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, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard

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

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

The 2013 *Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* was a collaboration with *APG* and the *World Bank*. This 2017 edition combines the *FATF Supplement* with the original *2013 Guidance*.

Citing reference:

FATF (2013-2017), *Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence,* FATF, Paris
www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

CONTENTS

2013 FATF GUIDANCE ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION

SUPPLEMENT TO THE 2013 FATF GUIDANCE ON AML/CFT MEASURES AND FINANCIAL INCLUSION

CUSTOMER DUE DILIGENCE AND FINANCIAL INCLUSION

FATF AND FINANCIAL INCLUSION

The FATF is committed to financial inclusion. The application of measures that enable more individuals and businesses, especially low-income, unserved and underserved groups, to access and use regulated financial services increases the reach and the effectiveness of anti-money laundering/countering the financing of terrorism (AML/CFT) regim.4(ieg)5.o/01 Tca91

18% of all adults without an account cited documentation requirements to establish proof of identity as an important barrier to account ownership.[4] These requirements could primarily affect people living in rural areas or employed in the informal sector (e.g. individuals paid in cash, undocumented migrants), who are less likely to have formal proof of identity or of address, and other checks often completed by banks in the process of verifying an individual's identity. This is more visible in low capacity countries, some of which do not have any national ID infrastructure. However, these challenges may also affect specific groups of people in developed economies, for example asylum-seekers and refugees from higher-risk countries. Financial institutions' concerns about the reliability and robustness of their identity documentation create challenges, but providing these people with oa4.2 Td-0(e)4.2 Td5 c 58-13.35m7( )15.8( )fe(o)10.9 ot.6(u fu)-1. hs-6.40.005 Tc -0.008 Tw[o)-0.62d[a)-10.1(s)

flexibility offered by FATF Recommendations, and further updates and steps might be needed based on initiatives developed at national level.

The objective of the paper is to encourage countries to implement the FATF Recommendations and the RBA in a way that responds to the need to bring the financially excluded into the regulated financial sector, while at the same time maintaining effective safeguards and controls against ML/TF risks. It focuses on initiatives to support access to and use of basic financial services and products for low income, unserved or underserved natural persons/individuals, which are generally limited purpose or restricted use products or services. Those products and services may (1) be exempted from some AML/CFT controls based on proven low risks; (2) benefit from a simplified due diligence (SDD) regime, based on evidence of lower risks; or (3) be submitted to standard CDD supported by the use of new or alternative forms of identity documentation, including digital solutions.

The paper provides examples submitted by FATF delegations, FATF-Style Regional Bodies (FSRBs) and observers: Australia, Belgium, Brazil, Canada, China, European Commission, France, Germany, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Spain, Sweden, Switzerland, Turkey, United States; APG (Fiji, Maldives, Marshall islands, Nauru, Samoa, the Philippines, Timor Leste); CFATF (Turks and Caicos islands); MENAFATF (Egypt, Jordan); GIABA (Burkina Faso, Cabo Verde, Ghana), Gafilat (Honduras, Chile, Guatemala); IMF; and World Bank (Pakistan, Nigeria, Peru, India) and Israel. Some of the examples mentioned are part of contributions received from partner organisations involved in financial inclusion (CGAP/Jordan, Peru, Pakistan, India, and Colombia).

The paper

ASSESSING RISK AND MITIGATION IN A FINANCIAL INCLUSION CONTEXT

Proportionate, risk-based AML/CFT controls may be applied to products or services intended to support financial inclusion, based on the nature and on the level of assessed ML/TF risks associated to these products or services. The products and services provided to newly banked people are often entry-level products and services with limited functionality or with restricted use. These types of products and services, by their own nature, may carry less ML/TF risks than standard products and services, and make them eligible for exemptions from some AML/CFT controls or SDD depending on the extent of lower risks.

The FATF Recommendations require countries to conduct risk assessments that take into account, in particular the ML/TF risks associated with the characteristics of the various customer target groups,

p16.8(it)11nd1t1.3(u)1.3(u)0 Tw2cy3.4 3.9(t)6(e)3.9(m.4(u)2.6.001 Tc -8(v)9(a)3.9(r)5/)

lower risk circumstances have been confirmed, based on a risk assessment, conducted at the national, sectoral or at the financial institution level (INR. 10 para. 16).[6]

The risk assessment needs to take a holistic approach and to consider several elements, including primarily the inherent risks of the products, but also the profile of the low income, unserved and underserved people targeted. It is important to recognise that targeted groups represent a very heterogeneous category, with very different ML/TF risk profiles in different jurisdictions. They cannot be classified as lower risk, solely on the basis that they are low income individuals, who are about to be or have recently been integrated into the regulated financial system, or are otherwise financially excluded.[7]

Where relevant, countries should also consider risks associated either with the digital nature of a particular product or service, including products involving new technologies, or with the distribution channel used. With regards to products and services provided through new technologies and services, including online banking, the risk assessment will have to consider factors such as the non-face-to-face relationships (taking account of the safeguards applied), the geographical reach, the methods of funding and the access to cash as well as the possible segmentation of services between several parties for the execution of payments.[8]

Identification of lower risk situations should be consistent with the country's assessment of its overall ML/TF risks (INR. 1 para. 5). Countries should include ML/TF risks associated with their financial inclusion challenges, when relevant, in their national risk assessment. This could involve, for example, the impact of financial exclusion on the extent of the cash usage in the economy; the existence of unregulated services, the attractiveness of the unregulated economy for illicit transactions; or the vulnerability of excluded people to financial crime and exploitation. Where such risks are present, addressing financial inclusion and broadening access to the use of formal financial services will be a part of the country's strategy for mitigating ML/FT risks.

Countries and institutions should keep these assessments under review. They should consider doing post-implementation assessments to determine whether in practice, the risks were actually lower, and the SDD measures were appropriate. This assessment may also analyse whether the simplified CDD serves to the objective effectively and improves financial inclusion. Such assessments are particularly important because risks tend to change over time. Risks associated with types of customers evolve, criminal abuse patterns also change and risk levels of products assessed as lower risk may increase over time, especially where criminals start to exploit simplified controls.[9]

---

6 INR.10, para 16 states: "There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures".

7 FATF Guidance on financial inclusion, 2013, para. 44

8 FATF Guidance for a RBA – Prepaid cards, mobile payments and Internet-based payment services, 2013, para. 39 and s., and Lauer and Lyman 'Digital financial inclusion: Implications for customers, regulators, supervisors, and Standard-Setting Bodies' CGAP Brief, 2015, www.cgap.org/sites/default/files/Brief-Digital-Financial-Inclusion-Feb-2015.pdf

9 De Koker 'The money laundering risk posed by low-risk financial products in South Africa', 2009; Findings and guidelines' 2009 Journal of Money Laundering Control 323, 334.

Box 1. **World Bank – Financial Inclusion Product Risk Assessment Module (FIRM)**

The World Bank's FIRM tool assesses the ML/TF risks associated with a particular product/service intended to support financial inclusion, and determines if a low/lower level of ML/TF risk can be associated to this product/service. The assessment is based on the net risk level of:

- the product features, which reflect the characteristics of the product as realistically as possible;

- the product-specific mitigating measures, in place or planned;

- and the overall risk environment, which includes the ML/TF threat in the country and the general AML/CFT control measures.

Countries (or financial institutions) using the World Bank tool are invited to provide information on these three parameters in an excel template. Based on the data collected, the module will produce an ML/TF risk assessment of the products.

If the assessment shows a lower level of ML/TF risk, this gives a green light to simplifying AML/CFT requirements. The assessment may result in medium or high risk, indicating that it is not appropriate to apply SDD and other simplified AML/CFT measures. In such a case, the tool guides the country in reducing the risk level of that particular financial inclusion product by modifying its features, functions, and improving the risk mitigation mechanisms. The tool has not only an assessment / diagnostics function, but also a guidance /design component.[10]

2. Appropriate risk mitigation measures

Incentives to financial inclusion are only acceptable in so far as this approach includes appropriate measures to mitigate the risks. In a number of countries, entry-level types of financial products have been developed, and adequate mitigation measures are embedded in their design, by limitations on the product's functionality or availability, or based on a progressive CDD approach. When SDD measures are applied at the on-boarding stage, the intensity of the monitoring process can be adjusted to mitigate the inherent risks of the financial products, and compensate for the relaxed initial due diligence checks.

a) Tiered CDD approach

Financial inclusion objectives have led a number of countries to design a so-called "progressive" or "tiered" CDD approach. Clients have access to a range of different account functionalities depending on the extent of identification/verification conducted by the financial institution. Strict pre-set thresholds are defined for the various account levels. Access to the basic, 1st level set of services is provided upon minimum identification. Access to the subsequent account levels and additional services (e.g. higher transaction limits or account balances, diversified access and delivery channels) is allowed only if/when the customer provides the required additional identification/verification information. In the meantime, the accounts have limited services (e.g. caps on daily/monthly withdrawals, deposit limits based on the level of CDD conducted and the customer's risk profile).

10 Further details on the World Bank's FIRM tool and examples of application are provided in the Appendix

Box 2. **China – Bank account management based on risks**

On the basis of a December 2015 Central Bank Circular, and with a view to help banks mitigate their AML/CFT risks, bank accounts for individuals have been classified into 3 categories. Type 1 account has full functions including cash deposit and withdrawal, transfer, purchasing financial products, making payments for goods and services, etc. Type 2 account can be used to purchase financial products, but limits transfers or payments to below certain thresholds. Type 3 account is limited to payments, subject to a specific volume cap. Both Type 2 and Type 3 accounts cannot be used to make cash deposits and withdrawals, and do not have physical cards associated to these accounts.

Type 1 accounts can only be opened through face to face. Types 2 and 3 can also be opened through remote video teller machines, smart teller machines, online or through smart-phones. When these remote onboarding opening channels are used, banks are required to apply additional CDD measures with the aim of effectively mitigating risks: customer's identity has to be verified by bank staff on site.

Countries should communicate the results of the national ML/TF risk assessments to financial institutions which enable them to develop financial inclusion products and services commensurate with national risks and in line with national financial inclusion priorities. Some countries may elect to define the appropriate parameters for the thresholds and other limits and requirements applicable to the tiered CDD approach, while other countries may have flexible laws/regulations that permit tiered CDD. Tiered CDD criteria are highly dependent on the national context, i.e. the profile of the financial excluded groups, their financial needs, the ML/TF risks in the country, the AML/CFT measures already in place, the existence of a national identification register, the technology available to monitor transactions etc. The number of tiers in the CDD regime should depend on the characteristics of the financial products and the needs of the low income, unserved or underserved groups.

Box 3. **Guatemala – Small account threshold based on an average income analysis**

In 2011, Guatemala conducted an income analysis based on the monthly minimum wage in the country, which was approx. 273, 44 USD, and the average remittances received on a monthly basis (according to the International Organization of Migration) which was 283, 74 USD (total monthly income of 584, 4 USD). Guatemala worked on the assumption that a family receives remittances and a salary on a monthly basis, or two minimum wages per month for their subsistence. On this basis, households with an average monthly income of less than 625 USD can benefit from simplified CDD measures.

Some countries laws and regulations provide flexibility for financial institutions to offer tiered accounts, according to the financial institutions' own criteria and account design, and based on the financial institution's own evaluation of identified risks, in accordance with national ML/TF risks. In adopting such an approach to permitting tiered CDD, it is important that supervisors closely follow-up with financial institutions and providers and assess their compliance rules and processes to confirm that they will have the resources and capacities to implement such a scheme. Supervisors

also need to check that proper account parameters and mitigating measures are in place and commensurate with risks identified at national level.

Box 4. **Peru – Simplified CDD measures based on a specific authorisation of the supervisor**

In 2015, the financial supervisor of Peru (SBS) issued a revised general AML/CFT regulation that enables financial institutions to apply simplified CDD measures, based on an authorization granted by the SBS for a specific product or service. When the SBS authorisation is granted, financial institutions only have to collect the full name, type and number of ID document of the customer, and the verification is done though the National ID or International ID (for foreigners). In the standard regime, customers would also be requested to provide information on their nationality and residence, phone number and/or e-mail address, occupation and name of employer.

b) Restriction of product functionalities and services

Financial inclusion products and services may present a lower risk when they are subject to restrictions or have certain features that address ML/TF risks identified in a risk assessment.[11] Such restrictions limit the attractiveness of the relevant products and services to criminal abuse, as well as the consequences of any abuse that may occur. Risk mitigation restrictions may apply to the way the business relationship is established or transactions are conducted (e.g. face-to-face only, or non-face-to-face with proper safeguards applied); the holder/beneficiary of the product (e.g. only natural persons who are nationals) or the geographical scope of the transactions (e.g. only domestic transactions or no cross-border transactions with countries with higher ML/TF risks). Examples of other restrictions include limiting the functionalities such as the number or total value of transactions per week/month, the amount per transaction, the overall monthly balance and/or the overall value of the account. The type of the restrictions required and whether more than one type of restriction will need to be imposed will depend on the risks identified during the risk assessment.[12]

11 Basel Committee on Banking Supervision Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion (2016) 29.

12 Basel Committee on Banking Supervision Range of Practice in the Regulation and Supervision of Institutions Relevant to financial inclusion (2015) 41.

a conservative view of what constitutes appropriate identity elements or identifiers, (e.g. date of birth, gender, source of income and address) and identification data which is often based on the use of identity documentation available to most members of the community (e.g. government-issued ID documentation or passport). This approach is also influenced by the guidance defined by banking supervisors and regulators at national and international level.[13]

Some countries do not prescribe specific identification sources, or include a broad list of valid documentation and data for purposes of proving identity and/or alternative or new means of identity verification. This approach is used to facilitate access to regulated financial services, including for foreign resident/people.

Box 6. **United States – A risk-sensitive application of the Customer Identification Programme**

In the United States, the RBA to the Customer Identification Programme (CIP) Rule under the Bank Secrecy Act (BSA) does not require a bank to establish the accuracy of every element of identifying information obtained. The bank must verify enough information to form a reasonable belief that it knows the true identity of the customer. Importantly, the CIP Rule permits flexibility with respect to the types of identifying information required in ways that facilitate financial inclusion. For example, if an individual does not have a residential or business street address, or an official Post Office box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer's physical location, can be used, potentially accommodating homeless persons. Equally, where banks opt to use documentary methods to verify a customer's identity, the federal banking agencies' expectation is that banks will review an unexpired form of identification issued by a government agency to the customer, evidencing nationality or residence and bearing photograph or similar safeguard, such as a driver's license or passport. The CIP Rule neither endorses nor prohibits a bank from accepting particular types of government identification cards. The CIP Rule also permits use of non-documentary identification/verification methods, such as independently verifying identity through a third party, such as a credit reporting bureau (consumer credit report), public database or other source; an inquiry to a fraud detection system; and more traditional non-documentary methods, such as contacting a customer from the phone information provided, checking references with other financial institutions, and obtaining a financial statement.

a) Alternative and new means of identification applicable to all customers

In some countries, national authorities (Central banks, FIUs) have taken initiatives to clarify and provide guidance on how to perform identification and verification of a customer's identity when the individual cannot provide "traditional" forms of identification. Those guidelines illustrate what constitutes a "reliable and independent" identification documentation and data in the

13 Such bank practices are often influenced by guidance from the regulators or, internationally, by guidance such as the Basel Committee on Banking Supervision General Guide to Account Opening and Customer Identification (2016) and annex to its Sound management of risks related to money laundering and financing of terrorism (2017). This guidance, in turn, should be read in the context other Basel Committee publications specifically addressing financial inclusion. See Range of Practice in the Regulation and Supervision of Institutions Relevant to financial inclusion (2015); and Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion (2016).

national/regional context. They often include a non-exhaustive list of adequate documentation, and provide scenarios that would be considered as meeting the requirements of the law, including for example, a voter card, tax card, employment card etc. Acceptable documentation can also extend to a reference letter from a "suitable reference", i.e. a person who knows the customer, and can confirm the customer's identity.

Box 7. **Switzerland – RBA to verifying customer's identity in specific situations**

As a rule, all Swiss banks must adhere to the regulations and considerations governing the opening of bank accounts, including the " Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 16)", which requires that banks prove the identity of their customers using government issued identification documents. The decision as to which documents to accept remains within the discretion of the individual banks, leaving banks free to deal with specific situations as appropriate in keeping with a RBA. In very exceptional cases where the identity of the customer cannot be verified in the prescribed manner, for instance because an individual has no identification documents, the bank may verify the identity by inspecting other credentials or by obtaining corresponding attestations from public authorities. Attestations and copies of substitute documents must be kept on file, and a file memorandum must be created explaining the reasons for the exceptional situation.

Box 8. **Canada – Flexible means of customer's identification when prescribed measures cannot be used**

In cases where banks cannot ascertain the identity of the client using prescribed AML/CFT measures, they can open deposit bank accounts for low-risk clients to allow for financial inclusion. Regulatory amendments of the AML/CFT framework that came into force in June 2016 allow retail deposit bank accounts to be opened for clients using more flexible means (such as non-photo ID issued by a government, or certain photo IDs not issued by government).

Box 9. **New Zealand - Amended identity verification Code of Practice**

The 2013 Amended Identity Verification Code of Practice (Code) allows new measures for verifying the identity of low and medium risk customers: international certification requirements (clarification that a trusted "referee" cannot be a person involved in the financial transaction or business requiring the certification); electronic (online) identity verification; reliance on a single independent electronic source of verification when that source establishes a high level of confidence; biometric identification measures. Verifying the identity of customers through one of the means referred to in the Code provides a 'safe harbour' to all reporting entities.

Box 10. **Fiji – Letter from a suitable "referee"**

In 2007, the Fiji FIU adopted provisions allowing financial institutions to rely on birth

customer.[14] In some countries, some established financial institutions have shown some initial reluctance to use these alternative identification data for CDD when dealing with customers who lack standard identification documents. Their reluctance was driven generally by fear that these alternative methods would be abused by customers and branch staff and applied in cases where customers were not eligible. National authorities should work with financial institutions to promote this flexible approach, through an education programme, ongoing dialogue, and regular feedback and interactions on lessons learned.

A growing number of countries are adopting innovative, technology-based means to verify customer identity. Some countries have set up country-wide national population registries that financial institutions can use to verify the identity of their clients. Some of these registries store biometric data, such as fingerprints and iris scans. One of the key challenges for these technology- -led solutions is for countries and for financial institutions to build the necessary infrastructure – adequate readers and sufficient internet connectivity to allow for real-time or similarly reliable authentication of the captured biometric data with the central database,[15] to ensure that the network of agents is technically equipped and capable to conduct identity verification, and to guarantee a satisfactory degree of certainty on whether the risk of identity fraud is adequately managed. The costs of using the real-time verification system can also be challenging for financial institutions. In addition, stringent data protection and privacy measures must be implemented across the system to ensure the data integrity, prevent data leakages that can facilitate identity fraud, including by money launderers and terrorist financiers, and to protect individuals' privacy and combat abuse.

Box 13. **India – e-KYC process**

Banks can use the Unique Identification Authority of India (UIDAI, also known as Aadhaar) as an electronic identity authentication process. The Aadhaar number is linked to biometric information stored in a central UIDAI database that includes fingerprint and iris scans and a photograph of the person. The database also includes demographic details, such as the individuals' name, address, date of birth, and gender. A customer can present his/her Aadhaar number at any banking location (a branch of any type bank or an agent/correspondent) that is equipped with a biometric fingerprint reader. The customer has to provide the bank with permission to obtain e-KYC[16] details from the UIDAI database and get his/her fingerprint captured. The bank then sends the customer's Aadhaar number and fingerprint to the UIDAI server. If the information matches, a bank can instantly open an account for the customer.

14 FATF Guidance on financial inclusion, 2013, para. 82

15 More details on the Aadhaar experience in India are available from: www.slideshare.net/CGAP/operational-innovations-in-amlcft-compliance-processes-and-financial-inclusion-emerging-case-studies (slides 56-60).

16 e-KYC refers to electronic means to conduct the customer's identification process, and allows the digital or online verification of customer identity https://www.rbi.org.in/scripts/FAQView.aspx?Id=82

Box 14. **Colombia –**

Box 17. **Spain – A large range of valid documents to verify a customers' identity, including the resident card**

Under the Spanish AML Regulation, foreigners can use the foreign identity card or the resident card as valid documents for identification purposes to open an account. The resident card is an official document, called NIE, issued by the Spanish Police within a very short timeframe, especially in cases of refugees or persons who seek asylum. It provides a means for foreigners to promptly obtain the necessary documentation in order to have access to financial services.

Box 18**. Australia - CDD procedures for Aboriginal and/or Torres Strait Islander people**

In Australia, in June 2016, the FIU issued a Guidance on CDD procedures for Aboriginal and/or Torres Strait Islander people.[1] The objective was to support the financial inclusion of Aboriginal and/or Torres Strait Islander people by presenting examples of scenarios where a reporting entity could utilise an alternative reference document provided by an indigenous customer to complete customer identification requirements, for example, a statement of referral made by a person of standing in the community (such as a tribal elder, medical practitioner or school principal), or a photographic reference provided by an entity, such as an indigenous land corporation. The Guidance also applies to a wider range of disadvantaged persons, such as persons who have been resettled in Australia as refugees

1. www.austrac.gov.au/aboriginal-andor-torres-strait-islander-people

Box 19. **Jordan – Using United Nations High Commission for Refugees (UNHCR).3 15oo.004Tw 0.3BT/C226dn**

Box 21. **US/Mexico – Use of the Consular Identification Card and Individual Taxpayer identification number**

The Matrícula Consular de Alta Seguridad (MCAS) (Consular Identification Card) is an identification card issued by the Government of Mexico through its consulate offices to Mexican nationals residing outside Mexico. An application for a MCAS must be submitted in person to a consular office. The applicant must present a Mexican birth certificate accompanied by a photo ID issued by a Mexican government authority, for ex. a voter registration card, passport, military service card, or old/expired MCAS. Financial institutions in the US may accept this card as an identification document. Through a programme providing information and counselling to migrants in the United States (Ventanilla de Acesoria Financiera), migrants are informed of the financial institutions in the area that accept the MCAS as an identification card.

Box 22. **Israel – Alternative arrangements for asylum seekers**

In Israel, asylum seekers who do not have a passport can use the temporary certificate issued by the State, as an alternative ID document to open a bank account. The applicant has to declare in writing that this is his/her sole account in the country. Limitations of service to mitigate the risk apply, such as a ceiling with regard to the balance in the account, which is set by banks depending on the customer's risk profile.

2. Simplified due diligence regime

Simplified CDD never means an exemption from CDD measures. A simplified set of CDD measures may be basic and minimal but must still respond to each of the four CDD components of R. 10 that apply to "standard" customer relationships and transactions (identification/verification of customer, identification/verification of beneficial owner, understanding the purpose and nature of the relationship, ongoing monitoring of the relationship). In line with the RBA, it is the timing, intensity and the extent of customer information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level. Simplified measures can be applied to all four CDD components, and not only to the identification/verification of customer part.

In a lower risk context, fulfilling customer identification, verification and monitoring requirements of R. 10 could for example entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information. INR. 10 para. 21 provides a number of examples of possible simplified measures with respect to the timing and verification of customer identity and intensity of transaction monitoring. These examples are proposed for guidance only and should not be considered as prescriptive or exhaustive.

Reduction on the extent of identification information required - Simplified identification measures can depart from "normal" CDD requirements regarding the range of information that the client has to provide, or the timing of verification.

Box 23. **Colombia – Basic ID information required**

In Colombia, simplified CDD requirements for electronic deposits are the same as for traditional savings accounts for individuals, and low-amount insurance products and low-amount consumer credit. Financial institutions must request and verify information included in a client's ID (provided to all Colombians): full name, ID number and ID issuing date, and verify this information (see box 14). Financial institutions are not required to keep records of signatures or fingerprints. Standard CDD requirements would additionally require the full name, ID number, address and telephone number of the legal representative or attorney; date and place of birth; residential mailing address and telephone; occupation or profession ; type of employment and economic activity; name, address, fax, telephone of employer or main office and branch or agency.

Box 24. **Egypt - Simplified due diligence measures for mobile payment services**

The FIU has defined SDD measures for mobile payment services which fulfil a set of predetermined thresholds and services limitations (for example, daily transactions not exceeding 286 EUR; monthly transactions not exceeding 2 400 EUR for natural persons and 4 800 for legal persons; maximum balance for any single account not exceeding 476 EUR at any point of time; maximum balance for all accounts of a single customer at a bank not exceeding 476 EUR at any point of time). The SDD regime includes: fewer documents to verify customer's identity, less data required when conducting domestic mobile transfers, the possibility to update customers' data and documents, using electronic means, permitting certain categories of service providers to conduct CDD procedures according to a set of prerequisites, permitting banks not to request the purpose and intended nature of the business relationship when it is quite obvious and can be easily inferred from the customers' activities and needs, the possibility of conducting CDD procedures at customers' premises.

Box 25. **Honduras - Simplified measures for opening of basic accounts and e-wallets**

The National Commission of Banks and Insurance (CNBS) developed a simplified due diligence regime for basic accounts and e-wallets which fulfil a number of conditions. For instance, the basic savings deposit accounts must be opened by natural persons of Honduran nationality only; they are only offered in national currency; the maximum balance is 363 EUR per month (amount that may be adjusted by the CNBS); the maximum amount of deposits or withdrawals accumulated monthly in the basic account is 726 EUR; there is no overdrafts to these accounts; and no withdrawals without the express authorization of the holder etc.. Under this regime, only the customer's full name, as shown in the identity card, his/her address, and land line and cell phone numbers, if any, are required. This information shall be checked against the information in the National Register of Persons (RNP), within up to 30 calendar days after the opening of the basic account or e-wallet. In comparison, the standard CDD procedure requires a set of 21 information items from potential customers

Postponing the verification of the identification information- R. 10 conceptually separates identification and verification (authentication), permitting identity verification to take place within a

certain conditions). Under appropriate, risk-based circumstances, justified by a thorough risk assessment, a tiered account approach (see above) could permit delaying verification of customer identity until a specified threshold is reached, based on, e.g., total account value, transaction value, or transaction velocity Examples of simplified due diligence measures in INR. 10 include verifying the identity of the customer and the beneficial owner after the establishment of the business relationship.

Box 26. **India -"Small accounts"**

"Small accounts" can be opened by individuals who do not have any proof of identity and address. These accounts can only be opened in the physical presence of the client at the bank, and on the basis of a self –attested photograph and affixation of signature or thumb print, in the presence of a bank official who certifies the signature of the prospective customer. These accounts are valid for a period of twelve months. Thereafter, such accounts are allowed to continue for a further period of twelve more months, if the account holder provides a document showing that she/he has applied for any of the officially valid document/Aadhaar number/Permanent Account Number (PAN), within twelve months of opening the small account. See also box 13 for the application of the e-KYC process.

Relying on a broader range of acceptable means of identity verification- The use of less formal or alternative means to verify the identity of the potential customer (ex. non-photo ID issued by a government ID without a photo, expired ID, healthcare document) can be envisaged as part of the SDD measures.[20]

Box 27. **Brazil - Simplified verification for electronic accounts**

Since the April 2016 Resolution of the National Monetary Council, natural persons can open accounts by using electronic means (remote channels and instruments used to communicate and exchange information, with no face-to-face contact between customers and institutions). The customer's signature can be collected by electronic means or substituted by a digital signature. Financial institutions must adopt procedures and controls that ensure the customer identification and verification and the authenticity of information, as well to adjust the procedures regarding AML/CFT, including the comparison of the information provided with those available on public or private database. They must also ensure the overall integrity and security of the electronic means used.

Identifying and verifying the beneficial owner based on information from the customer's profile - Regarding beneficial ownership requirements, in a financial inclusion context the beneficial owner will in most instances be the individual customer him/herself, or a closely related family member. Situations where suspicions arise that the account holder is used as a straw-man, or frontman and is not the real owner, should not be treated as a lower risk and normal, or even enhanced, CDD measures should be applied (INR. 10 par. 15 a, last bullet).

20 See Section III. 1. a)

Other examples of SDD measures - INR 10 mentions other examples such as reducing the frequency of customer identification updates, not collecting specific information, inferring the purpose and intended nature of the business relationship from the type of transactions or business relationship established, rather than collecting specific information or carrying out specific measures for this purpose (see box 24 on Egypt).

Ongoing monitoring of the relationship - Countries should also note that having a lower ML/TF risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions (INR. 10 para. 18). In most cases, the implementation of SDD measures is subject to specific thresholds or restrictions on the type or value of transactions that can be performed. Therefore ongoing monitoring should remain at the "standard" level, to verify that the transactions remain within the risk-based thresholds and in line with the customer's risk profile.

To manage the ML/TF risks associated with the trustworthiness of customer identification and verification data, financial institutions may choose to apply enhanced monitoring of the transactions or relationships. This may involve a regular and frequent review of the transaction patterns (especially when transactions are inconsistent with the customer's profile) and a focus on potentially suspicious transactions. It is important to ensure that simplified CDD at account opening provides enough information to be supportive of effective customer monitoring. Monitoring will not be effective as a control when an institution has too little information about its customers and their expected use of the relevant financial products.

Box 28. **Guatemala – Specific monitoring measures for small accounts**

Reporting entities that open small accounts must establish specific monitoring measures to verify that the amount of the transactions during a calendar month does not exceed the maximum of 663,5 USD. When this ceiling is reached in the course of a calendar month and/or when the customer accumulates in the account more than 2 654, 1 USD in a calendar year, the entity shall obtain from the customer the identification information required from "regular" customers. Ongoing monitoring systems of reporting entities should also prevent the abuse of small accounts, in particular through structuring transactions.

Box 29. **Fiji – Specific monitoring of accounts opened based on "referee" certificates**

In 2007, Fiji adopted provisions that enabled financial institutions to rely on birth certificates (available to all citizens) and a confirmation letter from a suitable "referee" when verifying customers who have insufficient formal ID documents (see box 10). Fiji considered the risk that use of referee certificates could be abused by members of the public due to the ease with which these could be obtained. To mitigate this risk, financial institutions were advised by the FIU to specifically monitor customers' accounts and transactions for any unusual transaction or pattern of transactions when account opening relied on a "referee" certificate.

specific circumstances, for example face-to-face via a non-bank agent or through a mobile phone or an e-money issuer. In some countries, this approach is supported by measures to regulate the issuing and operation of cell phones (registration and identification requirements) and mobile money (SDD/CDD requirements).

Box 30. **Ghana – CDD tiered approach for mobile money services**

In Ghana, the Central Bank published guidelines in 2015 to regulate the issuing and operations of electronic money. Non-bank e-money issuers have been allowed to enter the market. Customer accounts opened are categorised in three levels, with different CDD requirements for each, as part of a RBA. Level 1 is a minimum CDD account with very low transaction limits and documentation requirements.

In such digital financial services-focused initiatives, countries must calibrate regulation to ensure that the digital products and services are sustainable and lead to offering financial services that meet excluded and underserved customers' needs. Facilitating access to regulated, basic payment services is a key step to providing people with affordable and safe ways to send remittances or pay for goods and services. To meet broader financial inclusion objectives, countries should also introduce relevant measures to encourage providers to migrate "over-the-counter" customers, who *transfer money without opening a mobile wallet account, or obtaining other digital financial account-like services,* to account-based digital financial products and services. Clients should also get, progressively or concurrently, easy access to the larger range of needed financial services beyond e-money payments and value storage, including tailored savings, credit, insurance, and investment products.[22]

In some countries, branchless banking approaches have been developed through large networks of non-bank agents (ex. retail shops, petrol stations, lottery kiosks) covering the national territory, including rural and remote areas to reach unserved groups of people, and involving SDD. In such cases, countries need to ensure that key conditions are fulfilled to ensure that when financial institutions rely on third parties for CDD purposes or outsource the distribution of their products to other, non-financial services providers, CDD procedures are effectively conducted by the agents and financial institutions remain ultimately responsible for meeting their AML/CFT obligations. National requirements should:

- establish the unequivocal responsibility of the supervised financial institution for the sound and safe functioning of the system. This includes effective training and oversight of the network of agents to ensure that all of them are fully aware of their AML/CFT duties;
- make supervised institutions accountable for actions of their agents, including in the AML/CFT field, through agent agreements and agents managers, and responsible for the consequences in

In addition, countries may also permit financial institutions to rely on CDD conducted by third parties that are not agents of the financial institution, under the conditions specified in R. 17.

APPENDIX

EXPERIENCES FROM THE WORLD BANK'S SUPPORT TO FINANCIAL INCLUSION PRODUCT RISK ASSESSMENTS

THE WORLD BANK'S FINANCIAL INCLUSION PRODUCT RISK ASSESSMENT MODULE (FIRM):

The World Bank has developed a standalone ML/TF risk assessment module specifically to facilitate the assessment of the money laundering terrorist financing (ML/TF) risks associated with financial inclusion products in a systematic and evidence-based way. The module is based on following four steps:

Step 1–Analysing the product features and their risk implications At the first step of the assessment, the assessor identifies the features of the product and their possible implications on the money laundering/ terrorist financing risks. For example, having features such as "availability of international transactions", "non-face-to-face account opening", "anonymity", "delivery through agents", "availability to non-resident/non-citizens", or "availability to legal persons" increases inherent risk of the products and therefore, the need for stronger mitigating measures. In contrast, introducing a cap on transaction size and/or number or limiting some of the functions of the product reduces the risk level.
Step 2– Assessment of Risk Mitigation Measures The second step of the assessment focuses on the adequacy and quality of risk mitigation measures that are linked with each product feature. For example, if the product has a cap for amount or number of transactions, the module asks questions about the existence and quality of the analytical work that informed the decision for this cap. If the product allows international transactions, the module asks questions about the quality of relevant monitoring mechanisms of the institution. Moreover, if the product is offered through agents the procedures for onboarding, training, and monitoring of the agents need to be assessed.
Step 3– Assessing the impact of country risk context on the product The risk context of the country is important, because a financial inclusion product that may have low risk in a certain country context may not be necessarily low risk in another country. Step 3 of the assessment allows users to reassess the mitigation measures, considering the country's money laundering /terrorist financing threat and vulnerability context. The quality of the supervision and institution's capacity to detect and mitigate the risks are also assessed in this step. Inputs from country's national ML/TF risk assessment are crucial for this step.

23 Formerly named as FIRAT.

Step 4– Overall assessment

This final step facilitates the assessment of the ultimate net risk level which is a function of the product features, risk mitigation measures, and country's risk context. The country or institution may consider (or justify) a simplified CDD regime only if the assessment results in "lower" or "low" risk. If the assessment results are "medium" or "high" the country may use the module as a basis for the redesign of the product, then reassess the risk level. Limiting the functions of the product, lowering the caps, or improving the control and mitigation measures may reduce the risk level of the product.

The module has been used by a diverse group of countries in the assessments of their current or planned financial inclusion products. These countries include Botswana, Uganda, Armenia, Guyana, India, Tajikistan, Tanzania, Jamaica, Bangladesh, the Democratic Republic of Congo, Dominican Republic, El Salvador, Ghana, Guatemala, Malawi, Namibia, Nigeria, Nepal, The Philippines, Pakistan, Sierra Leone, Sri Lanka, and Zambia. The assessment of financial inclusion products was done as part of national risk assessments in most of these countries and as a standalone assessment in some others.

While being used for assessment and testing of the ML/TF risk of financial inclusion products, FIRM has served mostly as a diagnostic tool in these countries and has not been used as a basis for redesign of CDD regulatory framework so far. Thus, it has not been subject to any direct review or assessment during any mutual evaluation[24].

THE DIAGNOSIS OF THE IMPEDIMENTS TO FINANCIAL INCLUSION IS ESSENTIAL TO DETERMINE THE MOST APPROPRIATE POLICY FOR SIMPLIFIED CDD:

The Financial Inclusion Risk Assessment Module is being introduced to countries in a workshop. Typically, this workshop brings together experts from the financial intelligence unit, the financial sector supervision department, the financial inclusion department or group (usually part of the central bank), telecom authorities (with regulatory responsibilities for mobile money), and representatives from the private sector. The main objective of this workshop is assessing the impact of a country's current AML/CFT regime on financial inclusion and analysing how and to what extent possible simplifications of CDD requirements can help reduce financial exclusion.

This workshop usually provides a clear idea about the interplay between the current CDD requirements and financial inclusion in the country.

In some countries (such as Zambia, Tanzania, Bangladesh) this analysis showed that some parts of the CDD requirements were too stringent for the country conditions and were impeding access of certain low risk categories of customers to finance. On the other hand, in some other countries like India, the analysis concluded that the country's CDD regime was flexible enough to accommodate

24 Among the countries listed in previous paragraph, DRC, Sri-Lanka, and Guatemala have gone through mutual evaluations recently. DRC and Guatemala reports have limited references to FIRM. In Sri Lanka report, the assessors recommended a more flexible CDD regime that allows simplified CDD and supports financial inclusion. This is in line with the results of financial inclusion product risk assessment done by the country based on FIRM.

inclusion d that the developments in e-KYC further reduced the need for relying on d CDD pr ces.

The kshop rt with a stocktaking discussion that attempts to analyse the country's CDD regula ry work in force, as well as the state and reasons of financial exclusion. Next, the finan on risk assessment module is being introduced to the country's in-house assessors. Foll four-step methodology, explained in the previous page the assessors use the module g the risk evel of current or planned financial inclusion products/services in the country.

ME EXAMPLES FINANCIAL INCLUSION PRODUCTS WITH A LOWER OR LOW ML/TF RISK:

The table s a sample of the financial inclusion products that have been assessed and found or "low risk" by some of the countries which used the module. As seen in the s of countries concluded that their regulatory framework requires revisions to better the mplified customer due diligence and accommodate financial inclusion.

Examples of financial inclusion products assessed and found to be "lower" or "low risk"

Cou y	Financial Inclusion Product with Low or Lower ML/TF Risk*	Assessment's Conclusion on CDD Regulatory Framework
ngladesh	r Accounts. Banking Accounts. nts for Street Children.	Country's regulatory framework required revision to facilitate simplified CDD.
	Bank Accounts	Country's regulatory framework facilitated simplified CDD.
Malawi	Basic Saving Accounts. Basic Credit Accounts. Ordinary Farmer Bank Accounts. Micro-Credit.	Country's regulatory framework required revision to facilitate simplified CDD.
Nigeria	Low Amount Saving Accounts. Micro-Insurance Products. Micro-Credit Products. Some Mobile Money Products.	Country's regulatory framework facilitated simplified CDD.
Sri Lanka	Micro-Credit Products. Community Lending Products. Micro-Insurance Products.	Country's regulatory framework required revision to facilitate simplified CDD.

Country	Financial Inclusion Product with Low or Lower ML/TF Risk*	Assessment's Conclusion on CDD Regulatory Framework
	Certain Mobile Money Products Certain E-Wallet Products. Zanaco Xapid Account	

*The countries assessed a broader range of products. The products that were not found to be low risk did not qualify for simplified CDD- and have therefore not been included in this table.

COMMON ISSUES RELATED TO AML/CFT REGULATION OF FINANCIAL INCLUSION PRODUCTS:

Conducting the financial inclusion product ML/TF risk assessment in more than twenty countries revealed some issues which can also be of relevance to other countries seeking solutions to strike a balance between financial integrity and financial inclusion:

- In some countries,

- Lack of public-private dialogue for striking a balance between financial inclusion and customer due diligence requirements is

2013 FATF GUIDANCE ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION

EXECUTIVE SUMMARY

The promotion of formal financial systems and services is central to any effective and comprehensive AML/CFT regime. However, applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the formal financial system. The FATF has therefore defined a Guidance to provide support in designing AML/CFT measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime. The main aims of the document are to develop a common understanding of the FATF Standards[25] that are relevant when promoting financial inclusion and explicit the flexibility that the Standards offer, in particular the risk-based approach (RBA), enabling jurisdictions to craft effective and appropriate controls.

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

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

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

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

INTRODUCTION – BACKGROUND AND CONTEXT

Preliminary remarks

20. r9760

FATF members and observers but also more broadly from non-FATF and APG participants (individual jurisdictions and other FATF Style Regional Bodies (FSRBs)) and the private sector, through the FATF Private Sector Consultative Forum and beyond[29]. A first version of the Guidance was adopted in June 2011, based on the 2003 FATF Recommendations.

4. The FATF believes that this Guidance paper greatly contributes to the common objective adopted by the G20 to carry forward work on financial inclusion, including implementation of the *Financial Inclusion Action Plan*[30], endorsed at the G20 2010 Summit in South Korea. The 2010 Summit decided to launch the Global Partnership for Financial Inclusion (GPFI) as the main implementing mechanism. The GPFI is an inclusive platform for G20 countries, non-G20 countries, and relevant stakeholders intended to advance the "Principles for Innovative Financial Inclusion"[31] through multiple channels, including by encouraging standard-setting bodies to take full account of these principles[32]. The White Paper *Global Standard-Setting Bodies and Financial Inclusion for the Poor - Toward Proportionate Standards and Guidance*, adopted by the GPFI in September 2011 notes the steps taken by five international standard-setting bodies, whose activities are relevant to financial inclusion[33], to integrate–financial inclusion into their standards and guidance. It also underscores the critical importance of taking a proportionate approach to regulation that reflects (i) the risks of financial exclusion, (ii) the risks of increasing financial inclusion and (iii) country context in particular, countries that have high levels of financial exclusion and low regulatory capacity[34]. The White Paper welcomed the adoption of the FATF 2011 Guidance paper and highlighted the leading position taken by FATF to facilitate the implementation of its Recommendations whilst taking financial inclusion into account.

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

6. After an extensive consultation with both the public and the private sectors, this updated Guidance paper was adopted by the FATF at its February 2013 Plenary[35].

Scope of the February 2013 Guidance Paper

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

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

[31] See Annex 2

[32] 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.

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

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

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

7. The June 2011 version of the Guidance paper was developed within the framework of the 2003 FATF Recommendations. This 2nd version of the Guidance seeks to reflect the changes brought by the revised set of Recommendations, adopted on 16 February 2012[36].

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

9. The Guidance paper examines the existing requirements that are the most relevant when discussing the linkage between AML/CFT policies and the financial inclusion objective. It also refers to other initiatives that the FATF has already launched that have important linkages with financial inclusion[37].

Objectives of the Guidance

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

11. This Guidance paper does not explore how financial inclusion should be integrated into the mutual evaluation methodology and process. However, it highlights the need to better inform the assessors and the assessed countries based on the principle that financial exclusion could undermine the effectiveness of an AML/CFT regime given, among other things, the difficulty of detection (and enforcement of applicable law) in the informal sector[38]. A country's level of financial exclusion is

[36] FATF (2012)

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

[38] The precise nature and impact of financial exclusion risk differs from country to country. The identification and the assessment of the relevant risks depend furthermore on the policy and regulatory objectives that are threatened. Financial inclusion can for example impact on the objectives relating to financial integrity and consumer protection (see footnote 2). While the AML/CFT regulator and the FATF, for example, may focus on financial integrity risks, the banking regulator may focus on financial stability risks posed by financial exclusion. See CGAP (2012).

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

12. This Guidance focuses on financially excluded and underserved groups, including low income, rural and undocumented persons. It considers experiences in both developed and developing countries, although it focuses more on initiatives taken in developing countries where the challenge is the greatest. Since developing and developed countries differ with regard to the origin and the extent of financial exclusion, as well as possible ways to address the related challenges, this Guidance seeks to address a range of situations that jurisdictions should be able to refer to depending on their level of economic development[39].

Target Audience

13. The Guidance is intended for:

- The publ

certain financial sectors. Accordingly, different solutions must be adopted to address the specific factors that act as barriers for specific populations to specific financial services/products.

16. Along with the guidance set out in this document and for more specific aspects, jurisdictions should also refer to existing documentation that is available on the subject[41].

[41] See Bibliography and sources.

Anti-

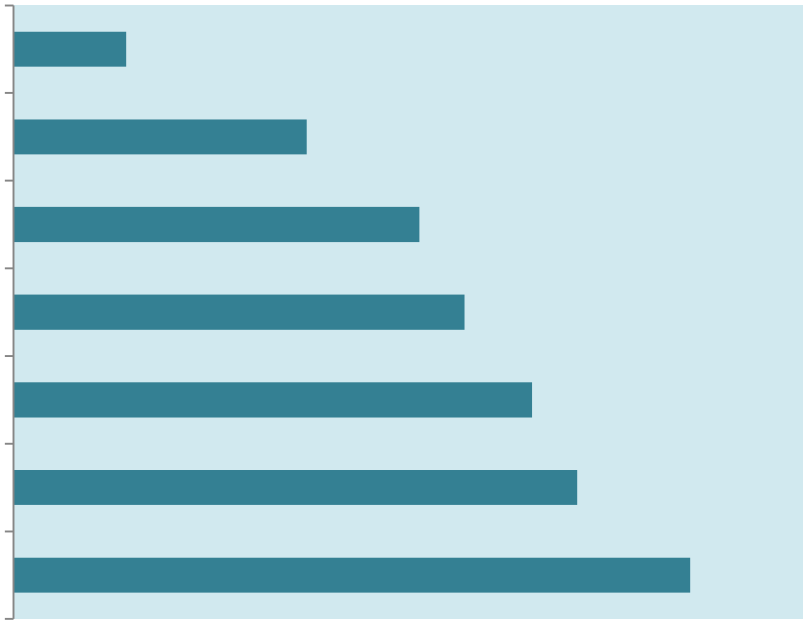
USD 2 a day, only 23% have access to a formal account[47]. Nevertheless, studies have demonstrated that a number of poor people in developing countries have developed sophisticated financial lives, transacting through remittance systems outside the formal bank sector, saving and borrowing with an eye to the future and creating complex "financial portfolios" using mainly informal tools[48].

20. As far as remittances are concerned, officially recorded flows to developing countries are estimated to have reached USD 372 billion in 2011, an increase of 12.1% over 2010. The growth is expected to continue at a rate of 7-8% annually to reach USD 467 billion by 2014[49]. However, some experts suggest that if informal and underreported flows were included, the total amount of migrant remittances would be considerably higher – possibly up two to three times higher[50].

The Diversity of the Financially Excluded and Underserved Groups

21. Disadvantaged and other vulnerable groups, including low income households, handicapped persons, individuals in rural communities and undocumented migrants in both develoe0.9(ig/MCID 71.1(x)

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



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

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

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

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

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

recent years to channel Government-to-Persons (G2P) payments, especially social protection benefits, through bank accounts[52].

26. There are also new financially excluded groups as a result of the introduction of inappropriate AML/CFT requirements which do not take into account the potential negative impact of such requirements. In some cases, the new AML/CFT requirements meant that services for those existing customers who could not provide the necessary documents had to be terminated[53]. In other instances it may mean that potential customers were not able to enter the formal financial system.

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

Balancing AML/CFT Requirements and Financial Inclusion

28. The impact of AML/CFT on the ability of socially and economically vulnerable people to access financial services has been under discussion for many years. In 2005, the World Bank supported a study to consider the impact of AML/CFT in selected developing countries. The report was published in 2008 and concluded that "*Measures that ensure that more clients use formal financial services therefore increase the reach and effectiveness of the AML/CFT controls"*[54]. Other studies, such as that conducted by CGAP in 2009[55], concluded that AML/CFT measures can negatively affect access to, and use of, financial services if those measures are not carefully designed**.**

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

30. In addition, new financial products and services have been created in the past few years which may contribute to expanding access to new markets and clients[56]. To date, challenges have appeared

---

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

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

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

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

[56] see Annex 5 for more details.

Anti-

CHAPTER 2 - GUIDANCE ON ACTION TO SUPPORT FINANCIAL INCLUSION

I. Preliminary Remarks

33. The FATF has identified a series of measures that financial institutions or any other profession subject to AML/CFT requirements must take on the basis of national legislation to prevent money laundering and terrorist financing. These measures, known as “preventive measures”, have been designed by the FATF to protect financial institutions from abuse, and help them to adopt adequate controls and procedures. Although these measures create challenging requirements, they have been elaborated with some degree o

guidance when institutions overestimate ML/TF risks or adopt overly-conservative control measures[62].

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

40. The application of the RBA, as outlined in Recommendation 1, requires as a starting point that countries take appropriate steps to understand, identify and assess the ML/TF risks for different market segments, intermediaries, and products on an ongoing basis[63]. This includes supervisors or other authorities assessing specific risks relevant to their functions. Equally, financial institutions are required under Recommendation 1 to understand, identify and assess the ML/TF risks relevant to their activities.

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

42. The FATF *Guidance on National Money Laundering/Terrorist Financing Risk Assessment*[64] defines key concepts and outlines the successive stages required to conduct a national risk assessment:

Box 31. **About the definition of risk**

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

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

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

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

[64] FATF (2013)

ML/TF risk assessment[1].

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

Note

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

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

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

- In general terms, the process of **identification** in the context of an ML/TF risk assessment starts by developing an initial list of potential risks or risk factors[1] countries face when combating ML/TF. Ideally at this stage, the identification process should attempt to be comprehensive; however, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.
- **Analysis** lies at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, the aim of this stage is to gain a holistic understanding of each of the risks – as a

43. The national risk assessment will provide useful background information to identify low risk situations which could benefit from an exemption, and lower risk situations for which simplified AML/CFT measures could apply. In the 2012 FATF Recommendations, FATF gives examples of circumstances where the risks of money laundering and terrorism financing could potentially be considered as lower, in relation to particular categories of customers, countries or geographic areas, or products, services, transactions or delivery channels (INR. 10 par. 17)[65]. The lower level of risk is very much determined by the national or local context and the specific environment of the customer. In most cases, a combination of several factors (such as the client's level of income, the business sector in which the client operates, the region's exposure to ML/FT threat etc.), rather than a single element, will be required. The risk assessment should therefore determine the common criteria according to which risks for a given market could be considered as lower.

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

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

46. It is important to emphasize that there is no requirement, or expectation, that an institution's RBA must involve a complex set of procedures. The particular circumstances of a firm's business, in particular its money laundering/terrorist financing risk will determine how it should implement an RBA: it should design and implement controls to manage and mitigate the risks, monitor and where relevant, improve the effective operation of these controls, and record what measures have been implemented and why. The appropriate approach is ultimately a question of judgement by financial institutions, expert staff and senior management. While no set of measures will detect and prevent all money laundering or terrorist financing, an RBA can serve to balance and focus the resources

terrorist financing, such as unaddressed history of terrorism financing activity or limited regulation of money or value transfer systems[70]:

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

51. As permitted by the FATF Recommendations (INR 1. par. 2), a country may take risk into account, and may decide not to apply certain AML/CFT measures to a particular type of financial institution or activity, or Designated Noin

9. Individual and collective portfolio management.

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

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

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

13. Money and currency changing.

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

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

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

or

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

3. 1. THE "PROVEN LOW RISK" EXEMPTION

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

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

56.

57. In most jurisdictions, the current exemptions or limitations on applying AML/CFT requirements to certain financial activities are essentially based on a "perception" of low risk because of the activity's size or nature (*e.g.*, leasing, factoring, life insurance) with little or no evidence to support the risk ranking. Only a few jurisdictions have undertaken risk assessments before exempting a sector. The World Bank has developed a tool to assess ML risk of financial inclusion products that may assist countries to undertake the required risk assessments[73].

3.2. THE EXEMPTION

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

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

60. The European Commission has attempted to define the notion of "financial activity carried out in occasional or very limited basis" in a systematic way in Article 2(2) of the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[74]. It provides a flexibility[75] similar to that set out in the FATF definition of financial institutions. Article 4 of Directive 2006/70/EC[76] which contains implementing measures for Directive 2005/60/EC sets out the technical criteria for simplified customer due diligence procedures and for exempting a financial activity conducted on an occasional or very limited basis. Using that legal framework and its safeguards, some EU members have opted for such exemptions.

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

[73] See Annex 6 II. for details.

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

[75] "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.

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

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

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

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

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

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

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

   (f) the person's main activity is not that of a person falling within regulation 3(1)(a) to (f) or (h)[77];

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

[77] *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.

Anti-

CDD measures - general

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

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

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

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

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

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

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

CDD measures - lower risk scenarios

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

transactions[82]. In line with the RBA approach[83], it is the intensity and the extent of customer and transaction information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level. In a lower risk context, fulfilling CDD customer identification, verification and monitoring requirements of Recommendation 10 could for example entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information.

72. INR. 10 par.21 provides a number of examples of possible simplified measures with respect to the timing and verification of customer identity and intensity of transaction monitoring. Again, these examples are proposed for guidance only and should not be considered as prescriptive or exhaustive. They include the possibility of verifying the identity of the customer and the beneficial owner after the establishment of the business relationship, reducing the frequency of customer identification updates or reducing the degree of ongoing monitoring and scrutinising transactions, based on a reasonable monetary threshold[84].

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

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

[82] See par. 65.

[83] See par. 37 and s.

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

be renewed for another 12 months if the account holder provides evidence that he/she has applied for valid identity documents within a year of account opening[85].

CDD measures – customer identification

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

76. The FATF Recommendations allow countries' laws or regulations to apply an RBA to the types of customer information that must be collected to start a business relationship. A carefully balanced approach has to be taken, because if identification processes are too lean, monitoring may make a limited contribution to risk mitigation, and manual or electronic scanning of transactions may not be able to identify individual suspicious activity effectively[86]. In some countries, differentiated CDD requirements have been introduced, in relation to certain types of financial products. For instance in Colombia, a 2009 modification of the Finance Superintendence of Colombia (SFC) Basic Banking Circular simplified AML/CFT procedures for low-value electronic accounts and mobile accounts that are opened via agents (who receive and forward the application materials).

CDD measures – verification of customer identification

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

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

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

[86] See also par 102.

79. The World Bank has pointed out that respondents to its recent survey often quoted lack of documentation as one of the central reasons for not having an account, especially in countries that require extensive or formal, government-issued documentation[87]:

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

Non-account-holders citing lack of documentation as a barrier (%)

Non-account-holders citing cost as a barrier (%)

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

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

80. *Relying on a broader range of acceptable identification means.* To address such challenges[88], countries have expanded the range of acceptable IDs for the verification process to include such documentation as expired foreign IDs, consular documents or other records that undocumented people can typically acquire in the host country (bills, tax certificate, healthcare document, etc.). Using an RBA, local authorities have often allowed a broader range of documentation in pre-defined

-

requirements with regard to acceptable IDs that will support the provision of relevant services to unserved groups[90].

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

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

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

84. *Postponing ID verification*–Amongst the examples of simplified CDD measures in INR. 10 par. 21, the verification of the customer's (and beneficial owner) identity after establishment of the business relationship is envisaged, *i.e.* if account transactions rise above a defined monetary threshold. As part of a tiered CDD approach[91], customers can be provided with limited and basic services, and access to a full or expanded range of services or higher transactions ceilings would only be granted once full identity verification has been conducted.

85. This flexible approach for limited purpose accounts, where verification is postponed but not eliminated, allows clients to get access to basic products with limited functionalities and for low-value transactions. It is very useful in a financial inclusion context since it enables unbanked individuals to get access to the basic formal services they need, and at the same time reduces the costs of small value accounts and increases financial inclusion outreach for financial institutions. Countries' experiences in dealing with identification and/or identity verification challenges are outlined in Annex 8.

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

[91] See par. 74.

CDD measures - Identification in non face-to-face scenarios[92]

86. The increasing use of technological innovations is a promising channel to expand the provision of financial services to unserved and remote population[93]. In this regard, mobile phone banking and mobile payments have developed significantly over the last years, and have major potential to facilitate access to basic services for unbanked people, especially in developing countries. According to the World Bank, around three quarters of the world's inhabitants now have access to a mobile phone, and the vast majority of mobile subscriptions (five billion) are in developing countries[94]. In Sub-Saharan Africa, the Gallup World Survey poll indicated that 16% of adults reported having used a mobile phone in the prior 12 months to pay bills or send or receive money[95]. Although mobile banking shows potential for financial inclusion purposes, at this stage, it primarily gives access to payment and transfer services. This functionality offers a useful first step to formal financial services but does not in itself provide the benefits of full banking or other financial services.

87. The development of branchless banking channels through non-bank agents (*e.g.,* petrol stations, lottery kiosks, grocery stores etc.), combined or not with mobile phone solutions, also offers significant potential by which financial services can reach the still unbanked or unserved groups[96].

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

89. As far as identification of lower risk customers at the account opening stage is concerned, financial institutions are requested to apply equally effective procedures as for clients with whom they meet. In a number of cases, although there is no direct face-to-face communication with the financial institution, a third party or an agent is involved in the account opening process. In this case, the principles relevant to agent or third party relationships will apply[97]. In most other cases, financial institutions require customers to send digital copies of their identification documentation, and the whole range of the account facilities are activated once the verification is completed[98].

90. *New products and technologies.* New FATF Recommendation 15 requires that countries and financial institutions identify and assess the specific risks that may arise in relation to the

[92] See also FATF (2013b).

[93] See G20 Fin-2.5(c)6.(T)-.3(n)(t)12993

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

91. Recommendation 15 is part of the section of the new Recommendations requiring additional CDD measures for specific customers and activities. This does not mean, however, that the use of new technologies to develop innovative distribution channels or products automatically calls for additional CDD measures in all cases. While an additional, particularized risk assessment of the new products business practices is required, the specific type of business relationships and transactions involved, the client target groups, the involvement of intermediaries, the sophistication of the technology used are all factors that must be taken into account in evaluating the risks, and determining the appropriate level of CDD that should be applied[99].

92. In the new technology/business practices/financial inclusion context, it is worth noting that the FATF Recommendations (INR. 10 par.11) allow financial institutions in non-face- to-face scenarios to verify the identity of the customer following the establishment of the business relationship (and not before or during the course of establishing a business relationship) when essential to not interrupt the normal conduct of business and provided that the money laundering risks are effectively managed[100].

93. *Reliance on third parties* - Reliance on CDD undertaken by third parties who are not agents of the financial institutions and are not covered by outsourcing agreements is permitted under the FATF Recommendations, provided that certain requirements are met (Recommendation 17). Third party CDD is not permitted in some countries, but when allowed, the ultimate responsibility for customer identification and verification must remain with the delegating financial institution. In a reliance scenario, a financial institution that is accepting a customer relies on a third party to perform some or all of the following elements of the CDD process (a) identifying the customer (and any beneficial owner), (b) verifying the customer's identity, and (c) gathering information on the purpose and intended nature of the business relationship. This information has to be provided immediately to the financial institution. Financial institutions must satisfy themselves that the third party is adequately subject to AML/CFT regulation and supervision by a competent authority and has measures in place to comply with the CDD requirements. New Recommendation 17 clearly limits such reliance on third parties to only other financial institutions (INR 17 par. 3). When they belong to the same financial group, the financial institution and the third party may be considered as meeting some of the required conditions as a result of their group-wide AML/CFT programme. In practice, firms develop measures to check the reliability of the third party (especially in a cross-border context) such as the degree of domestic AML/CFT regulation and supervision.

[99] See countries' experiences in Annex 7.

[100] See FATF (2013b).

Anti-

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

99. Monitoring under an RBA allows a financial institution to create monetary or other thresholds below which an activity will receive reduced or limited monitoring. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. Financial institutions should also assess the adequacy of any systems and processes on a periodic basis. The results of the monitoring should always be documented[101].

100. Some form of monitoring, whether automated or manual, a review of exception reports or a combination of screening criteria, is required in order to detect unusual and hence possibly suspicious transactions pp0.322 eer p9(r)5.3.9(p9(r)55.9..7(o)--0.008 6.2 p9(r)( )]Th7(ct)6e)3.8(d)-3.8(y322)

reasonable measures to make that determination are required in relation to domestic and international PEPs (Recommendation 12). What constitutes an appropriate risk-management system or reasonable measures to identify foreign PEPs could vary, depending on the risk presented by the customer base.

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

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

to comply swiftly with information requests from the competent authorities. The rationale is to facilitate the reconstruction of individual transactions and provide, if necessary, evidence for the prosecution of criminal activity.

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

110. Under the FATF Recommendations, the record keeping requirement does not require retention of a photocopy of the identification document(s) presented for verification purposes; it merely requires that the information on that document be stored and kept for five years. A number of countries, such as the United States, Australia and Canada, have considered, but rejected, imposing photocopying obligations on their regulated institutions for a number of reasons: for example, the photocopies could be used to commit identity fraud; their retention may breach privacy laws and they may reveal information about the client that could form the basis of discriminatory practices, such as the refusal of credit facilities[103].

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

- Scanning the verification material and maintaining the information electronically;
- Keeping electronic copies of the results of any electronic verification checks;
- Merely recording (hand-writing) reference8 Tw 11.0(36f(t(c)-3.7(s)l10.7(r)2.4(p)1.6(ab

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

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

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

115. In most countries, transactions with vulnerable categories of clients are not deemed to be subject to separate or specific monitoring systems to identify suspicious transactions. However, some businesses may have developed indicators. For example, money transfer businesses[104] would focus on the following, in addition to other criteria, such as systematic monitoring:

- A lack of cooperation at the counter when further questions are asked or suspicious behaviour is detected.
- An identified transaction pattern that is not consistent with the status of a financially excluded individual: *e.g.,* consumers who are sending or receiving large amounts of money are typically less likely to have limited access to ID documents (from the country of residency or from the country of origin). This disconnect is a source of potential ML/TF risks.
- Any signal that a consumer is engaged in a TF initiative, whatever the amount of money sent.
- Any signal that a consumer tries to bribe / influence the agent or staff at counter or is producing wrong information and recognizes it.

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

116. *General.* The use of non-bank agents to distribute financial services is part of an increasingly popular model for financial inclusion in many countries. Most of the countries that contributed to

[104] Based on the experience of Western Union.

this Guidance paper have developed some forms of agent banking options, some of which are referred to as branchless banking, or banking beyond branches. In these countries, banking and payment services are provided through channels such as post offices, mobile phones and small retail outlets, like airtime sellers, groceries, bakeries, etc., with the goal of providing a broader and cheaper access to financial services than the bank branch-based model. The development of these networks of non-bank agents also offers considerable potential to fill the physical distance gap that appears to be one of the major obstacles to financial inclusion[105]. Brazil has developed such a network so that all 5 564 municipalities in the country now have a banking access point, with 25% of the municipalities served only by such mechanisms [106].

Definitions and scope

117. *General.* Customer identification and verification obligations are normally predicated on the basis that these functions are carried out by the officers or employees of the financial institution. However, depending on the jurisdiction, and having regard to the diversity of the financial sectors, there may be occasions when these functions are permitted or are in practice performed by agents[107].

118. *Notion of agent*[108]*.* Although the business models and the terminology may vary significantly from country to country, it is understood that the agent, in any kind of branchless banking model and most mobile money businesses models, works on behalf of a financial institution (INR 17.1.)[109]. The latter has the business relationship with the customer and is accountable for it. The financial institution grants authority for another party, the agent, to act on behalf of and under its control to deal with a client/potential client. For instance, in the mobile money business, the agent can be working on behalf of a mobile network operator who has the license to issue e-money. So the customers tend to view the retailer/agent as a point of access and as a representative of the operator. An agreement creating this relationship may be express or implied, and both the agent and the financial institution may be either an individual or an entity, such as a corporation or partnership.

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

---

[105] See par. 22.

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

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

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

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

120. *Who can be an agent?* Many countries permit a wide range of individuals and legal persons or other entities to be agents for financial institutions. Other countries restrict the list of legally eligible agents[110]. For example, India permits a wide variety of eligible agents, such as certain non-profits, post offices, retired teachers, and most recently, for-profit companies, including mobile network operators. Kenya requires agents to be for-profit actors and disallows non-profit entities. Brazil permits any legal entity to act as an agent, but prevents individuals from doing so. This range of approaches reflects that countries have different regulatory concerns that balance agent eligibility requirements from an AML/CFT perspective with financial inclusion objectives. In some countries the list of eligible agents may be very extensive but under-used by the financial institutions, in which case, countries may wish to explore the reasons underlying the reluctance to engage agents[111].

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

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

AML/CFT functions of the agent and related challenges

123. The fact that agents act as an extension of the principal financial institution means that the processes and documentation, for AML/CFT purposes, are those of the principal financial institution. The main role and duties and how agents have to perform those duties will be determined by the principal financial institution. In this regard, it is essential that these duties are clearly specified in the agency agreement that sets the terms by which the retailer is appointed as an agent of the principal financial institution. In practice, the contracts between the principal financial institution and their agents vary considerably across countries and markets but common clauses generally include the duty to perform specified AML/CFT checks, record-keeping and reporting obligations.

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

---

[110] See CGAP (2011).

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

complementary and inclusive, keeping in mind that the principal financial institution bears ultimate responsibility for compliance with all applicable AML/CFT requirements.

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

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

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

128. Under Mexico's AML/CFT legal framework for instance, financial institutions are required to establish systems and mechanisms that allow them to receive online all transactions made through an agent, in the same way as those carried out in banking offices. Financial institutions must monitor the operations carried out by the agent and report to the FIU all cases where there is a suspicion of money laundering or terrorism financing. In addition, financial institutions must have automated systems that allow them to monitor client transactions and detect possible unjustified deviations in the client –transactional profile to enable the institution's Communication and Control Committee

applicable to agents. They may also be adapted to branchless banking scenarios, in which caa

Specific requirements for agents of Money and Transfer Value Service providers[115] (Recommendation 14)

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

135. The FATF makes explicit reference to the notion of "agent" in the context of Recommendation 14[116]. In relation to this Recommendation, the Glossary defines an agent as "*any natural or legal person providing money or value transfer service on behalf of an MVTS provider, by contract with or under the direction of the MVTS provider.*" As stated earlier, the FATF views that the agent is an extension of the financial institution, with the information and documents held by that agent being immediately available to the institution, and the agent being subject to the control of the institution through their contract.

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

137. Countries have adopted different practices regarding licensing, registration, or listing of agents of MVTS[117]. For example, South Africa, Uganda, and Mongolia require agents to obtain a license. Mexico, Guatemala, and Malaysia require agents to register with a designated competent authority. Where countries require MVTS providers to maintain a list of agents, two approaches have been observed:

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

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

[115] As defined in the Glossary to the FATF Recommendations, the term "MVTS ... refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs."

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

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

138. Recommendation 14 does not require the principal and agent to be in the same jurisdiction. It allows for the possibility that agent in country A could be listed by its principal in country B – provided that authorities in country A and B can obtain the list and the agent follows the AML/CFT requirements applicable to the principal. However, in many countries, if an MVTS agent is operating in a different jurisdiction from where its principal is licensed or registered, the agent is likely to be considered an MVTS[118] provider itself in the jurisdiction in which it is operating, and would have to be licensed or registered itself.

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

4.5. INTERNAL CONTROLS

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

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

- The nature, scale and complexity of a financial institution's business.
- The diversity of a financial institution's operations, including geographical diversity.
- The financial institution's customer, product and activity profile.
- The distribution channels used.
- The volume and size of the transactions.

[118] As defined in the Glossary to the FATF Recommendations, the term "MVTS … refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs."

- The degree of risk associated with each area of the financial institution's operation.
- The extent to which the financial institution is dealing d

144. In this regard, the FATF Recommendations promote domestic cooperation mechanisms (Recommendation 2) and encourage public authorities to assist the private sector in adopting adequate and effective AML/CFT measures (Recommendation 34). These principles should guide countries' efforts to implement an effective AML/CFT regime while working towards greater financial inclusion[119].

145. Lastly, the FATF supports increased cooperation among the private sector, and in particular the building of partnerships between different service providers, aimed at delivering innovative financial products that promote financial inclusion. Mobile-based payment services as well as remittance-linked products that promote the replacement of cash payments by bank accounts, payment accounts orTw 0.337 avo[La)-5.005 Tcc 0.004 Tw 02-1.359 d[l)15.1(ivc)]TJ0l.6(e)u5.7(FA)]TJ(r)16]

CONCLUSION

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

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

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

ANNEXES

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

ANNEX 1: MEMBERSHIP OF THE PROJECT GROUP

FATF MEMBERS/OBSERVERS

Australia, India, Italy, Mexico, New-Zealand, South Africa, Switzerland, the United States, the World

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

1. PRESENTATION OF THE G20 PRINCIPLES FOR INNOVATIVE FINANCIAL INCLUSION[120]

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.

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.

Anti-

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

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

- In 2011, **Fiji** transferred the payment method of its social welfare benefits from a manual voucher system to an electronic payment system where monthly welfare payments are deposited directly into beneficiaries' bank accounts[122]. Under the old voucher system, recipients had to cash their monthly cash vouchers at their nearest post office and in some cases spent 30%-50% of their benefit on travelling costs to the nearest post office. As a result of the transfer in the welfare payment method, some 22,000 welfare beneficiaries

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

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

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

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

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

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

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

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

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

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

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

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

related to drug cartels. As part of this assessment, the authorities took into consideration the typologies provided by FATF for new payment methods[124].

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

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

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

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

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

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

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

Description of the product and financial facilities (including whether there is banking arrangement)	Amount/threshold limitation	Customer identification requirements
LEVEL 1 Low risk account that may allow none face to face opening process, but subject to monitoring from financial entities and	Limited to a maximum deposit amount of 750 UDIS[125] per month	Customer identification and ID verification could be exempted – Banks can decide

[124] FATF (2010).

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

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

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

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

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

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

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

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

Account Level	Level 0	Level 1
KYC/Account Opening requirements /conditions	1. Original Computerised National Identity Card (CNIC) of the customer 2. Legible image of customer's original CNIC 3. Digital photo of the customer. 4. Transfer of customer's data electronically to the FI. 5. Cop ..7(.9(f)1)5(s)-(.7(f)945 0.ET/CTTw 4r)1.164r d (1ions	

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

ANNEX 6: EXAMPLES OF RISK ASSESSMENT TOOLS

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

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

2. The SIP Framework aims to use the Mutual Evaluation Report (MER) findings to develop a National Implementation Plan (NIP), concentrating on key areas found to be less than fully compliant. This involves prioritising and sequencing the implementation of MER recommendations on the basis of identified risks/vulnerabilities and the 16 core/Key FATF Recommendations[126], and factoring in resourcing and capacity constraint issues.

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

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

Figure 3. **SIP framework**

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

Background

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

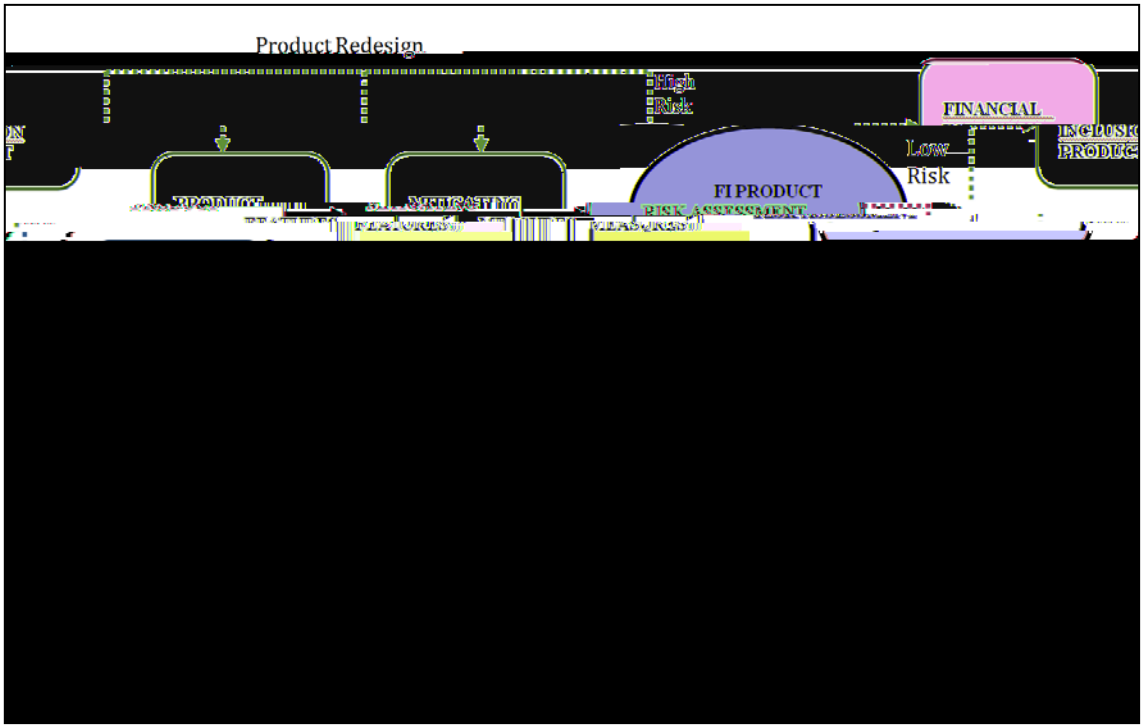
- Jurisdictions need a basis for prioritising and allocating limited resources to ensure their actions are focused effectively and efficiently.
- For the purpose of prioritisation and more efficient allocation of resources, jurisdictions may consider conducting a risk and vulnerability analysis to identify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

Methodology

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

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

Anti-



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

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

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

III. EXAMPLES OF RISK ASSESSMENT METHODOLOGIES DEVELOPED BY THE INDUSTRY

Western Union Risk Methodology

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

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

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

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

- **Services Risk** - The Company has created a Services risk model to identify the inherent ris(n)8.7( )13(o)1Bo

Source: Western Union, 2011

Risk-Based KYC developed by Globe Telecom in the Philippines

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

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

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

Full KYC[127] vs. Risk Based KYC:

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

GSMA Methodology for Assessing Money Laundering and Terrorist Financing Risk

In relation to mobile money services, the GSMA has developed a Methodology for Assessing Money Laundering and Terrorist Financing Risk[128], that offers–a systematic approach for assessing the

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

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

In late 2010, SMART Communications in the Philippines employed the GSMA Methodology to prepare a risk assessment and develop appropriate risk mitigation mechanisms in order to seek approval from the Philippines Central Bank (Bangko Sentral ng Pilipinas, or BSP) to apply reduced KYC requirements to certain customers registering for SMART Money. In early 2011, the BSP issued Circular 706 instructing institutions to "formulate a risk-based and tiered customer identification process that involved reduced CDD for potentially lower-risk clients and enhanced CDD for higher-risk accounts" and describing the requirements for reduced and enhanced CDD[129].

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

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

Source: GSMA Risk Assessment Methodology

Protecting Mobile Money against Financial Crimes, Global Policy Challenges and Solutions

[129] See Bangko Sentral Ng Philipinas (2011)

Type of risk	Observed risks

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

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

Malawi	„ - The ID card for social grant beneficiaries (different than the national official ID) is accepted for KYC exercise for the purpose of social grant payments. „ The record keeping of transactions and documents can be done in electronic format (documents scanned). „ The monitoring is done to identify unusual activity of an account. „ Banks accept.72 375c aw(u)2.7(is d)5l a.72 37 t.eify(ce)3.9lif(id)2(a)3.9(

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

USE OF INNOVATIVE TECHNOLOGICAL SOLUTIONS

Some countries are using innovative IT solutions to supplement efforts, like biometrics or voice prints. Such market-based solutions have been especially developed in Malawi (see table above) and **New Zealand** where Digicel Pacific Limited, a MNO which operates across the Pacific and is part of Digicel Group (operating in the Caribbean, Central America and the Pacific) has recently introduced in New Zealand a biometric ID system[131], In **Rwanda** and **Kenya**, storing electronic finger prints is permitted and in both countries credit unions have piloted fingerprint identification technology for rural poor customers.

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

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

opening. If there is a suspicion of money laundering or terrorist financing or other high risk

accountable institution[135] is - required under the exemption to conduct full CDD before completing any additional transactions associated with that customer‘s account.

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

- The Mzansi account was developed by the South African banking industry and launched collaboratively by the four largest commercial banks (ABSA, FNB, Nedbank and Standard Bank) together with the state-owned Postbank in October 2004. By December 2008, more than six million Mzansi accounts had been opened[136], and almost two thirds of South African adults

- 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** 0ut.9r)3.91(r)-8

p3o(1-5(b)-1920 /T1_0 06Td(7 0 /CS1 cs)0) scn/1.96TdTd[(p)0.8(r)3(of)w -4(n)2.8(O)(ifun)-911.9de)52. (3c)-5.8t ty)-p

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

In **South Africa**, a bank offering a mobile-payment service is required to obtain a name and a national ID number from the client and cross-reference these against an acceptable third-party database and then undertake additional electronic CDD measures, including cross-referencing the customers' information with third-party databases that source identity information from the Department of Home Affairs' population register and controls that prevent a customer from having more than one such an account with the bank[138]. However, since the regulator has determined that this service model introduces higher ML risk, clients who use the non-face to face registration process can– transact against their accounts in a total amount of no more than approximately US$120 (ZAR1,000) a day. The regulator thus chose to limit the functionality of the account rather than to prohibit the business model. The control measures also allow for flexibility: clients who wish to transact for larger amounts can be released from the restrictions after submitting to regular face-to-face CDD procedures[139].

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

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

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

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

- The product targets low income earners and maximum limit of withdrawals per month is K 50 000 (USD184.50)[140].

RISK FACTORS AND POSSIBLE APPROACHES TO VALIDATE CUSTOMERS' IDENTITY

In **the UK**, the Guidance issued by the Joint Money Laundering Steering Group[141] 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

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

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

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

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

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

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

Anti-

TABLE OF ACRONYMS

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

BIBLIOGRAPHY AND SOURCES

BIBLIOGRAPHY

”

” *et al*

”

”

” *et al*

” *et al*

”

Journal of Financial Crime,

”

2009 Journal of Money Laundering Control,

”

-
-
- **Development**
- *World Development Indicators database,*
- *Migration and Development Brief*
- *General guidelines for the development of Government Payment Programs*
-
- *n.d. Global Financial Inclusion (Global Findex) Database,*
-

RELEVANT FATF DOCUMENTATION:

-
-
-
-

”

”

”

OTHER USEFUL SOURCES:

” *n.d.*

”

”

”