserved groups, including low income, rural sector and undocumented groups. It extensively explores the initiatives to address financial inclusion within the AML/CFT context taken in developing countries, since this is where the challenge is the greatest, but it also considers examples of action taken in developed countries also. .

The Guidance is based on the important assumption that financially excluded and underserved groups, in both developing and developed countries should not be *automatically* classified as presenting a lower risk for ML/TF, but could be lower risk depending on the various risk factors.

The Guidance reviews the different steps of the AML/CFT process (Customer Due Diligence, record-keeping requirements, reporting of suspicious transactions, use of agents, internal controls), and for each of them presents how the Standards can be read and interpreted to support financial inclusion.

- *Customer Due Diligence.* With regard to customer identification, financial institutions may be able to apply differentiated CDD measures according to the profile of the (future) customer. In relation to wire transfers, a so-called "progressive" or "tiered" CDD approach can be applied. This may imply for undocumented people access to financial services with very limited functionalities, with access to broader services being allowed only if the customer is able to provide further identification data. As far as customer verification is concerned, the FATF requirement for "reliable, independent source documents, data or information" can extend to accepting a broad range of IDs and innovative IT solutions can also provide reliable identifiers. Countries should nevertheless remain mindful of the exposure of certain of these alternative acceptable IDs to fraud and abusive practices.

Simplified CDD measures can be applied in cases where there is a demonstrated low ML/FT risk, but this should in no case amount to an exemption from or absence of CDD. Financial institutions may apply simplified CDD measures based on an assessment of ML/FT risks and other risk factors (*e.g.,* types of customers, countries). Different levels of control will be designed and implemented according to the different categories of risks identified.

- *Record-keeping of CDD data and transactions.* The information on the identification document(s) does not always require the retention of a photocopy and electronic storage is acceptable, which is particularly useful in the context of mobile phone banking.

- *Ongoing due diligence and business relationship monitoring* have to be performed through manual or electronic scanning. A risk-based approach is allowed, with the degree of monitoring being based on the risks associated with a customer, an account, and/or the products or services used. Regulatory authorities should be mindful and give due weight to determinations (*e.g.,* any monetary or other thresholds set) made by financial institutions.

Monitoring to detect unusual, potential suspicious transactions is required, with any actual suspicion leading to an obligation to report, regardless of any threshold or exception. When serving low income and low risk customers, financial institutions will need to balance their assessment of ML/TF risks with their technical capabilities and the level/type of information available on customers. Simplified CDD could be mitigated by closer transaction monitoring, acknowledging however that an absence of sufficient information due to too little CDD could make monitoring meaningless.

- *Report of suspicious transactions.* The risk-based approach will enable financial institutions to direct additional resources at higher risk areas, but once a suspicion has been formed, RBA is not applicable.

- *Use of agents.* Agents are viewed by the FATF as an extension of the financial services provider. Consequently, the conduct of CDD by these agents is treated as if it were conducted by the principal financial institution. The national practices for licensing or registration of agents differ significantly. In the case of remittance services, the obligation to license or register agents can consist, at a minimum, of a requirement for the principal business to maintain a current list of agents which must be made available to the designated competent authority.

The fact that agents act as an extension of the principal financial institution means that the AML/CFT processes and documentation are those of the principal. However, it is crucial to take into account the potential practical limitations faced by retailers (*e.g.,* small shops). The challenges related to the identification and verification of customers' information will vary according to the agents' ability to conduct CDD measures.

Supervision and oversight will primarily focus on the principal financial institution, but could include onsite oversight visits to agents. The degree of monitoring of the agents will be based on the perceived risks, both external and internal, associated with the agent, such as the products or services being provided, the location and the nature of the activity.

- *Internal controls.* Financial institutions must develop an effective internal control structure, including suspicious activity monitoring and reporting and create a culture of compliance, ensuring that staff adhere to the financial institution's policies, procedures and processes designed to limit and control risks.

The FATF will continue to work to ensure that financial inclusion and AML/CFT objectives do not conflict and will keep financial inclusion issues on its agenda.

# *INTRODUCTION*
# BACKGROUND AND CONTEXT

## Preliminary remarks

1. The initiative for this guidance paper was launched under the FATF Presidency of Mexico, following the interest kindled by the Presidency of the Netherlands. In June 2010, the FATF agreed to have 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 inclusion1. FATF's interest in financial inclusion is driven by its objective of protecting the integrity of the global financial system, covering the largest range of transactions that pose money laundering and terrorist financing risks in the jurisdictions that have committed to the FATF Standards. In addition to the promotion of financial services that offset informal financial mechanisms secluded from the authorities' watch, FATF has also a strong interest in financial inclusion due to the fact that many of the countries that are part of the FATF network are jurisdictions that can be considered as emerging markets, developing countries, or Low Capacity Countries which benefit from clear guidelines and examples of implementation of AML/CFT requirements in cases that allow for certain flexibility. The APG Plenary in Singapore in July 2010 agreed to a FATF request that the APG Implementation Issues Working Group (IIWG), in partnership with the World Bank, work jointly with the FATF Working Group on Evaluations and Implementation (WGEI) to create a guidance paper, in response to international calls for FATF to consider AML/CFT requirements in the context of financial inclusion.

2. Insights have been sought from FATF members and observers but also more broadly from non FATF and APG participants (individual jurisdictions and other FSRBs) and the private sector through the FATF Private Sector Consultative Forum and beyond. The industry's involvement has included banks, savings banks, non-bank remittance operators, postal financial services, cooperatives, microfinance institutions, E-money businesses and mobile money providers. The World Savings Banks Institute (WSBI) has led the industry's involvement. The Consultative Group to Assist the Poor (CGAP) and the Alliance for Financial Inclusion (AFI) have also been associated to this project. A list of participants in this project is attached (see Annex 1).

3. The FATF believes that this guidance paper contributes very much to the common objective agreed by the G20. At the G20 Seoul Summit in November 2010, financial inclusion was prominently included in the Leader's Communiqué as well as emphasized as an important element of the Seoul Development Consensus and Financial Sector Reform agenda. The decision then was to launch the

[1] 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).

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" (the details of these Principles are provided in Annex 3) through multiple channels, including through standard-setting bodies that are encouraged to take account of these principles[2].

4. The 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.

5. After an extensive consultation with both the public and the private sectors (including a meeting hosted by the WSBI in Brussels on 5 and 6 May 2011), this Guidance paper was adopted by the FATF at its June 2011 Plenary. It was endorsed by the APG at this July 2011 annual meeting.

## Scope of the Guidance Paper

6. This Guidance paper has been developed within the framework of the FATF Standards as agreed and adopted in 2003. The drafting of this Guidance has been inspired by the lessons learnt by the FATF and the other assessment bodies during the assessment process started in 2005. The objective of the paper has not been to engage into a debate on the actual contents of the Standards but to look into the existing requirements that are the most relevant when discussing the linkage between AML/CFT policies and the financial inclusion objective. The current review of the FATF Standards[3] is therefore not discussed in this paper although references, where relevant, are made to some ongoing FATF work. The paper finally refers to other initiatives that the FATF has already launched that have some important linkages with financial inclusion[4].

## Objectives of the Guidance

7. The paper primarily aims at supporting efforts among competent authorities, across sectors and across jurisdictions that promote the complementarity of AML/CFT and financial inclusion. It also aims to support the development of a common understanding of the FATF Standards that are relevant when promoting financial inclusion and explicit the flexibility they offer, in particular the FATF risk-based approach. Finally, it shares countries' experiences and initiatives to address financial inclusion within the AML/CFT context.

8. This 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 following principles:

---

[2] 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.

[3] In October 2009, the FATF started a focused review of its Standards to ensure that they remain up-to-date and relevant and to benefit from lessons learnt from implementing and evaluating the current standards. This review was still ongoing at the time this paper was finalised.

[4] The FATF continues for instance working on the issue of "New Payments Methods", including the issue of agents and the challenges caused by their supervision and their regulation.

- Financial exclusion undermines the effectiveness of an AML/CFT regime. A country's level of financial inclusion and initiatives to expand financial inclusion should be considered when the effectiveness of their AML/CFT regime is assessed;
- The assessment of the application of the risk-based approach should take account of the nexus between financial integrity and financial inclusion and the cross-reinforcement between these two objectives.

9. This Guidance focuses on financially excluded and underserved groups, including low income, rural and undocumented persons. The Guidance considers experiences in both developed and developing countries, although the Guidance explores more extensively the initiatives taken in developing countries as it is where the challenge is the greatest. Since there is a distinction to be made between developing and developed countries 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 different range of situations that jurisdictions should be able to refer to depending on their level of economic development (see Annex 4 for examples of countries' actions to support financial inclusion).

## Target Audience

10. There are two main target audiences for the Guidance:

i. AML/CFT regulators and supervisors tasked with implementing the FATF Standards, including but not exclusively those with a mandate for financial inclusion;

ii. 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.

11. Many aspects of this document may also be useful to a broader audience including organizations bringing support to financially excluded and underserved groups[5]; those engaged in providing technical assistance; and other international stakeholders dealing with the subject of financial inclusion.

## Status and Content of the Guidance Paper

12. This Guidance is non-binding. It does not lower the FATF Standards but is in line with the flexibility provided in the Standards with regards to ML/TF risks. It is not intended to provide a single model for promoting financial inclusion in the AML/CFT context but seeks to provide experiences that jurisdictions and individual businesses may wish to consider. A variety of country experiences exist to address a variety of situations and economic circumstances. Since differing factors come into play to "exclude" certain sectors, different formats must be adopted to address the factors that currently act as barriers.

13. This guidance is intended to assist jurisdictions 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 seeks to provide support in designing AML/CFT measures that meet the goal of financial

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

inclusion without compromising the measures that exist for the purpose of combating crime. Greater financial inclusion can increase the effectiveness of AML/CFT measures. However, strategies to move the unbanked from cash to electronic transactions must be well thought through, in order not to trigger a push back and result in even greater use of cash for informal financial services. Both goals need not be seen as opposing, especially if implied risks in innovative products are adequately taken into account.

## Sources of the Guidance Paper

14. This Guidance provides the general framework to assist jurisdictions in implementing a proportionate AML/CFT system in the context of financial inclusion that is commensurate with their ML/TF risks. 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 (see Annex 2).

# CHAPTER 1
# Statement of the problem

## What is Financial Inclusion?

15. While there is a growing consensus regarding the importance of financial inclusion, the same consensus does not exist around its definition, which 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 is about providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural and undocumented persons, who have been underserved or excluded from the formal financial sector. It is also, on the other hand, about making a broader range of financial services available to individuals who currently only have access to basic financial products. Financial inclusion can also be defined as ensuring access to financial services at an affordable cost in a fair and transparent manner. For AML/CFT purposes, it is important that these financial products and services are provided through financial institutions subject to adequate regulation in line with the FATF Recommendations.

16. Low income people generally have basic financial needs, although diversified as far as the type of financial service is concerned. For example, low income or handicapped persons and those in rural areas of developing countries may need a remittance agent location close to home or a bank branch or an agent location where they can deposit small amounts of money for safe keeping. They may need a micro loan to pay for fertilizer for planting seeds. Insurance programs are still limited for the financially excluded although micro-insurance might provide them with a safety net when they face adverse situations.

## State of Financial Inclusion

17. More than half the world's adult population lack access to credit, insurance, savings accounts, and other formal financial services[6]. The problem goes further if focused on the poor people living on less than USD 2 per day, as their income is not only low but also irregular and are therefore more

[6] These figures should be read keeping in mind that access to sophisticated financial services (*e.g.,* the presence of a bank account at a financial institution) may not be the ultimate objective and that financial inclusion can be achieved through other means.

vulnerable to external shocks and uncertainties of their cash flows[7]. Less than 10% of the people who live with under USD 2 a day have access to formal financial services.

18. The number of unbanked adults is estimated to be 2.7 billion (72 percent of adults) in developing countries and 160 million (19 percent of adults) in developed countries[8]. It is estimated that 1.4 billion people, or one quarter of the population of the developing world, lived below an absolute poverty level of $1.25 a day in 2005[9]. More than 215 million people (or 3% of the world's population) live outside their countries of birth and sent an estimated $325 billion to developing countries in 2010[10].

## The Diversity of the Financially Excluded and Underserved Groups

19. Disadvantaged and other vulnerable groups, including low income households, handicapped, individuals in rural communities and undocumented migrants, in both developed and developing jurisdictions, are more likely to be excluded from the formal, regulated financial sector. The underserved are those who currently have access to financial services but in a limited manner. For example, someone may have access to a money service business, but not to a bank. Underserved may also mean that you technically have access, but you are not using it because of other barriers such as problems in meeting the documentary and other requirements, non-awareness, wrong 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 likely to be required to address this diversity. For an illustration of the situation with regard to financial inclusion in different countries, see Annex 5.

## Challenges of Financial Exclusion

20. There are many reasons why individuals may not take full advantage of mainstream financial service providers. For example, there may be a cultural mistrust of mainstream financial institutions; these individuals may come from countries where banks are not safe places to deposit funds or may be sources of information (or mis-information) for government authorities in repressive regimes. Another primary reason may be lack of understanding or familiarity with traditional financial services. There may be language barriers, especially with immigrant populations. And, in rural areas but even in urban areas, ready access to services may not be available. On the other hand, there may be some individuals who have mis-managed financial services in ways that make them higher risk. For example, individuals may have exceeded account limits so frequently that they become ineligible for standard banking products and require special programs to help them understand how to manage a basic financial product. And finally, it is important to recognize that public officials can sometimes take steps designed to "protect" those who are disadvantaged when those steps may actually become barriers that actually restrict access to financial services. For example, steps that add to the costs for prepaid products may make them less appealing to those living on the margin.

---

[7] G20 Financial Inclusion Experts Group's nine *Principles for Innovative Financial Inclusion*.

[8] Consultative Group to Assist the Poor (CGAP), *Financial Access 2009*.

[9] See the World Bank *Poverty Reduction and Equity*.

[10] See the World Bank *Migration and Remittances*.

21. The main obstacles to financial inclusion can be summarized as follows:

- Supply side
  - Outreach: low density areas and low income populations are not attractive for the provision of financial services and are not financially sustainable under traditional banking business models and corresponding regulatory requirements
  - Regulation: frameworks are not always adapted to local contexts
  - Business models: mostly with high fixed costs
  - Providers: limited number and types of financial service providers
  - Services: non-adapted products and services for low income populations and the informal economy
- Demand side
  - Irregular income
  - Frequent micro-transactions
  - Lack of trust in formal banking institutions
  - Literacy level, lack of awareness and/or knowledge/understanding of financial products
  - Cultural obstacles (*e.g.,* gender and cultural values).

22. 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 limited in developing countries. The key is finding alternative delivery channels that work for specific contexts and which may differ depending on the target audience. It also relates to changing financial habits. In that respect, one successful approach is to focus on changing how government payment such as wages, pension, and social and medical benefits are delivered in both developed and developing countries.

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 for paid subsidies through electronic transfers. For example, the coverage of the ~~"O~~*portunidades*" Program was 35% (2.3 million users) as of December 2010. Regarding this program, there are two mechanisms to pay subsidies: 1) for areas with banking infrastructure, the government transfer resources to a banking account. 2) For areas without banking infrastructure, the government transfer resources to a prepaid card and install Points of Sale in the governmental convenience stores located in these areas.

23. 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 requirement meant that services for those existing customers who could not provide the necessary documents had to be terminated. In other instances it may mean that potential customers were not able to enter the formal financial system.

24. 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 is not the magic wand towards fully inclusive financial sectors, but would be a milestone towards building an enabling framework[11]. At the same time, one cannot ignore the fact that financial exclusion is a ML/TF risk and that financial inclusion can contribute to a more effective AML/CFT regime (see below).

## What interaction has there been between financial inclusion and AML/CFT policies?

25. 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 Financial Sector Reform and Strengthening (FIRST) study to consider the impact of AML/CFT in five developing countries. The report was published in 2008[12].

> —The pursuit of financial inclusion and the pursuit of an effective AML/CFT regime are complementary and not conflicting financial sector policy objectives. The objective with financial inclusion is that individual clients, particularly low income clients currently excluded from using formal financial services, must be able to access and on a sustainable basis use financial services that are appropriate to their needs and provided by registered financial service providers. Without a sufficient measure of financial inclusion, a country's AML/CFT system will thus safeguard the integrity of only a part of its financial system – the formally registered part – leaving the informal and unregistered components vulnerable to abuse. Measures that ensure that more clients use formal financial services therefore increase the reach and effectiveness of the AML/CFT controls."
>
> (*Source: Bester, H., D. Chamberlain, L. de Koker, C. Hougaard, R. Short, A. Smith, and R. Walker. 2008. Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines. The FIRST Initiative. World Bank, Washington, DC*).

26. Other studies, such as that conducted by the Consultative Group to Assist the Poor (CGAP) in 2009[13], concluded that AML/CFT measures can negatively affect access to, and use of, financial services if those measures are not carefully designed**.**

27. It is acknowledged at the same time that financial exclusion works against effective AML/CFT policies. Indeed the prevalence of a large informal, unregulated and undocumented economy negatively affects AML/CFT efforts and the integrity of the financial system. Informal, unregulated and undocumented financial services and a pervasive cash economy[14] can generate significant money laundering and terrorist financing risks and negatively affect AML/CFT preventive, detection and

---

[11] CGAP (2009).

[12] Bester, H., Chamberlain, D., De Koker, L., Hougaard, C., Short, R., Smith, A., and Walker, R. (2008).

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

[14] FATF Recommendation 20 encourages countries to develop and use modern and secure techniques for conducting financial transactions that are less vulnerable to money laundering (including reducing reliance on cash).

investigation/prosecution efforts[15]. Dependence on mainly informal financial services also limits access to reasonably priced credit and slows country's development. If the funds are kept outside the formal system, there is a limited multiplier effect in the economy.

28. Promoting formal financial systems and services is therefore 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, international AML/CFT Standards 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.

29. 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 (see Annex 6 for more details). 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 (see below).

## Balancing AML/CFT Requirements and Financial Inclusion

30. AML/CFT obligations can increase the cost of doing business, which is transferred to customers, potentially discouraging some from using the formal financial system, particularly if informal options are cheaper and equally reliable.. A customer lacking a government-issued form of identification, for example, may result in a financial institution using 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 amounts to an additional barrier to financial inclusion, as they can be consequently deprived of any access to financial services[16].

31. The more attractive the underground economy is for legitimate transactions, the more available that market is for illicit transactions. As a result, these alternative or underground providers become a ready conduit for illegitimate transactions that are undetectable to governmental authorities and in turn 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. Experience shows however that, against this background, regulators, financial service providers and ultimately customers face major challenges that are further analysed in Chapter 2.

[15] Moving cash transactions from the informal to the formal financial system makes it easier to detect and combat money laundering and terrorist financing. The audit trail is increased and the flow of money used for money laundering and terrorist financing becomes traceable.

[16] 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

32. 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 of money laundering and terrorist financing 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 address domestic circumstances. Countries may also choose to use a risk-based approach (as defined by the FATF) to build their AML/CFT regime that addresses the most pressing ML/TF risks while taking into account the importance of financial inclusion, both from an AML/CFT perspective as well as from a social policy point of view.

33. 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 have taken advantage of a risk-based approach when implementing their AML/CFT requirements. Rather, most countries have introduced a uniform approach with the same AML/CFT requirements applicable to all financial institutions, products and services. This may create a problem for smaller financial institutions with limited financial products and services since they have to meet the same AML/CFT requirements as larger financial institutions with a broader range of products and services across borders. At the customer level, customers whose financial transactions are small and limited have to meet the same customer due diligence requirements as other customers who may conduct large, frequent transactions.

34. A clear and precise explanation of the core elements of the FATF Standards and its exact contents supports countries' efforts to tailor their AML/CFT regimes domestically and develop an AML/CFT framework that fosters financial inclusion. This Chapter (i) offers some explanation of the most relevant elements of the Standards, (ii) provides possible models of innovative legislation and (iii) gives examples of business practices that can help to promote better financial inclusion.

# II. Overview of the Risk-Based Approach of the FATF17

35. The FATF Recommendations contain language that permits countries to some degree to adopt a risk-based approach to combating money laundering and terrorist financing[18]. That language also authorises countries to permit financial institutions to use a risk-based approach to discharge certain of their AML/CFT obligations. By adopting such an approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This allows resources to be allocated efficiently. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, so that all financial institutions, customers, products, etc. receive equal attention, or that resources are targeted, but on the basis of factors other than the assessed ML/TF risks. This can inadvertently lead to a 'tick box' approach with the focus on meeting regulatory needs rather than combating money laundering or terrorist financing. Further, the risk-based approach avoids having excessive and unnecessary requirements that hinder financial inclusion, as described in chapter 2, reducing the scope of transactions conducted through the informal financial system, away from regulatory and supervisory oversight.

36. The general principle of a RBA is that where there are higher risks countries should 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. The application of a risk-based approach requires countries to take appropriate steps to identify and assess the ML/TF risks for different market segments, intermediaries, and products on an ongoing basis. The principle of a RBA applied to AML/CFT matters is very relevant for countries that wish to build a more inclusive financial system that can respond to the need of bringing the financially excluded (who may present a lower ML/TF risk) into the formal financial sector. It is broadly recognised that this approach requires significant domestic consultation and strong cross-sector dialogue[19].

37. The FATF acknowledges the fact that the application of a risk-based approach to terrorist financing has both similarities and differences compared to money laundering. They both require a process for identifying 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

---

[17] 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).

[18] In the context of the review of its Standards, the FATF is considering a single comprehensive statement on the RBA, which could be incorporated into the FATF Standards as a new Interpretative Note dedicated to the RBA. The proposed draft Interpretative Note would comprise the following elements: (i) a statement on the basic principles and objectives of a risk-based approach; (ii) the obligations and decisions for the countries and (iii) the obligations and decisions for financial institutions and DNFBPs.

[19] This guidance paper does not examine the challenges a country may face to conduct risk and threat assessments and the reader should refer to the guidance paper to be published by the FATF and referred to as "Guidance on Risk and Threat Assessment". This Guidance paper will address the challenges that countries face in identifying and assessing the ML/TF risks of certain of their financial institutions or financial activities when considering exempting them from AML/CFT requirements. This guidance paper aims at defining the different concepts of "risk", "threat" and "vulnerability".

considerations such as the relatively low value of transactions involved in terrorist financing, or the fact that funds can come from legal sources. This Guidance primarily addresses the risk of money laundering, leaving methods and efforts to detect terrorist financing to national authorities in close interaction with the industry[20].

38. Finally, it is important to note 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.

# III. The flexibility offered by the international standards in justified low risk scenarios: the exemptions

39. When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, the FATF Standards allow a country to decide that the application of anti-money laundering measures is not necessary, either fully or partially. In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may also decide not to apply some or all of the Forty Recommendations to some of the financial activities as defined by the FATF.

## *3.1. The non application of AML/CFT requirements to certain financial activities or the "de minimis" exception*

40. As permitted by the FATF standards, a country may take risk into account, and may decide to limit the application of AML/CFT measures to certain financial institutions or activities provided that certain conditions are met.

***41. What are these financial institutions or activities*?** In defining financial institutions, the FATF provides a list of financial activities or operations to be covered for AML/CFT purposes.

**FATF definition of "financial institutions"**

*Financial institutions*[21] means any person or entity 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.[22]
2. Lending.[23]
3. Financial leasing.[24]

[20] See in that respect footnotes 17 and 19.

[21] For the purposes of Special Recommendation VII, it is important to note that the term *financial institution* does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.

[22] This also captures private banking.

[23] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

**FATF definition of "financial institutions"**

4. The transfer of money or value.[25]
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, CDs, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (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[26].
13. Money and currency changing.

42. Any of these activities can potentially be fully or partially exempted from AML/CFT obligations under certain conditions.

43. ***What are the conditions to be met?*** The FATF definition of financial institution includes the following regarding exemption from the FATF Recommendations:

"When a financial activity 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 a low risk of money laundering or terrorist financing, a country may decide that the application of AML/CFT measures is not necessary, either fully or partially".

44. This language is broad and there is no guidance, within the definition, regarding how such an exemption is expected to be implemented. In particular the notion of "financial activity carried out on an *occasional and very limited basis*" leaves some room for interpretation. Countries that opt for such an exemption must be able to make and demonstrate the correlation and cause and effect relationship between, on the one hand, the very limited and occasional nature of the financial activity and, on the other hand, the assessed low level of ML and TF risk. When a country decides to exempt certain persons from AML/CFT requirements where such persons engage in financial activity on an occasional or very

---

[24] This does not extend to financial leasing arrangements in relation to consumer products.

[25] This applies to financial activity in both the formal or informal sector *e.g.* alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It 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 Interpretative Note to Special Recommendation VII.

[26] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

limited basis, the onus is on the country to justify that the general conditions set out in the FATF standards are met.

45. Only a few countries have undertaken risk assessments before exempting a sector, fully or partially. In most countries, the current exemptions or limitations of the application of AML/CFT requirements to certain financial activities are essentially based on a "perception" of low risk because of the size of the activity or its nature (leasing, factoring companies, life insurance activities for instance) with no or very little evidence to support the risk ranking.

46. An important initiative to define the notion of "financial activity carried out in occasional or very limited basis" in a systematic way has been taken by the European Commission. Article 2(2) of the Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, establishes a flexibility[27] similar to the one set out in the FATF definition of financial institutions. Directive 2006/70/EC of 1August 2006,[28] in its Article 4, lays down implementing measures for Directive 2005/60/EC as regards 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. Using that legal ground, some EU countries have opted for such exemptions using the safeguards set out in the Directive of 1 August 2006. For instance, the Money Laundering Regulations 2007 in the UK foresee such a scenario.

**The Money Laundering Regulations 2007 (UK)**

**Schedule 2 - Financial activity on an occasional or very limited basis**

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 GBP 64 000;

(b) the financial activity is limited in relation to any customer to no more than one transaction exceeding 1 000 EUR, 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)[29];

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

---

[27] "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.

[28] 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.

[29] *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.

47. In France, for two business sectors, the competent authorities have exercised the option offered by the FATF Recommendations not to apply some or all of the anti-money laundering measures to certain natural or legal persons carrying out a financial activity on an occasional or very limited basis (according to quantitative and absolute criteria), such that there is little risk of money laundering. This option has been exercised for money changers and for insurance intermediaries. The French authorities have based the exemption thresholds (*e.g.,* 5% of total sales and EUR 1 000 per money-changing transaction) on the provisions of Article 4 of European Commission Directive No. 2006/70/EC mentioned above. To be eligible for the exemption, the total currency purchase and sale transactions in one fiscal year must be under EUR 50 000. The authorities have indicated that these criteria must be read cumulatively. For both money changing and insurance intermediation activities, the FATF considers that the combination of criteria or thresholds which condition the exemption, due to the accessory and limited nature of the financial activity, appear to adequately incorporate the notion of proportionality with regard to the applicability of the AML/CFT requirements. In particular, the combination of these criteria limits the scope of the exemptions concerned to situations in which the risk of money laundering or terrorism financing appears low. The exemption from the AML/CFT provisions is mainly expected to apply to tourist offices, hotels, travel agencies, businesses serving foreign travellers, etc. The French authorities have been required by the FATF to apply adequate monitoring of these exemptions.

48. ***How could this exception serve financial inclusion objectives?*** The underlying rationale of the exemption is that, based on the minimal amount of financial activity that is being undertaken and the related limited ML or TF risk, the business engaged in the activity (the example commonly cited is a hotel doing some minimal money exchange business for guests) is not to be considered as a financial institution that has to comply with the FATF Standards. It falls outside the scope of entities covered by the FATF Recommendations. No examples were provided of countries using this exemption in the context of a financial inclusion policy.

### *3.2. The non application of some or all Recommendations to financial institutions or the "general risk exemption"*

49. The FATF Standards allow countries to not apply some or all of the FATF Recommendations for financial institutions provided: a) this occurs in strictly limited and justified circumstances; b) it is based on a proven low risk of money laundering and terrorist financing, and c) it relates to a particular type of financial institution or activity.

50. In line with the FATF Standards, a country may decide to exempt a specific type of financial institution or activity (as listed in the Glossary of the FATF Recommendations) from certain or all of the AML/CFT obligations. The main challenges for countries will be to demonstrate the limited and justified circumstances that surround the activity and the associated low risk of ML or TF. The country will have to develop a credible methodology or use a developed methodology in order to meet this threshold[30].

51. This type of exemption (although it requires countries to develop a process, which seems reasonable considering the range and possible impact of the exemption) offers a degree of flexibility that countries have used very marginally. However, countries like Canada and Hong-Kong have

[30] See footnote 19.

developed an AML/CFT Risk Assessment Methodology (although not specifically designed to address financial inclusion, see Annex 7 for details).

52. ***Assessment bodies' guidance***. In addition to the "Guidance on Risk and Threat Assessment" that the FATF is currently drafting, the APG and the World Bank have also developed a national AML/CFT risk assessment template as part of the Strategic Implementation Planning (SIP) Framework (see Annex 8). The SIP has been developed to assist jurisdictions in implementing the recommendations of their mutual evaluation reports, including on the basis of a risk assessment of both the financial sector and the DNFBPs. APG members are using this template to assist in undertaking their national risk assessments. The World Bank and IMF have also developed other types of risk assessment tools which are being used by some APG members and non APG members. These assessment tools and methodologies are being refined based on feedback from users.

53. ***Other relevant experiences***. Where relevant, the information available elsewhere may also be used to more fully inform the country's knowledge of the sector under review and its exposure to ML/TF risks. The final decision on assessment of the actual risks and possible exemption from AML/CFT requirements should in all cases remain with the country.

54. Law enforcement investigations, reports to financial intelligence units, and regulator experience are important sources of information to assess ML/TF risks. Industry is also well placed to provide insight into operations that may be exposed to ML/TF risks. .

55. In relation to mobile money services, the GSMA has developed a Methodology for Assessing Money Laundering and Terrorist Financing Risk[31]. The Methodology elaborates a systematic approach for assessing the vulnerabilities of mobile money to ML/TF risks, understanding how these vulnerabilities could be exploited by money launderers and terrorists, and identifying appropriate and effective tools to mitigate identified risks. A variety of risk-mitigation processes are discussed. Measures that reduce the risk of ML/TF by consumers, for example, include establishing limits on accounts, transaction frequencies, and volumes and monitoring of transaction flows on the system level. By assessing risk both before and after such mitigating controls are in place, service providers and regulators can evaluate the appropriateness of such mechanisms. A risk assessment once such controls have been applied then becomes an input to the establishment of CDD requirements. In late 2010, SMART Communications in the Philippines employed the Methodology when engaging with the Central Bank (Bangko Sentral ng Pilipinas, or BSP) to discuss whether reduced KYC requirements for certain customers registering for SMART Money would be permissible when enhanced risk-mitigation measures were applied. SMART used the Methodology as a reference when defining these risk-mitigation mechanisms and when preparing a risk assessment to discuss with BSP. In early 2011, the BSP issued Circular 706 in which it instructed institutions "formulate a risk-based and tiered customer identification process that involved reduced Customer Due Diligence (CDD) for potentially low-risk clients and enhanced CDD for higher-risk accounts" and described the requirements for both reduced and enhanced CDD[32].

56. In relation to remittances, Western Union has also developed a risk methodology 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

[31] Solin, Marina, and Zerzan, Andrew (2010)

[32] See Bangko Sentral Ng Pilipinas (2011)

relevant, categories are used in various combinations to further tailor Western Union's efforts to its specific risks (see the details of the Western Union risk methodology in Annex 9).

57. Other players may be in the position to inform a country of the exposure to ML/TF risks of a given sector. 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 money services[33]. Countries may find this risk categorization helpful in informing their risk analysis domestically and develop 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., Zerzan, A., Noor, W., Dannaoui, N. and De Koker, L. (2011)

58. The GSMA has also identified potential vulnerabilities for the risk categories described above 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

[33] Chatain, P-L., Zerzan, A., Noor, W., Dannaoui, N. and De Koker, L. (2011). See also: Chatain, P-L., Hernández-Coss, R., Borowik, K. and Zerzan, A. (2008).

# IV. Read and understand the FATF Standards in the light of the financial inclusion objective

## *4.1. Requirement to carry out Customer Due Diligence (Recommendation 5)*

59. Under the FATF Standards, financial institutions[34] must perform due diligence in order to identify their clients and ascertain relevant information pertinent to doing financial business with them. Under AML/CFT legislation, CDD policy objectives are to ensure that financial institutions can effectively identify[35], verify and monitor their customers and the financial transactions in which they engage, in accordance to the risks of money laundering and terrorism financing that they pose.

60. It must be understood that the three core notions of "identification", "verification" and "monitoring" are interrelated and very closely associated in the FATF Standards. 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.

*Circumstances in which CDD must apply*

61. In line with the FATF Standards, all financial institutions that are subject to AML/CFT obligations are required to undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations36;
- carrying out occasional transactions above USD/EUR 15 000 or that are wire transfers above USD/EUR 1 000;
- 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.

62. A number of countries have introduced reduced CDD requirements to take into account the non-applicability of the FATF Standards (no CDD in cases of occasional transactions below USD/EUR 15 000 or that are wire transfers below USD/EUR 1 000).

---

[34] With some adaptation, the CDD and other requirements that are applicable to financial institutions also generally apply to the categories of designated non-financial businesses and professions (DNFBPs) pursuant to Recommendations 12 & 16.

[35] The FATF Standards do not allow financial institutions to keep anonymous accounts.

[36] It is noticeable that the FATF Standards do not define this notion. It is left to countries to decide the circumstances where such a business relationship occurs.

*CDD measures - general*

63. Given the transaction thresholds and other criteria noted above, the customer due diligence measures that are to be taken by institutions, professions and businesses subject to AML/CFT obligations are as follows:

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

b) Identifying the beneficial owner, and taking 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) Obtaining information on the purpose and intended nature of the business relationship.

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

64. Applying these CDD measures is challenging for financial service providers, particularly small financial institutions and those in low capacity countries[37]. It is essential to distinguish between identifying the customer and verifying identification. Customer identification consists of obtaining information on the identity of the (future) customer (at this stage, no identification documentation is collected). In contrast, the verification of the customer identification requires collecting some documentation or checking an independent source that authenticates the veracity of the information obtained from the customer.

65. Feedback from the industry highlights a number of practical problems regarding the identification and verification requirements. It happens that most of these difficulties arise under national legislative or regulatory requirements, and not the FATF Recommendations, which do not require for instance information to be gathered on matters such as occupation, income, address for normal risk customers. Although a passport or ID card is one of the methods used to verify the identity of customers in a majority of countries, it should be noted that the FATF Standards does allow countries to use other reliable, independent source documents, data or information.

*CDD measures – customer identification*

66. In the banking sphere, information on the identity of the customer generally consists of obtaining from the customer information on (1) legal name and any other names used; (2) correct permanent address; (3) telephone number and e-mail address; (4) date and place of birth; (5) nationality; (6) occupation, public position held and/or name of employer; (7) an official personal identification number or other unique identifier contained in an unexpired official document; (8) type of account and

[37] This paper does not address the challenges of the identification of the beneficial owner since it targets more the identification of legal persons and arrangements.

nature of the banking relationship; and (9) signature[38]. The FATF Standards do not specify the exact range of customer information (referred to by certain countries as "identifiers") that the businesses subject to AML/CFT obligations should collect to properly carry out the identification process. The list of customer identification information set out above represents common practice in many regulatory frameworks. Domestic legislation varies although the minimum customer information (purely CDD driven) tends to consist of name, date of birth, address and an identification number. Other types of information (such as the occupation, the telephone and e-mail address of the customer, etc.) seem more business driven and do not constitute core information to be collected.

67. Countries' laws or regulations generally do not distinguish the types of customer information to be collected on the basis of a risk-based approach although the FATF Standards allow this. In most cases, existing requirements seem to apply uniformly to all businesses and professions subject to AML/CFT obligations, with no differentiation based upon the profile of the customer or the customer's ability to produce or not some form of identification. This general statement needs however to be nuanced. Differentiated CDD requirements have indeed been introduced in some countries, 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). People opening such accounts are subject to a different range of CDD requirements.

68. Specific CDD rules are applicable to wire transfers. For all wire transfers, of EUR/USD 1 000 or more, ordering financial institutions are required to obtain and maintain the following information relating to the originator of the wire transfer: (i) the name of the originator; (ii) the originator's account number (or a unique reference number if no account number exists); and (iii) the originator's address (countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth). For domestic wire transfers the ordering financial institution may include only the originator's account number or a unique identifier with the message or payment form. This option for domestic transfers is only permitted if full originator information can be made available to the beneficiary financial institution and to appropriate authorities within three business days of receiving a request, and domestic law enforcement authorities can compel immediate production of it.

69. In relation to wire transfers for instance, countries may consider applying the so called "progressive or "tiered" KYC/CDD approach" whereby the transaction/payment limits vary based on the CDD; the better the CDD process, the higher the limits. This may imply for undocumented people access to very limited functionalities, with access to broader services (*e.g.,* higher limits, transfers including cross-border) being allowed only if the customer provides proof of identity and address. For example, in Canada, customer identification (and verification) is required for remittances of CAD 1 000 or above. Some remittance companies introduced a "progressive approach" to CDD where sending more than CAD 1 000 required customers to provide additional information including their occupation and source of funds. One remittance company implemented an internal scrutiny program which required the remittance company's head office to make a decision on whether to allow the transaction to proceed, should it exceed CAD7 500. Prior to making the decision, usually an interview is conducted to gain

[38] Examples of the types of customer information that can be obtained are set out in the paper entitled General Guide to Account Opening and Customer Identification issued by the Basel Committee's Working Group on Cross Border Banking to which the FATF Recommendations refer to.

further information about the sender and the funds, asking for example about the source of funds and requesting a copy of invoices being paid if the payment is a commercial transaction[39].

*CDD measures – verification of customer identification*

70. The FATF Standards require the financial institutions, and designated non-financial businesses and professions to verify the customer's identity using reliable, independent source documents, data or information. The FATF does not provide further guidance on what the degree of reliability and independence of such documentation should be, although its exposure to fraud and counterfeiting is an important criterion for countries to consider. It is understood that it is the primary responsibility of countries to domestically identify what can constitute "reliable, independent source documents, data or information" although financial institutions may also implement a risk-based approach to verification (having recourse to the principles of proportionality and risk mitigation).

71. The customer identity verification stage is, in all instances, described by the industry as the most difficult and burdensome to achieve and as being a strong disincentive from a financial inclusion perspective.

72. *Relying on a broader range of acceptable IDs*[40]. In order to address these challenges[41], the list of acceptable IDs in the verification process has been extended in some countries to include a broader range of documentation such 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.). Usually, local authorities allow such an approach in pre-defined types of business relationships and below account balance limits *i.e.,* using a risk-based approach (see examples of countries' provisions in that respect in Annex 10).

73. The Mexican authorities have established a flexible listing of legal documents accepted as official identification. Examples of documents issued by the Mexican authorities considered as valid for personal identification include the voting card, passport, professional charter, national military service card, consular registration certificate, military identity card, membership card to the National Institute of Older Persons, credentials and identification cards issued by the Instituto Mexicano del Seguro Social, driver's license, credentials issued by the federal, state and municipal governments, and other identifications documents approved by the banking supervisor. For foreign nationals the same documents apply as well as documentation from the National Migratory Institute which certifies identification.

74. In Switzerland, competent authorities in partnership with the private sector have examined ways to improve access to financial services by foreign illegal migrants. These migrants fall under the category of persons entering the country illegally (in the absence of valid visa/permits or authorizations) or those, with no valid documentation who remain in the country illegally. A Swiss Banking circular establishes that the official documentation generally possessed by illegal migrants meets the

---

[39] World Bank (2009)

[40] Besides relying on a larger range of IDs for costumer identification and verification, there are other approaches to "flexible" CDD requirements that the FATF promotes (*e.g.* costumer ID verification being postponed, remote account opening, etc.).

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

requirements of 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. In the US, reliance on *matricula consular* cards for migrant workers or other non U.S. persons, particularly migrant workers from Mexico, are being used as forms of identification.

75. In India, special provision has been made for low income customers under the AML/CFT guidelines, which provides for opening accounts for those persons who intend to keep balances not exceeding INR 50 000 (about USD 1 000) in all their accounts taken together, and where the total credits in all the accounts taken together is not expected to exceed INR 100 000 (USD 2 000) in a year. In such cases, if a person who wants to open an account is not able to produce the normal identification documentation, banks are expected to open an account, subject to: (i) introduction from another account holder who has been subjected to full CDD procedure. The introducer's account with the bank should be at least six months old and should show satisfactory transactions. A photograph of the customer who proposes to open the account and his address need to be certified by the introducer; or (ii) any other evidence as to the identity and address of the customer to the satisfaction of the bank.

76. For potential customers in rural areas, in the Philippines, a Barangay Certification, a certificate issued by the elected head of a village, is accepted as a proof of identification and residence. In Malaysia, 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.

77. Efforts to expand the range of reliable documentary types of identification have been supplemented in some developing countries by innovative IT solutions. Some countries are developing acceptable non-governmental and even non-documentary methods of verifying identification, such as a signed declaration from the community leader together with a photograph taken on a camera phone, biometrics or voice prints (such market-based solutions have been especially developed in the Fiji[42], Philippines and Malawi). Countries are also developing electronic multi-purpose forms of identification[43].

[42] For instance in 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 laborers). 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.

[43] 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 concept of "Universal Electronic Card is also widely discussed in Russia.

78. The Guidance issued by the Joint Money Laundering Steering Group[44] in the UK 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 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

79. *Exposure of alternative acceptable IDs to fraud*. Countries should remain mindful of the exposure of certain of these alternative acceptable IDs to fraud and abuse practices. Whether reliance can be placed on a letter from a village chief to verify the identity of the customer depends on the knowledge and integrity of the village chief. In some cases, village chiefs started to demand money for these "verification services". Although this may not represent a wide spread practice, it is important to ensure that alternative identification processes do not create new barriers that further undermine

[44] 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.

financial inclusion. Every method of verifying customer identification requires some basic due diligence and monitoring to ensure integrity and reliability.

80. In South Africa, in May 2010, the Financial Intelligence Centre issued an advisory to banks telling 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 only after verifying the authenticity of the document with the Department of Home Affairs.

81. *Risk mitigation*. Although the probability of occurrence of an identity fraud based on less stringent ID documentation might be potentially higher, the exposure of these financial services to ML or TF has to be taken into account. This is why a proper risk analysis is crucial to support the adoption of verification processes that are proportionate to the level of ML/TF risk.

*CDD measures – verification of customer identification in low risk scenarios*

82. The current FATF Standards allow for simplified CDD measures in cases where there is a low risk of money laundering or terrorist financing. The general rule is that customers must be subject to the full range of CDD measures. Nevertheless, the FATF recognises that there are circumstances where the risk of money laundering or terrorist financing is lower (*e.g.,* certain customers such as government administrations or enterprises, transactions or products such as life insurance policies within limited annual premiums, see below). In such circumstances it may be reasonable for a country to allow its financial institutions/DNFBPs to apply simplified CDD measures when identifying and verifying the identity of the customer. Such simplified measures are allowed based on a risk analysis conducted either at the country or the financial institutions' level.

83. *Simplified CDD measures decided at country's level*. Basic minimum AML requirements can coexist with a risk-based approach. Indeed, sensible minimum standards, coupled with scope for these to be enhanced when the risk justifies it, should be at the core of risk-based AML/CFT requirements. These standards should, however, be focused on the outcome (combating through deterrence, detection, and reporting of money laundering and terrorist financing), rather than applying legal and regulatory requirements in a purely mechanical manner to every customer.

84. In relation to all the CDD components, a reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanisms to be used to meet these minimum standards. Once this determination is made, the obligation to keep records on documents that have been obtained for due diligence purposes, as well as transaction records, need to be met. In other words, the record keeping requirement is not dependent on risk levels and all components of this requirement under Recommendation 10 are fully applicable (unless there is a complete exemption as referred to above).

85. Countries may consider, for instance, not creating an obligation to collect specific information to understand the purpose and intended nature of certain low risk business relationships on the basis that the purpose and nature of the relationship can be inferred from the types of transactions established (*e.g.,* access to basic financial services). This would not breach the FATF Standards, though it should be noted that such simplified CDD measures are not acceptable whenever there is a suspicion of ML or TF or specific higher risk scenarios apply.

86. Simplified CDD does not mean in any case exemption or absence of CDD measures[45]. Very few countries have introduced simplified CDD. In Mexico, for instance, the current AML/CFT legal provisions for banking institutions establish three levels of account activity (low transactional accounts, low-risk accounts, and traditional accounts) and corresponding AML safeguards. As defined, low transactional accounts[46] were implemented under a balanced risk-based approach scheme to allow an increased level of financial inclusion underpinned by adequate AML/CFT controls. Mexican financial authorities are working on a second stage with an increased number of levels and controls based on their transaction levels. The lowest transaction level includes a prepaid card (see Annex 6).

87. When the South African authorities considered developing products designed to serve the financially excluded or underserved, it was recognised that full CDD, in particular, obtaining and verifying a residential address 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. It therefore revised an exemption, called Exemption 17, to release financial institutions from verification requirements under the money laundering and terrorist financing regulations and hence provides for a form of simplified due diligence, in respect of 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-no formal addresses). The institutions still have to 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 business relationships and single transactions must not enable the customer to withdraw or transfer or make payments of an amount exceeding R 5000 (approximately USD 110) per day or exceeding R 25 000 (approximately USD 550) in a monthly cycle; further it 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 and Swaziland).

---

[45] Some countries have introduced exemptions that go beyond the FATF Standards and have been criticised for such an approach. For instance, many FATF Mutual Evaluation Reports adopted since 2005 raise this issue and request countries to remedy the approach that exempts financial institutions from carrying out CDD measures in scenarios that are not foreseen in the Recommendations. For instance, some, if not all EU countries have introduced a complete exemption from key elements of the CDD process for certain customers (*e.g.* credit institutions, financial services institutions, insurance companies, etc. from another EU member state or a third country that applies equivalent requirements and supervision). It happens that these countries have not conducted any form of risk analysis to justify such exemptions.

[46] This type of accounts is for natural persons whose monthly deposits do not exceed 2 000 UDIs (approx. USD 720.43). To comply with CDD requirements, the customer file must be integrated only with the client´s basic data (name, address and birth date) and do not require to maintain a copy of the documents. However, in the event that the accumulated amount of transactions exceeds the maximum allowed transactional level, the banking institution is obliged to either, obtain additional information or integrate a complete customer file, according to the new upgraded risk level and if necessary, submit STRs and report the authorities whenever a single transaction exceeds the threshold limit of USD 10 000. In addition, the account opening procedures may be completed at a banking branch or at a banking agent facility (*i.e.,* Telco agent, commercial retail and convenient stores, etc.).

- The balance maintained in the account must not exceed R 25 000 (approximately USD 550) at any time; further, the same person must not simultaneously hold 2 or more accounts which meet the criteria of the exemption with the same institution. In cases where a customer exceeds the account limits, the accountable institution[47] is then required under the exemption to conduct full CDD before completing any additional transactions associated with that customer,,s account.

88. 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. Currently, at least one in ten South African adults has an Mzansi account and one in six banked people are active Mzansi customers. 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). Mzansi contributed to the increase in the unbanked adults being banked; in 2008, almost two thirds of South African adults were banked, a sizable increase from just under four years earlier. 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.

89. In India, people without any acceptable form of identification (migrant labour etc.) are allowed to open a "small account" where (i) the aggregate of all credits in a financial year does not exceed Rupees 100 000 (approximately USD 2000), (ii) the aggregate of all withdrawals and transfers in a month does not exceed Rupees 10 000 (approximately USD 200), and; (iii) the balance at any point of time does not exceed Rupees 50 000 (approximately USD 1 000). None of these limits can be exceeded. The small account can be opened *only in the presence of the "designated officer" of the bank, in whose presence the individual has to affix his signature or thumb print and produce a self attested photograph*. No other document is necessary. The other conditions are as follows:

i. the designated officer of banking company, while opening the small account, must certify under his signature that the person opening the account has affixed his signature or thumb print in his presence;

ii. a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place[48];

---

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

[48] India indicates that there are a few bank branches which do not have core banking solution (*i.e.,* computerized and networked). Theoretically, it will be possible that through oversight or otherwise, amounts may be credited to such account and such amounts taken out or transferred before it is realized that the crediting itself should not have been allowed (as it may exceed the monetary limits or as it may be a foreign remittance). To prevent this, it is

iii. a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;

iv. a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through the production of officially valid documents, as referred to in sub-rule (2) of rule 9;and

v. foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents.

90. Initiatives to address the customer identification/identity verification challenges in other countries are described in Annex 10.

91. *Simplified CDD measures decided at financial institution's level*. The risk analysis carried out at the financial institution's level should identify the money laundering and terrorist financing risks that are relevant to the business as well as different risk indicators/factors, including the risk in relation to types of customers, countries or geographic areas, particular products, services, transactions or delivery channels[49].

92. Once this risk analysis has been carried out, businesses should design and implement controls to manage and mitigate these assessed risks, monitor and improve the effective operation of these controls; and record appropriately what has been done, and why. The appropriate approach is ultimately a question of judgement by senior management, in the context of the risks they consider their business faces. No system of checks will detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual firms and their customers with a realistic assessment of the threat of the firm being used in connection with money laundering or terrorist financing. In this scenario, the regulator must be able to institute its own validation process to test the risk assessment conducted by the financial institution.

93. It is important to highlight that there is no requirement, or expectation, that a risk-based approach must involve a complex set of procedures to put it into effect; the particular circumstances of the business will determine the most appropriate approach. Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know who their customers are, what they do, and whether or not they are likely to be engaged in criminal activity or to be conduit for proceeds of crime.

94. During 2004 the Financial Intelligence Centre in South Africa published a Guidance Note concerning the identification of clients. This Guidance Note was intended to assist accountable institutions and supervisory bodies with the practical application of the client identification

---

necessary to stipulate that small accounts can be opened only in branches that are part of the core banking solution which will prevent crediting of such amounts into the account.

[49] These categories of risk are described in more details in the FATF RBA Guidance referred to in Chapter 1 of the Guidance.

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.

95. The combination of 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 all relevant clients.

96. In the Regulations reference is made to the fact that accountable institutions must verify certain particulars against information which can reasonably be expected to achieve such verification and is obtained by reasonably practical means. This means that in these specific instances an institution must assess what information may be necessary in order to achieve verification of the particulars in question and the means by which it can be obtained. In the Regulations where the expressions such as "can reasonably be expected to achieve such verification" and "is obtained by reasonably practical means", the balance between the accuracy of the verification required on the one hand, and the level of effort invested in the means to obtain such verification on the other, has to be commensurate with the nature of the risk involved in a given business relationship or transaction.

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.

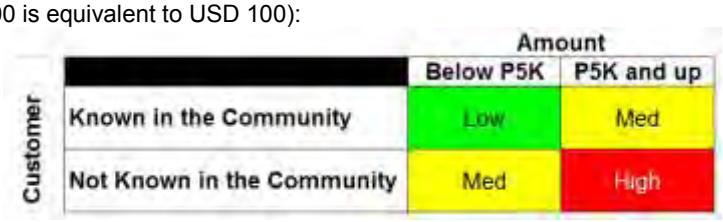
*Source: General Guidance Note Concerning Identification of Clients, South Africa, April 2004*

97. A risk assessment will often result in a stylised categorisation of risk: *e.g.,* high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional customer information and monitoring for each category, in a way that minimises complexity[50]. Examples of such assessments are as follows:

[50] Examples of the risks in particular industry sectors in the UK are set out in sectoral guidance and are available at www.jmlsg.org.uk.

**Case Study – Risk-Based KYC developed by Globe Telecom in the Philippines**

Part of our 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 will serve as basis for the three types of risk ratings: Low, Medium, and High.
Risk Rating KYC (P5 000 is equivalent to USD 100):




Full KYC 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: | | |
| Known in the community | Yes | No |
| Not known in the community | Yes | No if amount is less than P5,000 |
| | | Yes if amount is P5,000 and up |

98. The FATF has identified examples of customers, transactions or products that may present a lower risk of ML/TF and to which simplified CDD measures may be applied. Certain life insurance policies or pension schemes, for example, are lower risk financial products[51]. Simplified CDD may also apply to to electronic money on a non-rechargeable device with a maximum amount of USD/EUR 150, or a rechargeable device where the total amount transacted per year cannot exceed USD/EUR 2 500[52].

*Identification in non-face to face scenarios*

99. While face-to-face interaction is still relevant in certain types of banking activities (*e.g.,* private banking), it is not essential to many banking and non-bank relationships. Non face-to-face financial operations that may serve the undocumented and financially excluded population require

[51] *I.e,* life insurance policies where the annual premium is no more than USD/EUR 1 000 or a single premium of no more than USD/EUR 2500 or insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme. See the Interpretative Note to Recommendation 5.

[52] See in particular DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. In this context, "electronic money" means monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer.

specific verification processes which should not necessarily include submission of a conventional government-issued form of identification with photograph. Operators that supply online customer verification have expressed some concerns that in many countries, the current regulatory requirement that every transaction be verified against an ID is an inherent obstacle to the developments of these services and the related products[53].

100. 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 then cross-reference these against an acceptable third-party database and undertake additional electronic CDD measures. However, since the regulator feels this service model introduces higher ML risk, clients who use the non-face to face registration process cannot transact against their accounts for more than R1 000 (approximately USD 120) a day. The regulator therefore 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[54].

101. The process of reliance on third parties with respect to CDD is permitted under the FATF Standards (see provisions in relation to Recommendation 9). It can be broadly described as follows: a financial institution accepts a customer and 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. In such scenarios, financial institutions are required to satisfy themselves that a third party is adequately subject to AML/CFT regulation and supervision by a competent authority and has measures in place to comply with the CDD requirements. 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. In certain countries (such as Australia), consulates, embassies, police officers, licensed doctors, certain teachers, etc. can be third parties that financial institutions may rely upon to carry out some CDD functions. This model of business is not however available in all countries and, where available, are not being widely used on the basis that the ultimate responsibility for customer identification and verification should remain with the financial institution relying on a third party.

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

102. This requirement does not seem to raise concerns among the industry in the context of this guidance. A risk-based approach that would allow financial institutions/DNFBPs not to collect specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but to infer the purpose and nature from the type of transactions or business relationship established would be acceptable and in line with the FATF Standards (see comments above).

---

[53] It is worth mentioning that the FATF Standards allow financial institutions in non-face to face scenarios to verify the identity of the customer following the establishment of the business relationship (at not before or during the course of establishing a business relationship) provided that (i) the verification occurs as soon as reasonably practicable; (ii) this is essential not to interrupt the normal conduct of business and (iii) the money laundering risks are effectively managed.

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

*CDD measures - conducting ongoing due diligence and monitoring the business relationship (Recommendations 5 and 11)*

103. 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 used and these are scanned against national and international sanctions lists. The scanning process may flag a number of transactions for internal investigation. Transactions with values that exceed the normal value for that type of transaction, are often also flagged for internal investigation. 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.

104. The degree and nature of monitoring by a financial institution will depend on the size of the financial institution, the AML/CFT risks that the institution has, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach 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 perceived risks associate with the customer, the products or services being used by the customer and the location of the customer and the transactions. Monitoring methodologies and processes also need to take into account the resources of the financial institution.

105. 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 counter-measures are reasonable and adequately documented.

106. Monitoring under a risk-based approach allows a financial institution to create monetary or other thresholds below which an activity will not be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine 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.

107. Some form of monitoring, whether it is 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, trigger a process for appropriately revising the customer's risk rating. Equally, 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 risk-based approach, however within this context it should be understood that not all transactions, accounts or customers will be monitored in exactly the same way. 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.

*Level, scope and frequency of transaction monitoring by financial service providers serving low income customers and for low risk customers*

108. Setting up an adequate transaction monitoring will very much consist in a balancing exercise between the assessment of ML/TF risks, the technical capacities/facilities of the financial institution and the level/type of information the financial institution is able to obtain and verify in relation to the customer. Countries may introduce different monitoring requirements on the different types of financial service providers.

**Case study – example of monitoring of business relationships in the Philippines**

The AML/CFT regulation requires principals' (universal and commercial banks) AML systems to have at least the following automated monitoring facilities:

1. Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;
2. Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;
3. Investigation – checks for given names throughout the history of payment stored in the system;
4. Can generate all the Covered Transaction Reports of the covered institution accurately and completely with all the mandatory field properly filled up;
5. Must provide a complete audit trail;
6. Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and
7. Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of Senior Management whether or not a report was filed with the FIU.

For other covered institutions (principals other than universal and commercial banks), they need not have an electronic system of flagging and monitoring transactions but shall ensure that it has the means of flagging and monitoring the transactions mentioned in above. They shall maintain a register of all suspicious transactions that have been brought to the attention of Senior Management whether or not the same was reported to the FIU.

109. 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, scanning may not be able to deliver significant benefit in the absence of a sufficient range of available information.

### *4.2. Requirement to carry out record-keeping requirements (Recommendation 10)*

110. According to Recommendation 10, financial institutions and DNFBPs should maintain, for at least five years, all domestic and cross-border transaction (including the amounts and types of currency involved if any) 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.

111. The Recommendation states that financial institutions should keep records on the identification data obtained through the customer due diligence process (*e.g.,* copies or records of official identification documents (*e.g.,* passports, identity cards, driver's licenses and similar documents), account files and business correspondence for at least five years after the business relationship is ended.

112. The record keeping requirement under the FATF standards does not require the retention of a photocopy of the identification document(s) presented for verification purposes but merely that the information on that document be stored and kept for 5 years. A number of other countries, such as the United States, Australia and Canada, have considered but rejected imposing photocopying obligations on their regulated institutions. They decided against that for a number of reasons, for instance that the photocopies could be used to commit identity fraud; that they may breach privacy laws and that they may reveal information about the client that could form the basis of discriminatory practices, for instance the refusal of credit facilities to that client.

113. Recommendation 10 allows different forms of documents' retention , including electronic storage.

114. Depending on the size and sophistication of mobile provider's record storage, the following record retention techniques are acceptable:

1. Scanning the verification material and maintaining the information it electronically;
2. Keeping electronic copies of the results of any electronic verification checks;
3. The option of merely recording reference details may be particularly useful in the particular context of mobile banking, where mobile money agents are often the simple, modest 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.

115. In South-Africa, for instance, legislation allows for electronic capturing and storage record information, including in relation to documents of which copies have to be retained. In Rwanda and Kenya, storing electronic finger prints is permitted and in both of these countries credit unions ha ve piloted fingerprint identification technology for rural poor customers.

116. In Mexico, in an effort to expand efficient and secure financial services to people living in rural, marginalized areas of Mexico, 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 reduce the length of waiting time for members and enable credit union representatives to serve more people during field visits. It finally offers an interesting alternative retention technique of transactions.

### *4.3. Requirement to report suspicious transactions (Recommendation 13)*

117. 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. Unlike some other FATF Recommendations, there is no scope to exempt or apply reduced measures. Countries' reporting regimes are laid down in national law, requiring institutions to file reports when the

threshold of suspicion is reached. Where a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made and, therefore, a risk-based approach for the reporting of suspicious activity under these circumstances is not applicable.

118. A risk-based approach is, however, appropriate for the purpose of identifying suspicious activity, for example, by directing additional resources at those areas a financial institution has identified as higher risk. As part of a risk-based approach, it is also likely that a financial institution will utilize information 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.

119. FATF Recommendation 13 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 FIU. This obligation applies to all financial institutions that are subject to AML/CFT obligations, including those that serve the 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. It seems that in many countries, non-banks that serve low income people are equipped with internal systems and have adopted risk management procedures, as recommended by the FATF standards, including set of measures such as a limitation of the number, types and/or amount of transactions that can be performed.

120. In most countries, transactions with vulnerable group clients are not deemed to be subject to separate or specific monitoring systems that are developed at the financial institution's level. Some businesses may have however developed specific indicators as follows:

**Case-study – the detection of suspicious transactions in Western Union**

Important criteria to detect suspicious transactions that Western Union applies focusing on financially excluded groups are as follows (amongst other criteria, such as systemic monitoring):

- A lack of cooperation at the counter when further questions are asked or a suspicious behaviour is detected. WU believes that being undocumented / marginalized is not an excuse to a lack of mutually positive cooperation at counter.
- 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 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 belonging to that population is engaged in a TF initiative, whatever the amount of money sent.
- Any signal that a consumer belonging to that population tries to bribe / influence the agent or WU staff at counter or is producing wrong information and recognizes it.

### *4.4. The use of agents to carry out AML/CFT functions (including Recommendations 15, 23 and Special Recommendation VI)*

*General*

121. The use of agents to distribute financial services is part of an increasingly popular model for financial inclusion in many countries. Most countries that contributed to this guidance paper have

developed different business models using such arrangements. In these countries, banking and payment services are provided through mobile phones and small retail outlets, such as groceries, bakeries, etc. that provide a broader and cheaper access to financial services than a branch-based model.

*Definitions and scope*

122. ***General.*** The normal customer identification and verification obligations are normally predicated on the basis that these functions are carried out by officers or employees of the financial institution (or DNFBP). 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

123. ***Notion of agent***. Although the business models and the terminology may vary significantly from country to country, it is understood that the agent works on behalf of a financial institution. 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 third party. 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.

124. The FATF makes explicit reference to the notion of "agent" in the context of Recommendation 9 (see above) and Special Recommendation IV (remittance services). In the context of Recommendation 9, the FATF considers that an agent can be equated with the financial institution's employee in the sense that the agent is like an extension of the financial institution, with the information and documents held by that person being immediately available to the institution.

125. 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.

126. In the context of Special Recommendation VI, an agent is defined as "*any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).*"

127. ***Who can be an agent?*** Many countries permit a wide range of individuals and legal entities to be agents for financial institutions. Other countries limit a list of eligible agents on the basis of a legal form[55]. 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. It seems essential for countries that have different regulatory concerns to balance agent eligibility requirements (that are essential from an AML/CFT perspective) with the financial inclusion objective. This question may also require some discussion and consultation with the financial sector (in some countries the list of eligible agents may be

[55] CGAP (2011)

very extensive but underused by the financial actors that may be reluctant to engage agents)[56]. It must also be emphasised that retailers are not necessarily agents of the banking institution[57].

128. The principle of ultimate liability of the financial institution for agents' compliance with the AML/CFT requirements seems almost universal although the extent of liability may differ from one country to another.

129. 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 in respect of the provision of their traditional communications services. However, they operate under the oversight of the Central Bank in relation to the provision of any mobile financial services. It is worth noting that, in the context of SRVI, the obligation of licensing or registration can consist in an obligation put on the principal business to maintain a current list of agents which must be made available to the designated competent authority.

*AML/CFT functions of the agent and related challenges*

130. The fact that agents act as an extension of the principal financial institution means that the processes and documentation, notably 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 that context, it is essential that these duties are clearly specified in the agency agreement in terms of which the retailer is appointed as an agent of the principal financial institution. It seems that in practice, the contracts between the principal financial institution and their agents vary considerably across countries and markets but common clauses seem generally to include the duty to perform specified AML/CFT checks, record-keeping and reporting obligations.

131. In determining the AML/CFT role and duties of the agents, it is crucial to take into account the potential practical limitations faced by retailers (often small shops). Retailers generally have a partial knowledge of the transactions conducted by the customer (*i.e.,* the transaction conducted in their respective shops). AML/CFT duties of the agents and the principal financial institution should be seen as complementary and inclusive.

132. Although the precise role of such a retailer may differ from model to model, it generally involves providing cash-in and cash-out services but may 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. In some contexts, however, this basic functionality has been compromised by existing regulations that deem cash-in services as "deposit" taking, an activity that is limited to banks or that otherwise requires licensing (such as a money remittance license).

133. 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

[56] CGAP also 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.

[57] See World Bank (2011)

products. The challenges related to the identification of the customer and verification of the identity (as described in section 4.1) will therefore very much vary from country to country.

134. As indicated above, the FATF requires financial institutions to have appropriate systems and controls to monitor the transactions of each client, and report to the financial intelligence unit any transaction or activity that could be suspected to be related to money laundering or terrorism financing crimes. This monitoring requirement may require some adjustments in principal-agent scenarios although the models developed in countries under review seem very similar. In Mexico for instance, according to AML/CFT legal framework, financial entities 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. The operations carried out by the agent must be monitored by the financial entities and reported to the FIU in case of suspicion. In addition, financial entities must have automated systems that allow them to develop, among other things, the functions of detecting and monitoring transactions carried out by client and must have the purpose of detecting possible unjustified deviations in their transactional profile in order for the Communication and Control Committee (conformed by high ranking employees of the financial entities) to analyze them and if considered, report them to the FIU. Similar arrangements exist in Malaysia and South-Africa. In the Philippines, both principal and agents are covered institutions and 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.

135. Again, the challenges faced by agents would differ from country to country depending on the business models that are allowed and the related regulatory systems.

136. It is important to note that, in the context of SRVI, it is not the practice in most countries to impose independent AML/CFT obligations on the agents of the remittance services (instead, the principal, as a regulated institution, remains solely responsible for meeting the AML/CFT obligations, including for the actions (and omissions) carried out by its agents). This seems consistent with the general FATF approach of treating agents as an extension of the financial institution, and not as something entirely separate from it.

*Internal controls applicable to agents*

137. As part of the AML/CFT obligations, financial institutions are required to develop internal control programmes against money laundering and terrorist financing (see Recommendation 15). The type and extent of measures to be taken for each of the requirements under Recommendation 15 should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

138. 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 (see section 4.5 below).

*Oversight of agents*

139. Since agents are seen as synonymous with the principal financial institution, it is appropriate for supervision and oversight to primarily focus on the principal financial institution. Monitoring and

supervising thousands of agents in line with Recommendation 23[58] would be extremely challenging for most countries. Building up appropriate and balanced supervision or oversight regimes requires taking into account the ML/TF risks. If the scrutiny of agents is mainly performed by the principal financial institution, it is also essential that the supervisor gets oversight functions in relation to the policies, procedures, training and monitoring of agents put in place by the principal financial institutions. For instance, a representative sample of agents could be visited by the supervisor to inspect whether the principal financial institution is performing the required functions correctly. While the level and depth of such monitoring may be different, in principle this could be seen as comparable with a supervisor visiting a branch to see that the policies of the institution are being correctly applied. In Kenya, mobile financial service providers submit periodic returns on operations, volumes, frauds, customer complaints and other parameters to the Central Bank. The models are backed by trust accounts operated by independent trustees, with the fund held in commercial banks.

140. Agent monitoring is a very important element in an effective AML/CFT program where the concept of risk-based approach has an important role to play. While all agents require baseline monitoring to assess and address systemic risks such as inadequate training, new or changing services or products, and poor individual judgment or performance, the risk-based approach requires a higher level of monitoring to locate and eliminate the few agents that knowingly or through wilful blindness act in a way that may conceal their customers conduct from routine monitoring. The degree and nature of agent monitoring will depend on the transaction volume and principal volume of the agent with whom the principal financial institution shares responsibility for effective AML/CFT, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, the degree of monitoring will be based on the perceived risks, both external and internal, associated with the agent, such as the products or services being provided by the agent, the location of the agent and the nature of the activity.

### 4.5 Internal controls

141. The FATF Standards require financial institutions to develop programmes against money laundering and terrorist financing although with some degrees of flexibility having regard to the ML/TF risk. Using this flexibility is crucial, especially for businesses designed to serve the financially excluded or underserved. These 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

[58] "Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution. For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes. Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing".

culture of compliance, ensuring that staff adheres to the financial institution's policies, procedures and processes designed to limit and control risks.

142. The FATF acknowledges that fact 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.

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

- Provide 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.
- Provide 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.
- Ensure that adequate controls are in place before new products are offered.
- Implement risk-based customer due diligence policies, procedures and processes
- Provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
- Enable 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.
- Provide for appropriate training to be given to all relevant staff.

### 4.6 Other relevant issues

144. 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, 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.

145. In that respect the FATF Standards promote domestic cooperation mechanisms (Recommendation 31[59]) and encourage public authorities to assist the private sector in adopting adequate and effective AML/CFT measures (Recommendation 25[60]). These principles should guide countries' effort to build up an effective AML/CFT regime while working towards better financial inclusion. A sample of countries' experiences is provided in Annex 11.

146. Lastly, the FAFT 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 channelling of cash payments onto bank accounts constitute examples of such innovative products that effectively promote financial inclusion. The FAFT acknowledges the importance of promoting the exchange of experience at international level, in order to help identify best transferrable practices across FATF countries and beyond.

---

[59] "Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing".

[60] "The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions".

# Conclusion

147. 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 encourages the use of the flexibility and risk-based approach that are available in the AML/CFT Standards but which are not used as widely.

148. The FATF will continue to work to ensure that financial inclusion and AML/CFT objectives do not conflict. 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 new payments methods that can contribute to serve the financially excluded or underserved groups. It will also take it into account as it prepares the new assessment methodology based on the upcoming revised FATF Recommendations.

# Annexes

# 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.

### 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.

# ANNEX 2
# SOURCES OF THE GUIDANCE PAPER

## Bibliography


- *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).
- Bangko Sentral Ng Pilipinas (2011) *Updated Anti-Money Laundering Rules and Regulations,* www.bsp.gov.ph/downloads/regulations/attachments/2011/c706.pdf, accessed June 2011.
- Basel Committee on Banking Supervision (2001), *Customer Due Diligence for Banks,* Basel Committee on Banking Supervision, Basel, www.bis.org/publ/bcbs85.htm.
- Bester, H., Chamberlain, D., De Koker, L., Hougaard, C., Short, R., Smith, A., and Walker, R. (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.
- Chatain, P-L., Zerzan, A., Noor, W., Dannaoui, N. and De Koker, L. (2011) *Protecting Mobile Money Against Financial Crime: Global Policy Challenges and Solutions*, The World Bank, Washington, DC, www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2011/03/10/000333037_20110310000727/Rendered/PDF/600600PUB0ID181Mobile09780821386699.pdf
- Chatain, P-L., Hernández-Coss, R., Borowik, K. and Zerzan, A. (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.
- 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.
- Consultative Group to Assist the Poor (CGAP) (2011), *Regulating Banking Agents*, Focus Note n°68, March 2011, www.cgap.org/gm/document-1.9.50419/FN68.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.
- Isern, J., and De Koker, L. (2009), *AML/CFT: Strengthening Financial Inclusion and Integrity*, Focus Note 56. CGAP, Washington, DC, www.cgap.org/gm/document-1.9.37862/FN56.pdf

- Solin, Marina, and Zerzan, Andrew (2010), *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks*, GSMA Discussion Paper. GSMA, London

- 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 163. The World Bank, Washington, DC http://publications.worldbank.org/index.php?main_page=product_info&products_id=23110.

- World Bank (2009), *Canada-Caribbean Remittance Corridor Analysis*.

- World Bank (2011), *Protecting Mobile Money against Financial Crimes, Global Policy Challenges and Solutions*.

- World Bank *Poverty Reduction and Equity*, web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTPOVERTY/0,,contentMDK:22569498~pagePK:148956~piPK:216618~theSitePK:336992,00.html, accessed June 2011.

- World Bank *Migration and Remittances* at web.worldbank.org/WBSITE/EXTERNAL/TOPICS/0,,contentMDK:21924020~pagePK:5105988~piPK:360975~theSitePK:214971,00.html, accessed June 2011.

- 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.


## Useful additional sources

### *Relevant FATF documentation:*

- FATF (2008) *Guidance on Capacity Building for Mutual Evaluations and Implementation of the FATF Standards within Low Capacity Countries*

- FATF (2010) *Report on Money Laundering Using New Payment Methods*.

- FATF (2011, forthcoming) *Guidance on Risk and Threat Assessment*

### *Other useful sources:*

- CGAP financial inclusion regulation center www.cgap.org/p/site/c/template.rc/1.26.13751/

- G20 Financial Inclusion Experts Group. 2010. "Principles for Innovative Financial Inclusion" www.g20.utoronto.ca/2010/to-principles.html

- 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

- Basel Committee on Banking Supervision. 2010. Microfinance activities and the Core Principles for Effective Banking Supervision. Bank for International Settlements, Basel, www.bis.org/publ/bcbs175.pdf

- World Bank (2011), *Regulating and Supervising Remittance Service Providers* (provisional title)

ANNEX 3

# G20 PRINCIPLES FOR INNOVATIVE FINANCIAL INCLUSION AND ACTUAL RELEVANCE TO THE FATF

1. Presentation of the G20 Principles For Innovative Financial Inclusion

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, 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 4
# 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** | • Include financial inclusion as part of the broader financial sector strategy<br>• Develop a market based approach to financial sector development<br>• Various regulatory reforms and initiatives, including development of legislation to regulate micro-finance, credit unions and e-money and payments<br>• Provide greater operational independence for regulators<br>• Create space for innovation and stakeholder feedback<br>• Support financial education initiatives and consumer protection efforts<br>• Conduct the development of relevant and efficient banking and market infrastructure<br>• Promote initiatives to gather further information regarding current levels of financial inclusion and barriers to the supply of financial services<br>• Implement changes to the distribution of government subsidies in order to promote electronic transfers and financial inclusion |
| **Regulators** | • Adequate regulation and supervision of the banking and non-banking system, fostering orderly operation while simultaneously promoting development of products aimed at the underserved population<br>• Ongoing development of capacity to regulate micro-finance activities<br>• Create space for stakeholder consultation and feedback and provide regulatory guidance in these areas<br>• 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<br>• Innovation in products, channels and processes in partnership with others, such as mobile phone operators<br>• Active participation in discussions on regulatory changes, especially for micro-finance and credit unions |

ANNEX 5

# ILLUSTRATION OF THE SITUATION OF DIFFERENT COUNTRIES WITH REGARD TO FINANCIAL INCLUSION

The situation with regard to financial inclusion in different countries can be illustrated as follows:

| |
|---|
| In India, despite the widespread expansion of the banking sector a significant proportion of the households, especially in rural areas, are still outside the coverage of the formal banking system. These households have been dependent on the informal money lenders for their credit needs and had a few avenues for keeping their savings. The financially excluded sections largely comprise marginal farmers, landless labourers, oral lessees, self-employed and unorganized sector enterprises, urban slum dwellers, migrants, ethnic minorities and socially excluded groups, senior citizens and women. It is estimated that the proportion of rural residents who lack access to bank accounts remains at 40%. |
| In Kenya, the bankable population that accesses formal financial services still remains low at less than 25%. The proportion of the population excluded from any financial services is up to 32.7%. |
| Malawi has an underdeveloped finance sector—particularly in terms of serving the poor. Of the economically active poor in Malawi, it is estimated that only three percent have access to savings and one percent have access to credit. (UNDP Malawi). 85 percent of population is unbanked. |
| In Mexico, 10% of the 76.7 million adults have no access to financial services and 11% of the adult population living at rural municipalities has access to a branch. In transition municipalities (with 5 000 to 15 000 adults) 68% of adults have no access to financial institutions. In contrast, most adults at urban municipalities have access to financial services. |
| In South Africa , the latest Finscope Survey 2010 indicates the following:<br>- 77% of adult South Africans (16 years and older) are financially included (25,1 million individuals), meaning they use any kind of formal or informal financial service.<br>- 23% of adults are financially excluded (that is, using no financial products, formal or informal, to manage their financial lives).<br>- 63% of adults are banked (20,5 million individuals)<br>- 68% are formally included (22,2 million individuals)<br>- 47% have/use non-bank financial products and/or services. |

It seems overly simplistic to distinguish inclusion from exclusion with no further nuances. For instance, in Kenya, the access strand presents usage of financial services by level of formalisation:

- *Formal* – use a bank, PostBank or insurance undertaking.
- *Formal other* – do not use any formal product (as categorized above), but use services from non-bank financial institutions such as SACCOs (Savings and Credit Cooperative Societies) and MFIs (Micro-finance Institutions).

- *Informal* – do not use any formal/formal other products but use informal financial service providers such as ASCAs[61], RoSCAs[62] and groups/individuals other than family/friends.
- *Excluded* – use no formal/formal other or informal financial services.

Figures in Kenya are as follows (*source: FinAcess, 2009*):

| Formal (22.6%) | Formal other (17.9%) | Informal (26.8%) | Excluded (32.7%) |
|---|---|---|---|

In India, the National Sample Survey Organization (NSSO) (59th round) had brought out that:

- 51.4% of farmer households are financially excluded from both formal / informal sources.
- Of the total farmer households, only 27% access formal sources of credit; one third of this group also borrows from non-formal sources.
- Overall, 73% of farmer households have no access to formal sources of credit.
- Farmer households constitute 66% of total farm households. Only 45% of these households are indebted to either formal or non formal sources of finance.
- About 20% of indebted marginal farmer households have access to formal sources of credit.

[61] Accumulating Savings and Credit Associations.

[62] These are rotating savings and credit associations (ROSCAs), often referred to as merry-go-rounds or tontines in Africa. These provide a simple means through which to save and accumulate a lump sum through the regular pooling of usually small contributions in a group which is taken by each group member in turn.

ANNEX 6

# 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,<br>Postal Banks,<br>Financial Cooperatives<br>Savings Institutions | In branch<br>Agency<br>Electronic communication |
| Credit | Banks<br>Micro Finance<br>Financial Cooperatives | In branch<br>Agency |
| Payment services | Banks<br>Financial Cooperatives<br>Mobile Network Operators | Electronic communication |
| Remittance | Banks<br>Remittance companies<br>Financial Cooperatives<br>Mobile Network Operators | In branch<br>Agency<br>Electronic communication |
| Currency exchange | Banks<br>Money Exchange Businesses<br>Remittance companies | In branch<br>Agency |
| Cheque cashing | Banks<br>Money services Businesses<br>Financial Cooperatives | In branch<br>Agency |
| Issuance and/or cashing of traveller's cheques and money orders | Banks<br>Postal Banks<br>Money services Businesses<br>Money Exchange Businesses<br>Financial Cooperatives | In branch<br>Agency |
| Issuance of stored value products | Banks<br>Mobile Network Operators | In branch<br>Agency<br>Electronic communication |
| Micro insurance | Insurance Companies<br>Micro finance<br>Financial Cooperatives | In branch<br>Agency<br>Electronic communication |

## II. Examples of products offered to financial excluded and underserved groups[63]

*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 rupees one lakh (equivalent to $2000)<br>**+**<br>ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand(equivalent to $200)<br>**+**<br>iii) the balance at any point of time does not exceed rupees fifty thousand(equivalent to $1000)<br><br>Such accounts should be opened only in CBS branches ( that is computerized linked to bank servers) to ensure that the limits prescribed s are not breached, and<br><br>No foreign remittance can be credited to these accounts, and<br><br>Full customer due diligence to be carried out in case of suspicion of ML/TF. | An individual desirous of opening a —small account" should produce a self attested photograph and the designated officer of the bank has to affix his signatures to indicate that the person opening the bank account and the person as per the photograph are one and the same person.<br><br>Within 12 months of opening the bank account the account holder has to produce a document to indicate that he has already applied for an officially valid document (Passport, Voter's Identity Card, Driving Licence or Income Tax PAN card).<br><br>Only on production of such a document the bank would allow him 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. |

[63] Examples of products launched by the private sector are provided in Annex 4 of the paper.

*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 Rupees.10 000/- ( US $ 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 among the population in Mexico, the authorities have identified the risks, based on an assessment of product characteristics and considering its potential vulnerabilities. Based on an evaluation of the latter, coupled with relevant economic and market factors specific to Mexico, which included household income levels´ and official subsidies provided by the government to the low income sector, adequate thresholds for caps on deposits for low-risk accounts was 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, and 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[64].

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.

[64] FATF Report "Money Laundering Using New Payment Methods" October 2010.

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

| Description of the product and financial facilities | Amount/ threshold limitation | Customer identification requirements |
|---|---|---|
| **LEVEL 1**<br><br>**Low risk account that may allows a non face to face opening process, but subject to monitoring from financial entities and to enhanced supervision of the financial authorities.**<br><br>**Main characteristics:**<br><br>• **Customer identification and ID verification could be exempted.**<br>• **Restricted use for payment of services and/or products.**<br>• **Not linked to a mobile phone account (For funds transfers)**<br>• **Valid only in Mexico.**<br>• **Contracted at banking branches, banking agents, by phone or at the banking institution website.**<br>• **Unable to transfer funds (to other accounts or products)** | Limited to a maximum deposit amount of 750 UDIS[65] per month (*Based on the EU 2,500 USD/Euros threshold for reloadable cards*)<br><br>Limited to a non-cumulative maximum balance of 1 000 UDIS. | Not compulsory |
| **LEVEL 2**<br><br>• **Filing requirements are obtained from basic data of the client and account opening can be outsourced,**<br>• **Subject to monitoring by financial entities.**<br>**Two schemes:**<br><br>**a) Contracted directly at banking branches and banking agents.**<br>**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.**<br>**Based on this scheme, data verification by banking institutions will be validated through the system of the National Population Registry or RENAPO which contains relevant information from individuals living in Mexico.** | Limited to a maximum deposit amount of 3 000 UDIS (USD 950) per month.<br><br>If cross-checking of client's ID information isn't conducted in an 18-month period, maximum monthly deposits would be limited to 1,500 UDIS (USD 470) and the use of the account would be restricted to be valid only in Mexico. | Electronic file requires to be integrated only with basic client's data (Name, place and date of birth and gender and address). No copies required.<br><br>In case of the scheme a), the banking institution must obtain complete data on the name, birth date and address. Only name and birth date, should match with the official ID presented by the client. |

[65] The Mexican Investment Unit (UDI) is a unit of value calculated by the Central Bank of Mexico, which it 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 | Amount/ threshold limitation | Customer identification requirements |
|---|---|---|
| • **May be linked to a mobile phone account.**<br>• **May be used for funds transfers.** | | In case of the scheme b) the banking institution should validate that the data provided by the client matches that at the National Population Registry (RENAPO) using a unique official ID number CURP). Moreover, the CNBV, with opinion from the Ministry of Finance, may authorize the use of other processes to validate the data. |
| **LEVEL 3**<br><br>**The file requires to be integrated with the client's whole data list requirements (Obtained from an official ID).**<br>• **Account opening must be face-to-face**<br>• **May be contracted in banking branches, banking agents or companies.**<br>**May be linked to a mobile phone account.**<br>• **Could be used for funds transfers.** | **Limited to a maximum deposit amount of 10 000 UDIS (USD 3,150) per month.** | Electronic file requires to be integrated with the client's whole list data requirements (Name, gender, address, profession, birth date, telephone number, profession, nationality, place of birth, ID information, e-mail, federal taxpayer´s registry, among others). No copies required. |
| **LEVEL 4**<br><br>**Traditional Accounts**<br><br>• **The file requires to be integrated with the client's whole list data requirements, and the banking institution requires maintaining a copy of the documentation.**<br>• **Account opening must be opened in banking branches** | **No Limits** | The file requires to be integrated with the client's whole list data requirements (Name, gender, address, profession, birth date, telephone number, profession, nationality, place of birth, ID information, e-mail, federal taxpayer´s registry, among others). Hard copies are required. |

*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** | A person holding such an account is not able to withdraw or transfer or make payments of an | This product is only available to a natural person; the customer must be a South African citizen or |

| Description of the product and financial facilities (including whether there is banking arrangement) | Amount/threshold limitation | Customer identification requirements |
|---|---|---|
| **of simplified due diligence. 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).**<br><br>**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.**<br><br>**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 branches of its own and accessing bank accounts and conducting transactions are done by means of a cellular telephone.** | amount exceeding R5000 (approximately EUR 500) per day or exceeding R25 000 (approximately EUR 2500) in a monthly cycle.<br><br>The balance maintained in the account must not exceed R25000 (approximately EUR 2500) at any time.<br><br>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 and Swaziland).<br><br>The same person must not simultaneously hold two or more accounts which meet the Exemption 17 criteria with the same institution. | resident.<br><br>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.<br><br>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. |

*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.**<br><br>**A product of this nature can be used as a means of payment for goods and services within the Republic of South Africa only.**<br><br>**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 R3000 (EUR 300).<br><br>A limit on the balance on the product is R1500 (EUR 150) at any given time.<br><br>A limit on the spending on the product is R200 (EUR 20) per transaction. | None.<br><br>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 |

| Description of the product and financial facilities | Amount/threshold limitation | Customer identification requirements |
|---|---|---|
| | | 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. |

ANNEX 7

# EXAMPLES OF COUNTRIES THAT HAVE DEVELOPED AN AML/CFT RISK ASSESSMENT METHODOLOGY

***Canada***. Canada is one of the countries that have developed an AML/CFT Risk Assessment Methodology (dated October 2008). The methodology describes the criteria, process and factors on the basis of which a ML and TF risk assessment is conducted. The risk assessment serves as the basis for Canada's decisions regarding the coverage of specific industry sectors or sub-sectors, products and classes of customers under the AML/CFT legislation. The assessment may also lead to a policy response other than amendments to the AML/CFT regime, such as the development of industry-issued guidance or regulations, or promoting enhanced information sharing between domestic and/or international stakeholders. Risk can, for example, be categorised by sector, product, customer, activity or geographic location. Canada's AML/CFT Risk Assessment Methodology specifies the criteria to be assessed when determining the risk posed by a sector or product. This includes elements such as basic information on the sector/product; regulatory environment; extent and efficacy of compliance audits; enforceability of rule/guidance; existence of a regulator; international standards/conventions applicable to the specific sector/product; similar activities in other sectors; links with other financial intermediaries; nature of business relationships; delivery channel; legal or other constraints; possibility for cash payments; cross-border movements of funds; business and customer base in specific geographic areas; types of customers; coverage/requirements in other countries; source of funds; restrictions on deposits/withdrawals; and cost of services.

Similar to the sector/product analysis, a customer analysis will help determine whether specific types of customers warrant additional or reduced obligations under Canada's AML/CFT legislative framework. When assessing the risk posed by a certain category of customers the following information is analyzed: basic information on the customer; whether the customer is an entity or a person; non-residents; geographic area of concerns; international standards/conventions; regulatory provisions on the customer; restrictions on customer's transactions; cash transactions and cross-border funds transfers; requirements in other countries; and CDD / reporting measures currently performed.

**Hong Kong.** This risk assessment requires evaluation of the two components of risk, namely the magnitude of potential threat/hazard and the probability that such threat/hazard would occur.

***"Threat" Factors***

In assessing the magnitude of the threat/hazard posed by a specific sector in ML/TF context, we will take into account the following factors -

(a) number of establishments in the business sector;
(b) size of the clientele;
(c) volume of transactions/business turnover; and

(d) intelligence from law enforcement (*e.g.,* number of suspicious transaction reports and money laundering investigations conducted).

The assessment of potential threat/hazard defines the scope and severity of the problem that a sector would cause if it is abused for ML/TF purpose. For the purpose of assessing the potential threat/hazard posed by specific business sectors, factual and quantitative information concerning the factors listed above from various sources will be collected. A business sector's threat/hazard should be proportionate to its presence and economic significance. For example, the impact of abuses of those sectors with a small number of establishments locally, small client base, comparatively low business turnover or transaction volume on our overall policy objective would likely be low.

***"Probability" Factors***

The assessment will focus on the vulnerability of a particular business sector to ML/TF abuses. The assessment will take into account the following factors about the sector's regulatory oversight and mode of operation. The list of factors is drawn up having regard to the typical typologies on money laundering developed by the FATF and other international and regional bodies on AML –

(a) Regulatory oversight – whether the business sector is subject to any legal/regulatory oversight with clearly defined standards and requirements for business conduct/practices and sanctions for breaches. Businesses subject to formal regulatory oversight generally are less vulnerable to ML/TF abuses.

(b) Customer types and identification – whether the business sector has any restrictions on customer types (e.g., entities vs. persons, membership system, locals vs foreign nationals), how the customer identification process is conducted, and how customer information is obtained and verified. Businesses with restrictions on client types and proper customer identification arrangement are considered less vulnerable to ML/TF abuses.

(c) Record-keeping arrangement – whether there are established practices/requirements for keeping records of transactions which can be readily retrieved for construction of audit trails if follow-up investigations are necessary. Businesses with proper record-keeping requirements are considered less vulnerable to ML/TF abuses.

(d) Range of services provided – whether diversified financial services (via electronic means, acceptance of non-face-to-face transactions, cross-border transfers and transactions) are offered. Businesses which offer a higher degree of variety of services are considered more vulnerable to ML/TF abuses.

(e) AML/CFT awareness – whether the business practitioners are aware of the AML/CFT requirements and the legal obligation to report suspicious transactions to law enforcement agencies. Those businesses with higher AML/CFT awareness and regular awareness seminars/training are considered less vulnerable to ML/TF abuses. The number of suspicious transactions reports filed by the sector is considered a useful indicator of the sector's awareness.

Relevant information on the above factors will be collected through different means, including documentation researches, consultation and interviews with major stakeholders (*e.g.,* regulatory authorities and trade associations) for conducting the probability assessment. Those business sectors with great vulnerability will be the likely conduits for money laundering and the probability / likelihood of the occurrence of the potential threat/hazard will be higher.

On the basis of the outcome of the threat and probability assessments of a particular business sector, a qualitative assessment on the ML/TF risks of that sector will be made. The three levels of risks will be set as "High", "Medium" and "Low". Corresponding to the risks assessed, recommendations will be made on the appropriate follow-up actions, including whether and if so what specific AML/CFT measures should be implemented for the sectors concerned.

# ANNEX 8
# 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, 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.

**Component 1: National Risk Assessment (NRA) using Template 1**

- 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.

# ANNEX 9
# EXAMPLE OF A RISK METHODOLOGY 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 behavior 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.

| **Western Union Risk Methodology** |
| --- |
| **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

# ANNEX 10
# INITIATIVES TO ADDRESS THE CUSTOMER IDENTIFICATION/IDENTITY VERIFICATION CHALLENGES

| | |
|---|---|
| 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.<br>✓ The Central Bank has approved the following reduced CDD for Lesotho PostBank:<br>- 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).<br>- 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.<br>✓ The record keeping of transactions and documents can be done in electronic format (documents scanned).<br>✓ The monitoring is done to identify unusual activity of an account. |
| Malaysia Bank | ✓ 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.<br>✓ *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 implement a scheme for data verification process of non-face to face accounts opened by phone or at the banking institution website, where further ID verification will consist of clients' data validation by banking institutions through the system of the National Population Registry or RENAPO which contains relevant information of person living in Mexico) |
| Philippines | ✓ *Barangay Certification*, a certificate issued by the village master, is accepted as a proof of identification and residence.<br>✓ 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*. |

ANNEX 11

# 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.


*FATF/OECD*
*June 2011*

*www.fatf-gafi.org*