

AML/CFT and Financial Inclusion: New Opportunities Emerge from Recent FATF Action

Increasing numbers of countries worldwide are putting in place regulatory regimes that allow more poor people to access and use basic formal financial services they need to improve their lives. The Financial Action Task Force (FATF), which sets international standards for anti-money laundering and countering the financing of terrorism (AML/CFT),¹ has taken significant action over the past two years, making it easier for policy makers to pursue financial inclusion goals while combating money laundering, terrorist financing, and other financial crimes.

Current regulatory trends reflect steadily growing awareness among FATF members over the past decade that country-level implementation of FATF's AML/CFT standards and guidance can inadvertently prevent poor households and businesses from accessing formal financial services (or discourage their use even where there is access). The financial exclusion that results can compromise countries' ability to track money laundering and terrorist financing by relegating vast numbers of people and transactions to the untraceable world of cash.² This culminated in FATF's formal recognition of financial exclusion as a money laundering and terrorist financing risk as reflected in the FATF Ministers' approval of the organization's 2012–2020 mandate.³ Financial inclusion and AML/CFT are now recognized as mutually supportive and complementary objectives: the application of measures that enable more citizens to use formal financial services will increase the reach and effectiveness of AML/CFT regimes.

This formal recognition coincides with significant FATF actions of relevance to financial inclusion taken in the past two years:

- FATF's Forty Recommendations on AML/CFT⁴—the body's highest level normative pronouncements on the subject for countries to follow in crafting their domestic AML/CFT regimes—were revised to introduce the requirement of national and sectoral risk assessments, embedding a "risk-based approach" (RBA) to AML/CFT regulation and supervision, and expanding on the concepts of "lower risk" and "low risk" activities.
- FATF released updated guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion⁵ produced jointly with the World Bank and the Asia/Pacific Group on Money-Laundering, and new guidance was issued on Prepaid Cards, Mobile Payments and Internet Based Payment Services.⁶
- FATF revised the Assessment Methodology⁷ used to assess a country's compliance with the FATF Recommendations (which are vitally important in determining which countries get added to or removed from public lists FATF maintains of noncompliant jurisdictions), incorporating for the first time assessment of the effectiveness of a given country's AML/CFT regime, and explicitly including financial exclusion and financial inclusion policies as factors that assessors may consider in their evaluations.

Collectively, these actions clarify the landscape for country-level policy making, offering new

1 FATF's standards and work focus on preventing the abuse of financial services by criminal and terrorist financiers. This includes a wide range of topics beyond that directly relevant to financial inclusion. For example, FATF recently added international standards to combat financing related to proliferation of weapons of mass destruction. It has also traditionally provided guidance and published typology reports on topics such as anti-corruption, financial investigations, environmental crime, and stolen asset forfeiture and recovery (to prevent or investigate money laundering or terrorist financing emerging from such underlying crimes).

2 See, e.g., speech by FATF President Paul Vlaanderen (2010).

3 <http://www.oecd.org/unitedkingdom/financialinclusionandfinancialintegritycomplementarypolicyobjectives.htm>

4 In this Focus Note, "FATF Recommendations" refers to the document "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation."

5 In this Focus Note, "FATF Financial Inclusion Guidance" refers to the document "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion."

6 In this Focus Note, "FATF NPPS Guidance" refers to the document "Guidance for a Risk Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services." Prepaid cards, mobile payments, and internet-based payment services are recognized as key levers to advance financial inclusion.

7 In this Focus Note, "Assessment Methodology" refers to the document "Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems."

opportunities—in some cases, even *incentives*—for policy makers to adopt inclusion-friendly AML/CFT regimes. This Focus Note provides an overview of the relevant FATF standards and guidance, highlighting the topics that are most relevant for financial inclusion policymaking, including the specific standards and guidance that have changed, and suggesting implications for financial inclusion policymaking.⁸

The discussion is in three parts:

Part I provides background on FATF and the revised FATF Recommendations and new guidance, and outlines the areas of greatest relevance to financial inclusion affected by the recent FATF action summarized above. These include financial service providers' customer due diligence (CDD) practices,⁹ record-keeping and monitoring, remittances and other money transfer service obligations, and special issues relating to agents playing roles in AML/CFT compliance.

Part II discusses changes in AML/CFT compliance assessment introduced in the new Assessment Methodology and considers potential financial inclusion implications. Among these, the new focus on the *effectiveness* of a country's AML/CFT regime is the most fundamental, given that assessors may now consider inadvertent financial exclusion as a contextual factor bearing on effectiveness as well as steps taken to increase financial inclusion.

Part III reflects on the road ahead, including both new opportunities for countries to be proactive

in developing financial inclusion-friendly AML/CFT regimes as well as some foreseeable challenges countries will face that merit further attention, whether from country-level policy makers, from FATF and its affiliates, or from the international community at large.

Part I. The Revised FATF Requirements and Their Significance for Inclusion

The FATF Framework

FATF operates as a task-force-style collaboration among 34 member countries and two regional associations.¹⁰ It collaborates closely with eight FATF-Style Regional Bodies (FSRBs). These autonomous bodies have a collective membership of an additional 177 countries.¹¹ All have committed to implementation of the FATF Recommendations, which set standards for national AML/CFT regulation and supervision, covering a broad range of financial service providers, as well as certain nonfinancial businesses and professions at risk of exploitation for financial crime. The FATF definition of "financial institution" is activity-focused rather than institutional and covers the full range of products and providers of relevance to financial inclusion. (Despite this all-encompassing definition, many countries still have AML/CFT regimes that are institution-focused, rather than activity-focused, which can be both less effective due to coverage gaps and also less financial-inclusion friendly.)¹² The FATF Recommendations also call for countries to adopt a range of criminal law enforcement measures, to establish Financial Intelligence

⁸ This Focus Note represents CGAP's interpretation of these recent FATF actions. Policy makers are advised to refer directly to the relevant FATF documents for the complete and official articulation of issues discussed. Some of the examples and illustrations have not yet been discussed in the context of a mutual evaluation.

⁹ CDD policies are often colloquially referred to as "know your customer" (KYC) policies. However, in other contexts KYC carries somewhat different connotations. Accordingly, in this Focus Note the FATF term CDD is used throughout.

¹⁰ The collaboration works within a periodically renewed and updated mandate approved by the finance ministers of FATF member countries. The current 2012–2020 FATF mandate covers financial crime and integrity-related topics beyond the scope of this Focus Note, such as preventing proliferation of weapons of mass destruction.

¹¹ In total, 19 international bodies have observer status at FATF (not including FSRBs, which are referred to as FATF Associate Members), including but not limited to the International Monetary Fund (IMF), the World Bank, the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors, and the Organization for Economic Cooperation and Development.

¹² AML/CFT regimes that are institutionally focused may result in an unlevel playing field, as well as gaps in coverage. For example, an electronic wallet for which a nonbank institution serves as the legal issuer of stored value may not be explicitly covered by a given institutionally focused law on AML/CFT, even though an equivalent product offered by a bank would be. While such a coverage gap could result in new entrants offering products that avoid the expense of AML/CFT compliance faced by banks, uncertainty as to their AML/CFT compliance obligations could also discourage nonbank providers that may be better positioned to serve financially excluded and underserved populations.

Units (FIUs) to receive, analyze, and disseminate suspicious transaction reports and to ensure that appropriate regulatory and supervisory bodies oversee implementation of AML/CFT regulation and supervision.

FATF, FSRBs, the World Bank, and the International Monetary Fund (IMF) use a mutual evaluation mechanism to assess the extent to which countries have implemented the FATF Recommendations (as discussed in Part II). These bodies work cooperatively with countries to undertake country assessments using the same newly revised Assessment Methodology.¹³

RBA, Low Risk, and Lower Risk

Strengthening and clarifying the application of the RBA to AML/CFT regulation and supervision constituted a central objective of the revisions to the FATF Recommendations approved in 2012. The RBA is now a mandatory element of a compliant AML/CFT regime, and the primacy of the RBA is underscored by making identifying, assessing, and understanding risks and applying the RBA the first of the revised FATF Recommendations.¹⁴

The RBA is fundamental because it recognizes the wide variability among countries' potential exposure to money laundering and terrorist financing, and calls on country-level policy makers to identify, assess, and understand their own specific risks (see Box 1). The RBA is particularly critical to crafting a financial-inclusion-friendly AML/CFT regime, as it affords the flexibility to tailor risk mitigation policies to the specific nature, levels, and types of relevant risk of concern in a given market. Financial institutions covered by the AML/CFT regime are required to apply the RBA.

The centrality of the RBA in the revised FATF Recommendations puts a premium on the quality

Box 1. Country Risk of Money Laundering and Terrorist Financing Can Vary Significantly

Money laundering and terrorist financing risks vary greatly, from region to region, from country to country, and even subnationally. Pakistan, for example, which neighbors India, Afghanistan, and Iran, suffered from a number of terrorist attacks in recent years and might have comparatively higher terrorist financing risk relative to some of its more remote South Asian neighbors such as the Maldives and Bhutan. Haiti, a theater in a protracted drug war given its central location between drug producers to the West and South and drug consumers to the North, will face different money laundering risks relative to countries that lie below the equator and may assess terrorist financing risks comparatively lower. Country-level money laundering and terrorist financing risks are also not static, changing often dramatically over time in accordance with evolving social, political, and market conditions, subnationally, nationally, regionally, and globally.

of the assessment of risk conducted with respect to a given country context. Moreover, the FATF Recommendations call for an assessment of risk to be undertaken both at the country level and at the level of financial service providers operating in that country. FIUs, supervisors, and other relevant country-level policy makers must therefore be knowledgeable, not only about general country-level money laundering and terrorist financing risks, but also about money laundering and terrorist financing risks that vary according to the nature and type of the financial service provider, financial service, and customer segment involved.

The revised FATF Recommendations differentiate between "low risk" and "lower risk" scenarios. In strictly limited circumstances where there is "a proven low risk of money laundering and terrorist financing,"¹⁵ countries are permitted to decide not

¹³ For further explanation of the assessment process, see FATF (2013e, p. 16).

¹⁴ Prior to the 2012 revisions, the FATF Recommendations permitted (but did not explicitly require) countries to implement a risk-based approach in relation to some aspects of the AML/CFT regime. This left open the possibility of misinterpretation and inconsistent interpretation in the application of the concept—including among assessors participating in mutual evaluations—undoubtedly contributing to an overly conservative approach, at least in some countries' AML/CFT regimes.

¹⁵ See FATF Recommendations, Interpretive Note to Recommendation 1, p. 31.

to apply certain Recommendations to a particular type of provider or activity. FATF has not elaborated on how a country should “prove” low money laundering or terrorist financing risk, leaving this for countries to determine. The concept of lower-risk scenarios (while also not sufficiently elaborated on, but does not require countries to “prove” anything), may therefore have greater practical significance for creating AML/CFT regimes that support financial inclusion efforts, at least in the short term (see Part III). Where countries identify lower risks, they may decide to allow “simplified measures” for some of the FATF Recommendations under certain conditions.¹⁶ The concept of simplified measures arises importantly with several of the AML/CFT topics of greatest relevance to financial inclusion, particularly CDD (as discussed in “AML/CFT Topics Relevant to Financial Inclusion”).

Accounts and Business Relationships, Occasional Transactions, and Special Rules for Wire Transfers and Money and Value Transfer Services

The activity-focused nature of the FATF definition of “financial institution”¹⁷ calls for a highly flexible conceptual typology of activities and transactions financial service providers might carry out to accommodate widely varying financial systems and approaches to delivering financial services, as well as potentially fast-evolving changes in any given environment. The concepts of “accounts,” “business relationships,” and “occasional transactions” all have special relevance for financial inclusion—particularly innovative business models for reaching financially excluded customers—as do the special rules for “wire transfers” and “money and value transfer services.”

Accounts, business relationships, and occasional transactions. The term “account” is not defined in the FATF Recommendations although the General Glossary indicates that “references to ‘accounts’

should be read as including other similar business relationships between financial institutions and their customers.”¹⁸ This would imply that the term encompasses some of the types of innovative delivery most relevant to financial inclusion—for example, a mobile wallet-type stored-value account with a mobile network operator or its affiliate.

Similarly, the term “business relationship,” which appears extensively throughout the revised FATF Recommendations, is not defined and is used to refer to a broad range of commercial arrangements between parties. Any narrower definition could risk omitting relevant types of arrangements. In a practical sense, the concept is perhaps best understood in counter distinction to “occasional transactions.” While “occasional transactions” are also not specifically defined in the FATF Recommendations, it is clear from the contexts in which the concept appears that these are generally one-off transactions that occur outside an ongoing arrangement between customer and provider (see Box 2). A “business relationship” could, for example, be a stored-value account in the customer’s name or loan to a customer.

Special rules for wire transfers and money and value transfer services. Accessible and affordable means of moving value from one party to another—including electronically and potentially across borders—lie at the heart of innovative financial inclusion. They are also key to the massive potential gains in countries’ capacity to identify and stop money laundering and terrorist financing that accompany significant progress in bringing financially excluded households into the formal financial system. Unfortunately, they are also uniquely useful in money laundering, terrorist financing, and other types of financial crime because of the speed and frequency with which value can be moved, potentially over great

¹⁶ See FATF Recommendations, Recommendation 1, p. 11.

¹⁷ See FATF NPPS Guidance, p. 11. The FATF Recommendations also apply to “designated non-financial businesses and professions” (DNFBPs), such as legal professionals, accountants, dealers in precious metals and stones, casinos, and real estate agents, who are subject to AML/CFT regulation and supervision because they may be involved in handling large amounts of cash or otherwise are in a position to disguise illicit proceeds (General Glossary, FATF Recommendations, p. 113). DNFBPs are generally not discussed in this Focus Note.

¹⁸ FATF Recommendations, General Glossary, p. 110.

Box 2. A Challenge for AML/CFT Policy Makers: What Constitutes an “Account Based” vs. an “Occasional” Transaction?

Innovation—often spurred by financial inclusion objectives—is stimulating the introduction of new retail products and services in countries across the globe that don’t divide neatly between “account based” and “occasional” transactions.^a

Over-the-counter transactions

Over-the-counter (OTC) customers might generally be assumed to include those who do not have an electronic wallet registered to their name and who visit agents from time to time to have the agents conduct remittance or bill paying transactions on their behalf. Such customers might be assumed to be conducting “occasional transactions” rather than having an established “business relationship,” as the latter connotes some type of contractual or legal arrangement in the customer’s name through which the transactions are processed. But what if the same customer visits the same agent frequently to conduct such transactions? Policy makers in at least one country are debating whether these customers should be viewed as having an established “business relationship” with the agent in question even in the absence of any formal account if they conduct OTC transactions as frequently as every month.^b

Transactions using prepaid cards

A similar question arises with prepaid cards. Over the years, such instruments have reflected a wide range of business models and associated functionality, presenting unique challenges to AML/CFT regulation and supervision.^c For example, a nonreloadable prepaid

card such as a retail store gift card might generally be assumed to qualify as an “occasional transaction” given that it was purchased only once. Although multiple transactions can occur, it is discarded once the monetary value stored on it is spent. The user has no “account based”/business relationship with the issuer of the card because no further transactions can be made with the card once the card’s original value is spent. (See FATF Recommendations, General Glossary, p.110.) However, if this same card can be reloaded with funds and used on a recurring basis, the question arises whether the relationship between the card’s holder and its issuer should be deemed an “account based” relationship.

What are countries supposed to do?

As FATF does not define “account,” “business relationship,” or “occasional transactions,” the responsibility falls to countries to provide reasonable meanings for these terms, taking into consideration the innovations emerging in their markets and creating distinctions in their AML/CFT regimes based on local circumstances.

a. See, e.g., CPSS (2012, p. 34).

b. This debate exemplifies the practical challenges of applying the FATF Recommendations in practice, particularly for policy makers thinking ahead to future mutual evaluations of their AML/CFT regime. If the decision is reached not to treat such OTC transactions as occasional transactions, what might be inferred by assessors regarding this decision? It is understandable that the policy makers in question have requested not to be identified in this Focus Note pending a final decision.

c. See FATF NPPS Guidance, p. 5.

distances and in potentially significant aggregate volume (even if individual transactions are small).

For this reason, there are FATF Recommendations dedicated specifically to “money or value transfer services”¹⁹ and “wire transfers,”²⁰ containing a number of special rules of particular relevance to financial inclusion (as discussed in “AML/CFT Topics Relevant to Financial Inclusion”). The rules distinguish between cross-border wire transfers

(where at least two countries’ AML/CFT regimes come into play) and domestic wire transfers (where only a single country’s rules are implicated).²¹ They apply to the entire spectrum of organizations facilitating the transfers, from well-known money transfer operators such as Western Union to remittance corridor-specific “mom and pop” providers of “money or value transfer services”—of particular importance to financial inclusion in many contexts.²²

19 FATF Recommendations, Recommendation 14, p. 17.

20 FATF Recommendations, Recommendation 16, p. 17. The term “remittance” is not used in the FATF Recommendations. “Wire transfers” should be understood as a subset of domestic and cross-border transfers (i.e., those that are accomplished electronically).

21 A super-national entity may petition FATF to be designated as a single jurisdiction for the purposes of (and limited to) an assessment of Recommendation 16 compliance, as, e.g., the European Union/European Economic Area has done (FATF Recommendations, General Glossary, p. 75). As a result, a transfer between Greece and Germany will be treated as a domestic transfer.

22 According to the Glossary for Recommendation 16, “[m]oney or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs.”

AML/CFT Topics Relevant to Financial Inclusion

While most of the subjects covered in the FATF Recommendations and new guidance have a bearing on financial inclusion, four topics are most relevant—particularly to the types of innovation with the greatest potential to be used by massive numbers of households that are currently financially excluded or underserved. These are CDD practices, record-keeping and monitoring, remittances and other money transfer services, and issues relating to agents playing roles in AML/CFT compliance.²³

Customer Due Diligence

CDD and financial inclusion. The revised FATF Recommendations provide greater clarity on the application of the RBA to the implementation of a financial service provider’s CDD policies—that is, steps taken to identify and verify the identity of customers and of the “beneficial owners,”²⁴ to understand the purpose and nature of their financial transactions and to conduct appropriate ongoing monitoring of customers to ensure that the transactions are consistent with the customer’s profile. Historically, countries have often included in their AML/CFT regimes inflexible identification and verification requirements that many poor households cannot meet. For example, customers are required to provide specific types of identification that poor people often do not have, or providers are required to verify a customer’s fixed address, which is impossible for billions of people around the world living in informal housing (Isern and de Koker 2009). The revised Recommendation on CDD,²⁵ when read together

with the Recommendation on the RBA, calls for policy makers to fashion CDD requirements that do not inadvertently exclude the “unidentifiable” poor, and they provide the flexibility necessary to do so (Basel Committee 2014, p. 7).²⁶

Technical components of CDD. While countries are encouraged to take advantage of this flexibility, rules on CDD have to include some essential components. First, providers must be required to undertake certain CDD measures (i) when establishing a business relationship with a customer; (ii) when carrying out occasional transactions above USD/EUR 15,000 (or in the case of certain wire transfers, as discussed in “Remittances and Other Money Transfer Services”); (iii) if there is a suspicion of money laundering or terrorist financing (as discussed in “Record-Keeping and Monitoring”); or (iv) if the provider has doubts about the veracity or adequacy of previously obtained customer identification data.

CDD measures include four elements:

1. Customers have to be “identified” and their identity “verified” using reliable, independent source documents, data, or information.
2. “Reasonable steps” must be taken to identify the “beneficial owner”²⁷ involved. (In the case of individuals—particularly poor customers transacting in small amounts—providers might reasonably assume that the customer is transacting on his or her own behalf, but in the case of legal entities, establishing beneficial ownership generally will call for additional examination and verification.)

²³ FATF Financial Inclusion Guidance, p. 6.

²⁴ The General Glossary to the FATF Recommendations defines “beneficial owner” as a “natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted.”

²⁵ FATF Recommendations, Recommendation 10, p. 14.

²⁶ The Basel Committee on Banking Supervision has recently issued this AML/CFT guidance for banks, which is called on to include risks relating to money laundering and financing of terrorism within their overall risk management framework. Interpreting FATF Recommendation 10 and Basel Core Principle 29, the guidance provides that banks generally should not establish a business relationship, or even carry out transactions, until the identity of the customer has been satisfactorily established and verified. While the Basel Committee guidance acknowledges the flexibility now incorporated in the FATF Recommendations, it does not tackle the questions of banks’ approach to CDD in lower-risk or low-risk scenarios.

²⁷ The General Glossary to the FATF Recommendations defines “beneficial owner” as a “natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted.”

3. When CDD measures are being carried out to establish an ongoing business relationship between a provider and a customer such as the opening of an account or the extending of a loan (rather than in the context of an occasional transaction) the provider must understand and obtain information, as appropriate, on the purpose and intended nature of the business relationship.
4. For business relationships, the provider must be required to conduct ongoing due diligence on the business relationship and to scrutinize transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with the provider's knowledge of the customer, including his or her business and risk profile.

Simplified CDD for lower-risk scenarios. Perhaps the most important clarification regarding CDD is that countries should design CDD requirements applying the RBA. This includes explicit authorization to apply simplified CDD measures in lower-risk scenarios (as identified in the risk assessment of the country in question). In the financial inclusion context, this could allow, for example, for the concept of "tiered accounts"²⁸ in a country's AML/CFT regime—where limited functionality for the bottom tiers lowers the associated money laundering and terrorist financing risk, and consequently justifies simpler approaches to CDD (see Boxes 3 and 4).

CDD and nonface-to-face transactions. For AML/CFT purposes, the specific types of business relationships and transactions involved, the targeted client groups,

the involvement of intermediaries (such as agents, as discussed in "Agents and AML/CFT"), and the sophistication of the technology used are examples of factors that should be considered by providers and country regulators to evaluate the appropriate level of CDD applied.²⁹ Nonface-to-face business relationships or transactions are identified in the FATF Recommendations as presenting potentially *higher* risk situations (triggering enhanced, rather than simplified, CDD).³⁰ These requirements collectively call for creativity in applying the RBA to reach financially excluded populations, particularly those in remote, sparsely populated areas where conventional, face-to-face approaches to CDD are prohibitively costly yet where there is lower risk of money laundering and terrorist financing. The answer could be as simple as the use of camera phones or voice recognition software, leveraging the same low-cost technologies that enable financial service delivery also to accomplish low-cost CDD.

Record-Keeping and Monitoring

AML/CFT record-keeping requirements are challenging for all financial service providers, but have historically presented particular disincentives to move down market. The reason is simple: the costs and practical challenges of record-keeping don't generally decrease in proportion to the transaction size, and indeed they may increase (e.g., in the case of serving remote customers). Many countries' existing AML/CFT regimes only contribute to the problem, such as by requiring the collection and retention of photocopies of all customer records collected as part of CDD, regardless of the nature of the provider, the

²⁸ The phrase "tiered accounts" in the AML/CFT context refers to a progression of types of accounts, ranging from a basic, low-value product with limited functionality to a conventional transaction account with greater functionality and higher value limits. See Chatain, et al. (2011, p. 111). Account "tiers" directly link the level of CDD to the extent and range of financial services offered to a customer. For example, a level 1 tier could mean that customers are provided with limited and basic services after undergoing a simplified verification. A level 2 tier could mean the customer accesses an expanded range of financial services with higher transactions ceilings provided that further customer verification has taken place.

²⁹ In addition, a separate, particularized risk assessment of the relevant delivery channels is required in the case of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products (FATF Recommendations, Recommendation 15, p. 17).

³⁰ FATF Recommendations, Interpretive Note to Recommendation 10, p. 63. For example, the risk of nonface-to-face transactions, such as impersonation fraud, will increase in the absence of adequate risk-mitigating controls. See FATF NPPS Guidance, p. 14. However, as noted in FATF Recommendations and underscored in FATF Financial Inclusion Guidance, these examples are given as general guidance only, and the risks may not be higher in all situations (FATF Recommendations, Interpretive Note to Recommendation 10, para 14, p. 63; Financial Inclusion Guidance, p. 34).

Box 3. In the Financial Inclusion Context, What Might “Simplified CDD Measures” Involve?^a

1. *Allowing flexibility to define what constitutes “reliable, independent, source documents, data or information” for verifying and monitoring customer’s identities.*

Because the FATF Recommendations provide flexibility on the types of information collected for the purpose of CDD, countries may be pragmatic and creative regarding the type of credible identity verification documents permitted. For example, a customer unable to provide government-issued identification documents might be allowed to use a credible letter from a village chief or references from existing customers.^b Countries without comprehensive national or subnational identification systems might allow a range of alternative source documents, with a view to positioning all population groups to provide some form of identity verification.

2. *Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship and until the account reaches the next tier level.*

When a product presents a lower risk of money laundering or terrorist financing (e.g., a simplified account with low maximum transaction and balance limits), the verification of customers’ identity could be postponed, rather than conducting verification before allowing the customer to transact.^c This allows, for example, for a customer to open a deposit account pending identity verification.^d More importantly from a financial inclusion perspective, it allows for a tiered approach whereby customers may open a very basic account such as a mobile wallet subject to low transaction limits with minimal upfront identity verification, but the provider must undertake more extensive verification before the customer migrates

to the next tier of account with higher transaction limits and greater functionality. If the customer never migrates to the next tier of account, verification may not be necessary.

3. *Reducing the frequency of customer identification updates borne by the provider.*

For lower-risk scenarios involving an ongoing business relationship such as a mobile wallet subject to low transaction limits, customer information does not need to be updated as frequently as for other categories of products. Frequency of updates should be determined by taking into account the functionality of and controls that apply to the financial product in the context of local circumstances as documented in a country’s assessment of risk.

4. *Reducing the degree of ongoing monitoring and scrutinizing of transactions.*

Relatedly, for such lower-risk scenarios as the mobile wallet subject to low transaction limits, it is also permissible to reduce the degree of ongoing monitoring and scrutinizing of transactions (as discussed in “Record Keeping and Monitoring”).^e

5. *Not collecting additional information or carrying out specific measures to understand the purpose and intended nature of the business relationship.*

While collecting information to understand the purpose and intended nature of the business relationship is an important component of CDD, the FATF Recommendations allow this information to be inferred in lower-risk cases. For example, if the product is a basic savings account, it may be inferred that the customer opens the account to save money.

a. Italicized text in the five subheadings is paraphrased from the FATF Recommendations, Interpretive Note to Recommendation 10, p. 66, and FATF Financial Inclusion Guidance.

b. In some cases, such an approach may be the only one practicable. However, regulators should always be mindful of potential unintended ancillary consequences. For example, where regulations were amended to allow those who do not have formal proof of their personal particulars to present letters of affirmation drafted by their employers, it was found to increase the power and hold of employers over vulnerable employees, and in some cases where village chiefs were allowed to draft such letters, the chiefs started to demand money for these “verification services.” See de Koker (2011).

c. The postponement of verification is permitted in other contexts as well, not just in situations of low risk.

d. Although this provision facilitates the opening of deposit accounts by lower-income clients, it also raises questions at a practical level in case clients are not able to reach the verification threshold. For example, do their monies remain frozen while they try to reach the verification threshold? Will the bank return the funds when it lacks assurance, including assurance that the person in front of them is the person who opened the account? These are just a few illustrative questions that will need to be addressed through the development of appropriate business practices and regulation at the country level.

e. In determining an appropriate approach to CDD, the degree of ongoing monitoring required should also be considered together with the approach taken to upfront identification and verification: relaxed requirements at the identification and verification stages could hamper certain aspects of monitoring the business relationship over time.

Box 4. Are Anonymous Accounts Allowed?

The FATF Recommendations clearly prohibit “anonymous accounts,” as customers must be identified and their identity verified in establishing the business relationship.^a Yet the concept of anonymity is not defined. Poor customers transacting in their community using only cash are clearly transacting anonymously for AML/CFT purposes in the sense that the transactions cannot be tracked through the formal financial system. When these customers accomplish the same transactions using a mobile wallet with strict limits on the amounts and frequency involved and number of other parties with whom they can transact, the money laundering and terrorist financing risk may remain low while minutely specific “financial identities” emerge, associated with the SIM cards used. Moreover, these SIM-based identities, coupled with the feasibility of mapping transaction flows down to the level of specific cell phone towers and agent locations, offer both providers and law enforcement new means of discerning suspicious transactions and finding perpetrators of financial crime. The phenomena also trigger strong reactions from some privacy advocates across the country income level spectrum. An alternative policy approach permitted under the revised FATF Recommendations and new guidance would involve targeted exemptions from CDD requirements for such specially designed and limited basic accounts, based on a finding of proven low risk.^b

a FATF Recommendations, Recommendation 10, p. 14.

b As observed above, and as noted in “Foreseeable Challenges Meriting Further Attention,” FATF has not yet offered insights into how a country or provider “proves” low risk.

customer, or the transaction. Similarly, monitoring transactions can be prohibitively expensive for providers trying to serve excluded customers unless they are risk-adjusted (something not provided for in many existing AML/CFT regimes).

Technical components of record-keeping, monitoring, and suspicious transaction reporting. Such country-level rigidity in record-keeping and monitoring requirements run counter to the spirit—and the

technical components—of the record-keeping and monitoring requirements under the revised FATF Recommendations and new guidance. With respect to record-keeping, these are straightforward: providers must maintain records on transactions for at least five years; CDD records (e.g., identification documents such as passports) must be held for at least five years after the business relationship is ended, or after the date of an occasional transaction.³¹ With respect to monitoring and suspicious transaction reporting, providers of all types are called on continually to monitor money laundering and terrorist financing risks emerging from their business, including outsourced relationships, such as agent networks, and to report suspicious and unusual transactions to their country’s FIU.³²

Clarifications on record-keeping. For purposes of fashioning a financial-inclusion-friendly AML/CFT regime, the important clarification about record-keeping to be gleaned from the revised FATF Recommendations and new guidance lies in the flexibility now explicitly permitted regarding the *manner* in which records are gathered and kept. For example, the provider may scan documents and store electronic copies or hold physical photocopies, or staff may simply record details manually.³³ This explicitly permitted flexibility positions regulators to accommodate record-keeping that is practical and inexpensive for the smallest microfinance institution or the most vast and diverse network of mobile wallet cash-in/cash-out agents.

Clarifications on monitoring transactions. Given the adverse commercial and regulatory consequences that may emerge from illicit financial transactions flowing through their systems, mainstream financial service providers have an incentive to invest heavily in automated transaction monitoring and pattern detection systems and related human resources. Under the revised FATF Recommendations and

31 FATF Recommendations, Recommendation 11, p. 15.

32 FATF Recommendations, Recommendation 20, p. 19.

33 Financial Inclusion Guidance Paper, para. 111, p. 39.

new guidance, the level and form for ongoing monitoring of customers and transactions should be risk-based. The degree of monitoring should therefore be determined with reference to the risks associated with customer segments and the products or services these customers use. This means that cost-effective monitoring could be done manually in the case of a small microfinance institution where personal knowledge of staff position them to identify suspicious transactions, but via sophisticated electronic transaction monitoring and pattern-detection systems in the case of a mobile network operator offering mobile wallets through a vast network of agents.³⁴

Remittances and Other Money Transfer Services

Remittances, other money transfer services, and financial inclusion. Remittances—money sent from earners in one location to a distant household or community—have been recognized as a lifeline for poor families (Dilip 2005). Cross-border remittances are critical components of the economy in many lower-income countries; therefore it is a worrying trend that the accounts of many remitters are currently under threat of closure (see Box 5).³⁵ More broadly, the capacity to move money or value electronically—inexpensively and conveniently—from one place to another (referred to as “money or value transfer services” [MVTs] in the FATF Recommendations) is critical to the goal of financial inclusion, given the potential to build on other

financial services that poor customers want and need (CGAP 2013).³⁶

Technical components of remittances and other money and value transfer services. As observed, the FATF Recommendations distinguish between domestic remittances (where only a single country’s AML/CFT regime comes into play) and cross-border remittances (where at least two countries’ AML/CFT regimes—the sending country and the receiving country—need to be considered).³⁷ Also, because of the speed and frequency with which value can be moved electronically, potentially over great distances and in potentially significant aggregate volume (even if individual transactions are small), a separate Recommendation is dedicated to the subject of “wire transfers”³⁸ (both domestic and cross-border), which under FATF’s definition is any electronic transfer.³⁹ The wire transfer rules apply to any kind of money or value transfer service, from huge bulk fund transfers via SWIFT to person-to-person (P2P) transactions through the smallest money transfer operators;⁴⁰ however, the rules vary between account-based transfers and occasional transactions (to the extent CDD requirements with respect to the party sending or receiving the transfer have already been met).⁴¹

Under the FATF Recommendations and new guidance, for both account-based transfers

34 Even sophisticated transaction monitoring and pattern detection systems will not obviate the need to involve employees or agents, because they can observe facts about customers that are not captured as data in the systems.

35 The World Bank estimates that in some areas of Somalia, remittances accounted for more than 70 percent of GDP in 2006. See, also, Dilip (2012). In countries such as Tajikistan, it is estimated at 47 percent of GDP (April 2013). See <http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationDevelopmentBrief20.pdf>

36 See, also, Todoroki, Noor, Celik, and Kulathunga (2014).

37 More than two countries’ AML/CFT regimes could be involved in the case of rules governing obligations of intermediaries; e.g., a remittance transfer between Canada and Jamaica may involve a U.S. bank as an intermediary, thus triggering the AML/CFT regimes of all three countries. The distinction between domestic and cross-border remittances is drawn in FATF Recommendation 16 (Wire Transfers).

38 The FATF Glossary of Specific Terms used in the Interpretive Note to Recommendation 16 defines a wire transfer as “any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person” (p. 76).

39 FATF Recommendations, Recommendation 16, p. 17.

40 Recommendation 16 aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available to relevant authorities and financial institutions. The Recommendation does not cover debit, credit, or prepaid cards if they are used for the purchase of goods or services and an accompanying identification number is able to track the full payment transaction. However, it does apply when these payment instruments are used to conduct person-to-person remittances.

41 FATF Financial Inclusion Guidance, p. 25.

Box 5. The Challenge of Cross-Border Remittances to Conflict Hotspots: The Case of Somalia

In post-conflict and fragile states such as Somalia, money transfer businesses operating from diaspora communities abroad are essential to the very survival of large segments of the population. Moreover, given the country's underdeveloped financial infrastructure, AML/CFT-related obligations at the receiving end are inherently challenging to discharge. Recently a number of U.K. banks, including most notably HSBC and Barclays, have moved to terminate hosting relationships with hundreds of such money transfer businesses operating in Somalia and other countries purportedly due to concerns regarding questionable AML/CFT compliance policies.^a The actions by the U.K. banks are increasingly mirrored by those of banks in other remittance-sending countries such as the United States.^b Indeed, this is not a new phenomenon; large banks in the United States and Canada took similar actions over the past decade, although the recent U.K. and U.S. actions have attracted additional media outcry given the severe humanitarian implications in Somalia.^c

The U.K. government is attempting to better understand and address the situation by establishing a national-level "Action Group on Cross Border Remittances." Comprising of relevant domestic agencies in the United Kingdom, including the National Crime Agency, Her Majesty's Revenue and Customs (the national tax authority in the United Kingdom), and the U.K. Department for International Development (DFID), the Action Group has a 12-month mandate and will focus on identifying policy recommendations that would ensure continuation of vital formal remittance flows to fragile states such as Somalia while providing

sufficient comfort to providers and regulators that integrity risks are adequately mitigated. It will develop its guidance through the following:

1. *Identifying associated financial crime risks (led by the National Crime Agency)*. This includes providing more detailed and specific risk assessments and alerts about the sector to banks and money transfer businesses, to help differentiate the risks involved in dealing with different money transmitters.
2. *Improving supervisory guidelines (led by Her Majesty's Revenue and Customs)*. This will entail increasing "days of action" with law enforcement as well as the number of risk-targeted supervisory visits Her Majesty's Revenue and Customs undertakes to provide further confidence that noncompliant money transmitters are being required to improve or are removed from business. Her Majesty's Revenue and Customs will also provide further training to money transmitters to help them achieve an effective level of compliance.
3. *Creating and testing the possibility of a "safer corridor" pilot between the United Kingdom and Somalia (led by DFID)*. The pilot will create and test alternative mechanisms in which certain money transfer operators could continue operating in Somalia in an environment that provides sufficient comfort to bank partners and regulators. It is expected that this work will lead to certain regulatory, operational, and commercial models that could be replicated globally, with application to remittance corridors facing comparable market environments and dynamics.^d

a. In May 2013 in the United Kingdom, e.g., Barclays Bank, which at the time was estimated to hold more than 200 money transfer accounts of businesses in the United Kingdom, gave 60 days' notice of its intention to close money transfer business accounts that did not meet its new eligibility criteria. See <http://www.bankingtech.com/154562/barclays-under-fire-for-outrageous-remittance-closures/>. Barclays and some other banks have expressed their rationale in public press releases. See, e.g., <https://www.newsroom.barclays.com/Press-releases/Barclays-statement-on-Money-Service-Businesses-aa8.aspx>. While the U.K. government is looking at alternatives, the concern is real for the dramatic impact this would have on the lives of millions. <http://www.theguardian.com/global-development/2013/jun/24/somalis-barclays-remittance> and <http://www.theguardian.com/global-development/2013/oct/16/barclays-somalia-remittances-court-ruling>, <https://theconversation.com/banks-move-on-money-remitters-but-will-it-really-combat-crime-16969>

b. Large banks such as JPMorgan Chase (Rapid Cash product), Bank of America (SafeSend product), and Citigroup's BANAMEX USA unit (prompted by a federal criminal investigation related to money laundering) have eliminated low-cost money transfer options catering to some low-income immigrant populations, in particular Mexican immigrants sending remittances to their families back home. Regulators acknowledge that banks must now invest significantly more to monitor the money moving through their systems or risk substantial penalties (Corkery 2014).

c. Somali money transfer businesses in the United States are facing similar challenges. See, e.g., National Public Radio (2014).

d. Written Ministerial Statement, Money Service Businesses, HM Treasury (10 October 2013). See <http://www.parliament.uk/documents/commons-vote-office/October%202013/10%20October/2.CHANCELLOR-money-service-businesses.pdf>

and occasional transactions,⁴² countries may significantly reduce information requirements for cross-border wire transfers below USD/EUR 1000.⁴³ For these transactions, the minimum information required is (a) name of the originator of the wire transfer (the remittance sender), (b) name of the beneficiary (the remittance recipient), and (c) account number of both the sender and recipient (if the transfer is account to account) or, alternatively, a unique transaction reference number for the transaction. Importantly, this customer information does not need to be verified, unless the transaction is viewed as suspicious or unusual by the provider.

For domestic wire transfers (including domestic remittances) below USD/EUR 1000, and applicable to account-based and occasional transactions, the requirements are even fewer: only the name of the remittance sender is required, and this does not need to be asked for upfront if it can be made available to the recipient financial institution and relevant authorities through other means, such as an account number or unique transaction reference number that can trace the transaction back to either the remittance sender or recipient.⁴⁴ Further, for domestic and international remittances, where remittances and other money transfers are made specifically from existing accounts, there is no need to perform CDD each time a remittance transfer is made following the initial account opening.⁴⁵

New recognition of financial exclusion risks in the area of remittances and other money transfer

services. The revised FATF Recommendations and new guidance reflect a growing recognition that overly strict CDD requirements disproportionate to the risks observed regarding remittances and other money transfer services threaten financial inclusion goals and risk relegating poor customers to informal means of moving funds, and that this, in turn, compromises a country's capacity to trace transactions and identify suspicious patterns. The interpretive note to the Recommendation on wire transfers states that to accomplish the objectives of the Recommendation "countries should have the ability to trace all wire transfers" but should also take into account "the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system."⁴⁶

Agents and AML/CFT

Agents and financial inclusion. In increasing numbers of countries worldwide, agents⁴⁷ are being used by banks and other financial institutions as a way to reduce cost and increase outreach to low-income customers—often these are customers who could not be reached profitably with traditional branch-based financial service delivery. The models vary widely from country to country and even within some countries. The common feature of agents (as the term is used in this Focus Note) is that a party other than the legal provider of the financial service—typically a local retail establishment—interacts with retail customers, often serving as the cash-in/cash-out point and potentially performing

42 FATF Financial Inclusion Guidance, p. 38, and FATF Recommendations, FATF Recommendation 10, p. 14.

43 Countries may elect to set a lower threshold in their AML/CFT regime. For cross-border wire transfers over USD/EUR 1000 (or the applicable lower threshold), the required information includes (a) the name of the originator; (b) the originator account number where such an account is used to process the transaction; (c) the originator's address, or national identity number, or customer identification number, or date and place of birth; (d) the name of the beneficiary; and (e) the beneficiary account number where such an account is used to process the transaction. The information about the originator needs to be verified for accuracy. And this information needs to be sent through the payment chain. See Interpretative Note to Recommendation 16 (Cross-Border Qualifying Wire Transfers), para 6.

44 FATF Recommendations, Interpretive Note to Recommendation 16, p. 72.

45 As mentioned in Box 4, "account" based remittance transfers could enable reductions in frequency of customer identification updates. This would suggest that CDD would not need to be done every time a remittance transaction is made by a specified account that is used by the specified account holder (after the initial transaction).

46 FATF Recommendations, Interpretive Note to Recommendation 16, p. 71.

47 In this Focus Note, an agent is considered any third party acting on behalf of a bank (or other principal), whether pursuant to an agency agreement, service agreement, or other similar arrangement.

other functions as well on the financial service provider's behalf.⁴⁸

FATF's approach to agents. FATF considers agents an extension of the financial service provider, which remains responsible for the agents' actions and for ensuring agents' compliance with FATF norms.⁴⁹ This includes the requirements outlined above on CDD, record-keeping, monitoring, and reporting suspicious transactions, as well as wire transfers and money and value transfer services. Agents' roles in record-keeping, monitoring, and reporting suspicious transactions vary based on the model in question,⁵⁰ and there are often opportunities to use the same communications infrastructure by which transaction details are transmitted between providers and agents (such as mobile phones) also to facilitate remote compliance, though at a minimum agents must be involved in identifying and reporting suspicious transactions, as they are the ones dealing directly with customers. (See Box 6.)

Cash-in/cash-out functions relating to wire transfer services⁵¹ fall within FATF's definition of money and value transfer services; therefore, the Recommendations applicable to wire transfers and money and value transfer services apply to agents that perform such functions on behalf

of the providers of the money or value transfer services (see "Accounts and Business Relationships, Occasional Transactions, and Special Rules for Wire Transfers and Money and Value Transfer Services").

Implications of the revised FATF Recommendations and new guidance for the use of agents. The previous version of the FATF Recommendations preceded widespread use of agents as they are used today around the world to advance financial inclusion. Among the challenges to the use of agents historically was the country-level interpretation given to the requirement that third parties to which a provider outsourced CDD responsibilities be "licensed or registered" by the competent national authority.⁵² The revised FATF Recommendations still require that money or value transfer service providers be licensed or registered by the country's competent authority. However, Recommendation 14 explicitly permits such providers to satisfy the licensing or registration requirement with respect to their agents⁵³ simply by maintaining an updated list of them and making the list accessible to relevant competent authorities if and when requested.⁵⁴ This is crucial as it applies, not just to the agents of banks and other traditional suppliers of money or value transfer services, but also to agents of the entire range of stored-value issuers that satisfy FATF's definition of money

48 FATF defines the term "agent" as follows for the purposes of Recommendations 14 and 16: "agent means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider" (FATF Recommendations, General Glossary, p. 110). It should be emphasized that FATF contrasts "reliance on third parties" (Recommendation 17) with an outsourcing or agency relationship, stating that the "third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity" (Interpretive Note to Recommendation 17, p. 77).

49 Indeed, the revised FATF Recommendations and new guidance make it clear that even when a third party dealing with customers on a provider's behalf is itself a financial institution "adequately subject to AML/CFT regulation and supervision by a competent authority," the provider retains ultimate responsibility for customer identification and verification (FATF Financial Inclusion Guidance, p. 35).

50 "AML/CFT functions of the principal financial institution and its agents should be seen as complementary and inclusive, keeping in mind that the principal financial institution bears ultimate responsibility for compliance with all applicable AML/CFT requirements" (FATF Financial Inclusion Guidance, p. 143).

51 An example of cash-in/cash-out transactions relating to wire transfers is a person-to-person remittance transfer of any form. Such functions would not include cash-in/cash-out transactions for bill payments, merchant payments, and other such services currently offered by agents of financial service providers in an increasing number of developing countries.

52 FATF Special Recommendations (2001, p. 14, Rec. SRVI [alternative remittance]).

53 FATF has a special definition for agents of money and value transfer service providers, which the General Glossary defines 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" (FATF Recommendations, p. 110).

54 FATF Recommendations, Recommendation 14, p. 17.

Box 6. Using Agents in AML/CFT Compliance: Illustrative Examples from Three e-Money Issuers

Table B6-A illustrates which entities are *operationally involved* on behalf of e-money issuers in managing AML/CFT compliance for particular stages of a typical P2P transaction. The comparisons have been made assuming that customers have registered electronic wallets (e-wallets) with the e-money issuer in question, and thus are treated as account-based, rather than occasional, transactions.

AML/CFT compliance management among e-money issuers can vary significantly across the diversity of business models that now exist around the world. Therefore, the practices of the three highlighted e-money issuers—M-PESA in Kenya, G-Cash in the Philippines, and Easypaisa in Pakistan—might not be applicable to other business models.

Table B6-A. Using Agents in AML/CFT Compliance

	M-PESA	G-Cash	Easypaisa
Initial e-Wallet Opening	A, CM	CM	A, CB
Entities Operationally Involved in Cash-In/ Cash-Out Transactions	A, ATM	A, ATM	A, ATM, B
Identification for Cash-In/Cash-Out Transactions	A	A	A
Verification for Cash-In/ Cash-Out Transactions	A, CM	A, CM	CB
Transaction Monitoring for P2P Transactions	CM	CM	CB
Nonface-to-Face Account Opening*	A, C, CM	A, C, CM	A, B, CB
Record Keeping	A, CM, O	A, CM, O	A, CB, O
Reporting Suspicious Transactions**	A, C, CM	A, CM	C, CB
Blocking Suspicious Transactions	A, CM	A, CM	CB

* For purposes of this table, “face to face” account opening takes place at a branch or other physical premises staffed by the financial institution’s employees, not using agents and not allowing the customer to automatically register for the e-wallet himself/herself.

** For purposes of this table, reporting suspicious transactions refers to the entities that may be operationally involved in some form to report suspicious transactions, not the entity legally authorized to report suspicious transactions.

A = agent; ATM = automated teller machine; B = branch personnel; C = customers; CB = Central Bank; CM = central compliance; NA = not applicable (nonexistent practice); O = other outsourced entity on behalf of central compliance

Source: M-PESA, G-Cash, Easypaisa, 2014.

or value-transfer service providers and whose business models potentially depend on vast agent networks that may be impossible to license or register individually.⁵⁵

The cost-reducing implications of this FATF provision are significant and translate into potential for increased outreach to financially excluded customers. It should be noted, however, that the service offerings available through agents of banks and other similar financial institutions in many countries are not always confined to money or

value transfer services. Many agents, for example, facilitate merchant payments, which are excluded from the FATF definition of money or value transfer services. These agents may, for example, also facilitate delivery of microinsurance, savings, and credit products. In the case of M-Shwari in Kenya, for example, agents facilitate access to a savings and credit product; the agents are managed by a mobile network operator, although the legal provider of the loans and savings accounts remains a bank.⁵⁶ For such agents, a country’s AML/CFT regime should calibrate the degree of oversight

⁵⁵ For all agents falling within FATF’s definition, the MVTS provider is required to include them in its AML/CFT programs and monitor them for compliance with these programs (FATF Recommendations, Recommendation 14, p. 17).

⁵⁶ See, e.g., <https://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/m-shwari>. Because the FATF Recommendations are activity based, rather than based on institutional type, if nonbank agents and bank agents in a given country offer identical financial services, the country’s AML/CFT regime should accord them identical treatment.

(by both the providers hiring them and the relevant authorities) to the specific services the agents offer and the risks they represent.

The new FATF guidance also takes stock of the importance of agents to an inclusion-friendly AML/CFT regime in additional respects. The nature of the typical retail establishments serving as agents to reach financially excluded populations is now understood, as is the fact that they see only part of the transactional picture with respect to a given customer.⁵⁷

Part II. Enforcement—The New FATF Assessment Methodology

FATF is unique among the global standard-setting bodies in that it has a comprehensive mechanism for assessing compliance with all its standards and a peer pressure mechanism to address compliance deficiencies.⁵⁸ The new Assessment Methodology carries significant potential ramifications for financial inclusion. Among these, the new focus on the effectiveness of a country's AML/CFT regime is the most fundamental, given that assessors may now consider both inadvertent financial exclusion and steps taken to increase financial inclusion as factors that may affect how effective the systems are at reaching their objectives.

Background

FATF Mutual Evaluations

FATF's Mutual Evaluations Reports, now entering their fourth round, are the means by which compliance with FATF standards is assessed. All FATF and FSRB member countries—which

collectively comprise nearly all the countries in the world—participate, with FATF and the separate FSRBs each conducting evaluation of its members.⁵⁹

Mutual evaluations are either conducted by teams composed of AML/CFT experts from FATF and FSRB member countries or by teams led by the World Bank or the IMF. The evaluations are a cooperative activity between the evaluating teams and the evaluated country. The result is a Mutual Evaluation Report, which is submitted for adoption by the FATF Plenary (including for mutual evaluations conducted by the IMF or the World Bank) or the relevant FSRB. This report becomes publicly available, and countries found to be insufficiently compliant are called on to improve their AML/CFT regimes based on the report's recommendations. A follow-up process with countries' reporting on progress made to address the deficiencies identified is organized after the publication of the report.

The FATF Lists and Their Ramifications

A Mutual Evaluation Report, which identifies a number of deficiencies, holds potential adverse economic implications for a country.⁶⁰ This negative potential increases when a country is placed on one of FATF's public lists of high-risk jurisdictions presenting major deficiencies and not making sufficient progress in addressing them. The listing process is overseen by FATF's International Cooperation Review Group (ICRG).⁶¹ Countries are referred to ICRG if they hold a specified threshold of key deficiencies based on their latest Mutual Evaluation Report, do not participate in the global network as a member of FATF or

⁵⁷ "Retailers generally have only partial knowledge of the transactions conducted by the customer (i.e., the transaction conducted in their particular shops)" (FATF Financial Inclusion Guidance, p. 43).

⁵⁸ The Basel Committee on Banking Supervision has implemented an assessment program for country-level compliance with the Basel III Capital Accords, though the program does not assess compliance with Basel Committee standards and guidance across the board (April 2012 Basel III regulatory consistency assessment program). See <http://www.bis.org/publ/bcbs216.pdf>.

⁵⁹ For the schedule of mutual evaluations as of April 2014 for FATF and FSRBs, and conducted by FATF, FSRBs, IMF, or the World Bank, see <http://www.fatf-gafi.org/media/fatf/documents/assessments/Global-Assessment-Calendar.pdf>. In countries such as Mexico, which is both a FATF and an FSRB member, FATF's policy is that FATF members that are also members of FSRB(s) will undergo a joint evaluation by these bodies.

⁶⁰ See, e.g., <http://allafrica.com/stories/201404100466.html> (9 April 2014).

⁶¹ As of June 2014, FATF is currently reviewing the ICRG process, to align it with the new 4th Round of Mutual Evaluation follow-up processes.

an FSRB, or are referred by any FATF member country. Each ICRG-reviewed country is provided an opportunity to participate in face-to-face meetings with the relevant ICRG regional review group to discuss the report, as well as the chance to develop an action plan with FATF to address the identified deficiencies. The agreed action plan, which is not a public document, provides the basis for evaluating progress. FATF specifically requests high-level political commitment from each reviewed jurisdiction to implement these action plans, which are updated as reforms are implemented. FATF publically reports progress (or lack of progress) on the action plan and its underlying rationale, providing significant peer

pressure for countries to improve their AML/CFT regimes.

FATF's tiers of public lists of high-risk jurisdictions—colloquially referred to as the “grey, dark grey, and black lists”—trigger four different possible calls for action by FATF (determined by consensual agreement among FATF member countries during a thrice yearly FATF Plenary meeting) as shown in Table 1.

FATF itself has no independent sanctioning authority. However, Recommendation 19 states that countries should require financial institutions to apply enhanced due diligence when this is called

Table 1. FATF's Public Lists, as of June 2014

FATF Listing Categories	FATF Call for Action	Number of Countries
BLACK (with call for counter-measures) High-risk and noncooperative jurisdictions	“The FATF calls on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing risks emanating from the jurisdictions.”	2
BLACK Jurisdictions that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies	“The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction.”	4
DARK GREY Jurisdictions not making sufficient progress	“The FATF is not yet satisfied that the following jurisdictions have made sufficient progress on their action plan agreed upon with the FATF. The most significant action plan items and/or the majority of the action plan items have not been addressed. If these jurisdictions do not take sufficient action to implement significant components of their action plan by xx, then the FATF will identify these jurisdictions as being out of compliance with their agreed action plan and will take the additional step of calling upon its members to consider the risks arising from the deficiencies associated with the jurisdictions.”	0
GREY Jurisdictions that have made “high-level political commitment to address the deficiencies through implementation of an action plan developed with the FATF”	“The FATF calls on these jurisdictions to complete the implementation of action plans expeditiously and within the proposed timeframes. The FATF will closely monitor the implementation of these action plans and encourages its members to consider the information [FATF] presented [on the countries].”	22

Source: FATF. <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/public-statement-june-2014.html> and <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2014.html>

for by FATF and “apply countermeasures when called upon to do so by the FATF.” FATF’s calls to action have historically been heeded, particularly with respect to countries listed as high risk and noncooperative.⁶³

For grey-listed countries the consequences may be less severe than for black-listed countries, including those for which counter-measures are called for, though still substantial, potentially affecting not just the decision making of foreign financial institutions with respect to business in the country in question, but also the contracting and investment decisions of companies across the economic spectrum.⁶⁴

Unfortunately there is little empirical evidence analyzing the aggregate economic impact on countries of appearing on these lists; the economic effects of criminal flows of funds have also not been extensively studied by economists to date.⁶⁵

New Assessment Methodology and Financial Inclusion

Assessment Methodology Components and Their Relationship

Given the potential political and economic consequences, fear of negative Mutual Evaluation Reports has historically steered some countries toward “over-compliance” with aspects of the FATF Recommendations—sometimes with a particular adverse impact on financial inclusion (Isern and de Koker 2009). The assessment methodology used before the 2012 revisions to the FATF Recommendations primarily evaluated the extent to which a country’s AML/CFT regime

met the technical requirements of FATF standards. Effectiveness was used only as a variable to adjust the ratings. The new Assessment Methodology dramatically changes this dynamic by introducing, in addition to the technical assessment component, a component analyzing the *effectiveness* of the evaluated AML/CFT regime—that is, the extent to which the regime actually accomplishes its objective to prevent money laundering and terrorist financing. For example, the new Assessment Methodology calls for judgments on whether the prescribed AML/CFT preventive measures are commensurate to particular risks faced, which would have a bearing on the overall effectiveness of a country’s AML/CFT regime. A country with negligible domestic capital markets and high use of cash might be found to have an ineffective AML/CFT regime if it is spending significant money and staff resources policing its companies’ registries and securities sector, instead of focusing on the area of high risk. Conversely, an effective AML/CFT regime for a sophisticated financial center providing easily usable incorporation services would need to include close attention and devote significant resources to such issues (Pesme and Van Der Does 2014).

The effectiveness and technical assessments are linked enquiries. In the majority of cases, a low level of technical compliance will probably result in a low level of effectiveness. For example, the lack of appropriate laws and regulations to combat money laundering and terrorist financing would mean that authorities do not have a sufficient legal basis to prevent—or possibly even to investigate—financial crime and other illicit activities.⁶⁶ This technical

63 In FATF’s February 2014 Public Statement regarding Iran and North Korea, e.g., FATF called on its members and other jurisdictions to apply counter-measures (which could be interpreted as including sanctions) “to protect the international financial system from the on-going and substantial money laundering and terrorist financing risks emanating from the jurisdictions.” <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatf-public-statement-oct-2013.html>. See, also, Wright (2008).

64 See Byron (2014). Further, see Halliday, Levi, and Reuter (2014).

65 While the literature is minimal, the IMF has published research examining the macroeconomic impacts of some countries faced with AML/CFT sanctions. See IMF (2011, pp. 82–83).

66 Many countries, e.g., have AML laws and regulations that comply with the FATF Recommendations, but they lack FATF-compliant CFT laws and regulations. See, e.g., <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/public-statement-feb-2014.html>. Indeed, a primary motivation for FATF public listing of many countries currently listed is nonexistent or deficient CFT laws and regulations.

deficiency would generally also dictate low AML/CFT effectiveness levels in the country.

It is also possible that a highly technically compliant country does not have an AML/CFT regime that addresses its risks with a similarly high level of effectiveness. This possibility is particularly relevant to financial inclusion. A country might, for example, have technically compliant AML/CFT measures in place that protect its formal financial services against criminal abuse, but which in turn are so strict or expensive to comply with that the majority of the population is compelled to use informal services.

The starting point for every assessment, applicable to both the technical compliance component and the effectiveness component, is the assessors' identification, understanding, and assessment of the country's risks and context, in the widest sense, and elements that contribute to them.⁶⁷ In this regard, there are four broad areas assessors should consider—risks, materiality, structural elements, and contextual factors:⁶⁸

- The nature and extent of the money laundering and terrorist financing *risks* in the country.
- The circumstances of the country affecting the *materiality* of different Recommendations (e.g., the makeup of its economy and its financial sector).
- *Structural elements* that underpin the AML/CFT regime (e.g., political stability; a high-level commitment to address AML/CFT issues; stable institutions with accountability, integrity, and transparency; the rule of law; and a capable, independent, and efficient judicial system).

- Other *contextual factors* that could influence the way AML/CFT measures are implemented and how effective they are (such as the maturity and sophistication of the regulatory and supervisory regime in the country, the level of corruption, and the impact of measures to combat corruption or the level of financial exclusion).⁶⁹

Technical Compliance Component

The technical compliance component of the new Assessment Methodology evaluates the design of a country's legal, regulatory, and supervisory framework for AML/CFT against FATF's technical requirements, for example, whether the country has criminalized money laundering and terrorist financing as prescribed and whether the required regulatory authorities were created and endowed with relevant powers. The technical compliance assessment does not consider whether laws and authorities are effective, but merely whether they exist and are sufficient to meet FATF's technical standards. For each of the FATF Recommendations, assessors should reach a conclusion about the extent to which a country complies (or not) with the standard. There are four possible levels of technical compliance: compliant, largely compliant, partially compliant, and noncompliant.⁷⁰

Effectiveness Component

High-Level Outcome, Intermediate Outcomes, and Immediate Outcomes. The Assessment Methodology defines *effectiveness* as the "extent to which the defined outcomes are achieved."⁷¹ The "High-Level Outcome" for any AML/CFT regime under evaluation is that "[f]inancial systems and the broader economy are protected from the

⁶⁷ For additional information on the key pillars of the risk assessment, see FATF (2013c, p. 21).

⁶⁸ See Assessment Methodology, pp. 5 and 130. The Mutual Evaluation Report template calls for a section setting out the country's main policies and objectives for combating money laundering and terrorist financing, "noting where there are also wider policy objectives (such as financial inclusion) which affect the AML/CFT strategy" and calls on assessors to "note any other contextual factors that might significantly influence the effectiveness of the country's AML/CFT measures," including such issues as financial exclusion (Assessment Methodology, Annex II—Mutual Evaluation Report Template, p. 130).

⁶⁹ FATF makes a distinction between "structural elements" and "other contextual factors," though there could be overlap among them. Structural elements define the baseline environment relevant to AML/CFT, whereas "other contextual factors" connote a broader universe of factors bearing on overall technical compliance and effectiveness (including unique, context specific factors that may not be easily grouped in the three other key criteria).

⁷⁰ In exceptional circumstances, a Recommendation may also be rated as not applicable (Assessment Methodology, p. 11).

⁷¹ Assessment Methodology, p. 14.

threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security.”⁷² Three “Intermediate Outcomes” contribute to the “High Level Outcome,” and they entail that

- Policy, coordination, and cooperation mitigate the money laundering and financing of terrorism risks.
- Proceeds of crime and funds in support of terrorism are prevented from entering the financial and other sectors or are detected and reported by these sectors.
- Money laundering threats are detected and disrupted, and criminals are sanctioned and deprived of illicit proceeds. Terrorist financing threats are detected and disrupted, terrorists are deprived of resources, and those who finance terrorism are sanctioned, thereby contributing to the prevention of terrorist acts.⁷³

The assessment of effectiveness should not directly focus on the Intermediate or High-Level Outcomes, but rather on evaluating the extent to which a country achieves 11 “Immediate Outcomes” (see Box 7).

To guide assessors, the Assessment Methodology includes for each Immediate Outcome a box with characteristics of an effective AML/CFT regime with respect to the outcome in question. These boxes set out the situation in which a country is effective at achieving the outcome in question and provide the benchmark for the assessment. They also correlate the Immediate Outcome with the primarily relevant FATF Recommendations.⁷⁴

In addition, for each Immediate Outcome there is a list of “Core Issues” to be considered in determining if the outcome is being achieved, together with examples of information and specific factors to

Box 7. Immediate Outcomes Indicating an Effective AML/CFT Regime^a

1. Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.
2. International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.
3. Supervisors appropriately supervise, monitor, and regulate financial institutions and defined nonfinancial businesses or professions (DNFBPs) for compliance with AML/CFT requirements commensurate with their risks.
4. Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks and report suspicious transactions.
5. Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.
6. Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.
7. Money laundering offenses and activities are investigated, and offenders are prosecuted and subject to effective, proportionate, and dissuasive sanctions.
8. Proceeds and instrumentalities of crime are confiscated.
9. Terrorist financing offenses and activities are investigated, and persons who finance terrorism are prosecuted and subject to effective, proportionate, and dissuasive sanctions.
10. Terrorists, terrorist organizations, and terrorist financiers are prevented from raising, moving, and using funds, and from abusing the nonprofit sector.
11. Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving, and using funds, consistent with the relevant UN Security Council Resolutions.

a. Assessment Methodology, p. 15.

⁷² Assessment Methodology, p. 14.

⁷³ Assessment Methodology, p. 14

⁷⁴ Predictably, at least elements of Recommendation 1—the RBA—are recognized as correlating with a large number of Immediate Outcomes: Immediate Outcome 1 and Immediate Outcomes 3–10.

support a conclusion on the issue in question. The Core Issues are the mandatory questions assessors should seek to answer to get an overview of how effective a country is under each outcome.

For each Immediate Outcome there are four possible ratings for effectiveness, based on the extent to which the identified Core Issues and characteristics are addressed: high level of effectiveness, substantial level of effectiveness, moderate level of effectiveness, or low level of effectiveness.

Elements of effectiveness assessment relevant to financial inclusion. Most of the Immediate Outcomes have at least some relevance to financial inclusion, though Immediate Outcomes 1, 3, and 4 are the most directly relevant.⁷⁵ Moreover, the Assessment Methodology's general mandate to assessors to consider a country's specific money laundering and terrorist financing risk picture; the materiality of different Recommendations in that country's case; structural elements, such as political stability and the rule of law; and contextual factors, including the country's level of financial exclusion, introduces the opportunity for financial inclusion considerations to play a major role in effectiveness assessments.

The following topical areas cutting across various Immediate Outcomes merit highlighting, as set forth in Box 8.

Implications of effectiveness assessments for financial inclusion. Effectiveness assessments may have a significant positive impact on countries that have not yet fully embraced financial inclusion. Assessment questions regarding the measures that were taken to promote financial inclusion and whether the application of AML/CFT measures prevent the legitimate use of the formal financial

system should help to focus the attention of countries that are not promoting inclusion or have adopted exclusionary AML/CFT measures. Assessors may also recommend practical steps that countries should take to address financial exclusion risk. In these cases, the assessments may have a beneficial impact on financial inclusion policies.

For countries that have adopted financial inclusion measures involving simplified CDD, the effectiveness assessments will put a premium on the quality and documentation of the risk assessments performed, both by policy makers and providers, as assessors will be looking for evidence to substantiate a claim of lower money laundering and terrorist financing risk. If providers are permitted to apply simplified CDD measures where risks have not been adequately assessed and are actually high, the effectiveness of the AML/CFT regime in question could be assessed negatively, which in turn could have a chilling effect on financial inclusion policy making going forward in that country.

In general, the effectiveness component of the new round of assessments will emphasize unique country conditions and factors more strongly than under the previous Assessment Methodology, which primarily focused on technical compliance with FATF standards. The new Assessment Methodology requires assessors to tailor their approach to the profile of the country in question more than the previous assessment methodology when designing, scoping, and performing their assessment; further, the effectiveness component will be country specific—including weighing the money laundering and terrorist financing risks of financial exclusion. On the one hand, this liberates policy makers from a "one size fits all" mentality out of step with their on-the-ground realities. On the other hand, there will be less scope for reliance on assessments from other countries as potential benchmarks.⁷⁶

⁷⁵ The Assessment Methodology also makes the point that the Immediate Outcomes are not independent of each other. In many cases an issue considered specifically under one Immediate Outcome will also contribute to the achievement of other outcomes (Assessment Methodology, p. 19).

⁷⁶ South Africa's CCD-related reforms of the mid-2000s, e.g., were studied by other countries considering similar financial inclusion approaches, but some countries waited to see how FATF assessors would judge these measures in the 2009 South Africa Mutual Evaluation Report before proceeding with their own national initiatives.

Box 8. Effectiveness Assessments: What Are the Specific Opportunities for Advancing Financial Inclusion?

Financial inclusion can be included as an area of increased focus—In the scoping note prepared in advance of a mutual evaluation, the nature and extent of financial exclusion and measures taken to increase financial inclusion could be included in the list of areas for increased focus by the evaluators (FATF 2013e, p. 8).

Risk and associated alignment of risk-based measures for lower-risk financial inclusion products and services must be assessed—Core Issues to be considered in relation to Immediate Outcome 1 (regarding risk assessment and mitigation) focus on the overall quality of the country’s money laundering and terrorist financing risk mitigation systems. Assessors are specifically required to consider how risk assessments were used to justify exemptions and to support the application of simplified measures for lower-risk scenarios. In view of the importance of risk assessment and mitigation to the revised FATF Recommendations, risk-related questions also feature in the assessment of a number of other Immediate Outcomes, especially Immediate Outcomes 3 and 4.

Levels of financial exclusion to be considered—Assessors are called on to consider various structural and contextual factors relating to a country when assessing the effectiveness of its AML/CFT regime. The level of financial exclusion is specifically mentioned as a factor to be considered.^a Given the formal recognition of financial exclusion as a money laundering and terrorist financing risk in the approval by FATF Ministers of the organization’s 2012–2020 mandate, the stage is set for assessors to evaluate negatively the effectiveness of AML/CFT regimes that poorly take advantage of the flexibility afforded

by the FATF Recommendations to bring excluded populations into the world of traceable formal finance.

Informal and unregulated services may be assessed—Assessors may ask for data regarding the size, composition, and structure of the country’s financial sector and its informal or unregulated sector to determine the relative size, importance, and materiality of each. If a substantial volume of transactions in a given country falls outside the formal, regulated sphere, it could be evidence of regulatory and supervisory approaches that are ineffective at achieving Immediate Outcome 3 (regarding regulation and supervision). The examples of specific factors that could support conclusions on Immediate Outcome 3 include the extent to which supervisory and regulatory measures inhibit the use of the formal financial system.^b

Financial exclusion and the promotion of financial inclusion may be probed—Immediate Outcome 4 (regarding institutional risk management and compliance) invites the question whether the manner in which AML/CFT measures are applied prevents the legitimate use of the formal financial system and what measures are taken to promote financial inclusion. For example, the overall national regulatory and supervisory approach in a country, among other factors, could trigger “over-compliance” by providers, that is, AML/CFT controls that are disproportionate to the risks of serving financially excluded customers, preventing potential customers from legitimate use of the formal financial system, and perpetuating financial exclusion.

a. Assessment Methodology, p. 6.

b. Assessment Methodology, pp. 97–98.

Part III. The Road Ahead—Opportunities for Country-Level Progress and Foreseeable Challenges Meriting Further Attention

The flurry of FATF actions in 2012 and 2013—including the FATF Ministerial declaration that financial exclusion presents money laundering and terrorist financing risks, the adoption of the revised FATF Recommendations, the guidance on financial inclusion and on new payment products and services, and the new Assessment Methodology—

marks a remarkably productive period of rapid evolution in standards and guidance on AML/CFT. As FATF and FSRBs turn their attention to their new round of mutual evaluations, a new chapter opens—one in which country-level leadership applying the revised FATF Recommendations and guidance can inform future global discussion of what works to build AML/CFT regimes that are both financial-inclusion friendly and effective at combatting money laundering and terrorist financing. There are both current opportunities for progress and foreseeable challenges meriting further attention.

Opportunities for Progress

Since 2011,⁷⁷ FATF has made significant progress toward enabling countries to align financial inclusion and financial integrity objectives through risk-based policy making. The onus is now on country-level policy makers to take advantage of the additional guidance and clarity and demonstrate “results on the ground.” By building the evidence base of approaches that achieve this alignment, countries will be advancing an increasingly important domestic policy agenda while also helping FATF and their peers committed to combatting financial exclusion.

To build this evidence base, policy makers must also develop their own understanding of the fast-evolving landscape of providers capable of serving financially excluded populations. New models that hold potential for inclusion—and bring new customers into the traceable world of electronic transactions—also raise new risks that both policy makers and providers will best address through knowledge-sharing.

Though the new round of mutual evaluations will yield more country context-specific reports than under the previous assessment methodology, there will still be value in cross-country dialogue. In particular, in 2014 the effectiveness assessment is being tested on developing countries for the first time.⁷⁸ There will be a vital period of “test and learn” by both FATF and countries to fine-tune the new processes—processes with important potential to counter the incentives for an overly conservative approach that could perpetuate financial exclusion.

Countries also have an opportunity—and a strong interest—to document thoroughly their domestic

realities as to both money laundering and terrorist financing risk and financial inclusion.⁷⁹ Sharing of such documentation will help to build global understanding about the diversity of country contexts in which policy makers are seeking to align simultaneous pursuit of financial inclusion and financial integrity.⁸⁰

Foreseeable Challenges Meriting Further Attention

A “test and learn” approach presupposes that not everything will work out as anticipated. Countries must therefore be prepared to give feedback to FATF about what is working and what is not, whether directly, in the case of FATF members, or indirectly, through their respective FSRBs, so that these unforeseen challenges emerging from the new standards and guidance are understood and addressed.

Other challenges are by their nature more foreseeable, and while they may not be appropriate for FATF guidance (or may not yet be ripe), they nonetheless merit further country-level attention and global discussion and analysis.

Assessor capacity and judgment. Assessors participating in mutual evaluations are picked from a wide range of institutions and countries with varying perspectives, awareness, and capacity levels. As a result, country assessor teams and the authorities in the countries they are assessing will have different interpretations on the nature, type, and extent of risk; the approach to be used to measure risk; and its relative weighting in the overall assessment given that judgment will be involved when considering a risk assessment (Pesme and Van Der Does 2014). A number of steps—such as strengthened training

⁷⁷ The initial FATF guidance on financial inclusion was adopted in June 2011. See FATF (2011).

⁷⁸ The Democratic Republic of Congo and Ethiopia are the first developing countries to undergo a mutual evaluation with the revised Assessment Methodology. (Neither country has had a full mutual evaluation under the previous methodology.)

⁷⁹ As noted, the specifics of a country’s context must inform its national risk assessment, and the rationale and evidence behind specific AML/CFT regulatory and supervisory decisions should be documented looking ahead to a mutual evaluation sometime in the future.

⁸⁰ Policy maker appetite for such sharing and building of global understanding can be seen in the establishment of the Alliance for Financial Inclusion’s Financial Integrity Working Group. See <http://www.afi-global.org/about-us/how-we-work/about-working-groups/financial-integrity-working-group-fintwg>.

of assessors and upstream quality control of draft Mutual Evaluation Reports—have already been taken to strengthen the quality and consistency in the assessment process. Moreover, since the timetable for the new round of mutual evaluations stretches over approximately seven years, country and assessor awareness and capacity can be built incrementally.

Deepening understanding of financial exclusion risk and factoring it into national risk assessments. The nature and extent of financial exclusion risk has yet to be systematically studied. Indeed the February 2013 FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment does not mention financial exclusion. As a consequence, countries currently are challenged to think through largely for themselves the specific money laundering and terrorist financing risks flowing from transactions in the cash economy by populations excluded from, or underserved by, the formal financial system.⁸¹

At the same time, a majority of countries have not yet conducted a national risk assessment. There is therefore an important opportunity to introduce this subject explicitly into their risk assessment planning and to build regional and global understanding on the subject country by country. Doing so will be vital to providing a balanced picture of national money laundering and terrorist financing risks—one that also focuses appropriate attention on the risk-mitigating benefits of increased financial inclusion.

“Proving” low risk. While the FATF actions discussed above introduce significant guidance regarding lower-risk scenarios, countries have been left for the time being to explore how low-risk situations are “proven.” The issue is important because the FATF Recommendations explicitly permit countries “in strictly limited circumstances and where there is a *proven low risk* of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity” (*emphasis supplied*).⁸² On the one hand, this leaves the door open to responsible country-level experimentation, which can contribute incrementally to the global knowledge base. On the other hand, some countries may be reluctant to take advantage of this flexibility until there are other examples to follow.⁸³

Reducing incentives for provider-level over-compliance and taking stock of its consequences. Given that over-compliance at the provider level (which perpetuates or exacerbates financial exclusion) increases national-level (and in some cases international-level)⁸⁴ money laundering and terrorist financing risk, policy makers have an impetus to seek ways to reduce incentives for over-compliance and create incentives for those providers willing to offer lower-risk products and services. A first step is gaining a better understanding of the dynamics shaping compliance behavior generally at the country level, regionally, and internationally, as well as the specific drivers of over-compliance.⁸⁵

81 Countries could leverage the national risk assessment tools offered by the World Bank and IMF to scope the nature and extent of their financial exclusion risk. The World Bank offers a “Financial Inclusion Product Risk Assessment Module” (for formal financial inclusion products) to complement its National ML/TF Risk Assessment Tool. In the World Bank tool, specifically, national risk levels are based on overall threat and vulnerability levels. High levels of financial exclusion would be incorporated in the vulnerability assessment, which has a bearing on the overall national risk. For more information about the World Bank tools, see FATF Financial Inclusion Guidance, p. 69.

82 FATF Recommendations, Interpretive Note to Recommendation 1, p. 31.

83 It has been observed that “the requirement that low risk must be proved or demonstrated is problematic in respect of new products and services such as mobile money. The language creates a regulatory deadlock: proof and demonstration requires evidence and evidence can only be generated by launching and testing the product. Yet, the product cannot be launched without a facilitative regulatory framework that can only be shaped within the context of the low-risk exception and exemptions. When the text of the FATF Recommendations and interpretative notes are amended, it would be helpful if the word ‘proven’ is not used in this context. Language that supports a thorough and objective risk assessment and a reasonable and justifiable conclusion about the risk profile of a product will be more appropriate to financial inclusion products than language requiring proof and demonstration” (de Koker 2011).

84 See, e.g., Box 5. Further, FATF has acknowledged that over-compliance by regulators and financial institutions may increase overall money laundering and terrorist financing risks (FATF Financial Inclusion Guidance, p. 18).

85 Some of these drivers are outside the control of country-level policy makers. For example, the high profile \$1.9 billion fine imposed on HSBC by U.S. authorities (<http://www.reuters.com/article/2012/12/11/us-hsbc-probe-idUSBRE8BA05M20121211>) figures among the key drivers of a phenomenon referred to by global banks as “financial crime related de-risking,” triggering their exit from entire markets and market segments that wary compliance officers assess to create too great an exposure for the profitability of the business in question.

Though the revised FATF Recommendations enshrine the RBA as Recommendation 1, which is intended to inform all the subsequent Recommendations, there is no explicit standard and/or guidance provided for addressing over-compliance, which undermines the purpose of the RBA: the proportionate allocation of limited resources applicable to both country-level supervision and enforcement and provider compliance. For example, if the law allows providers to adopt simplified due diligence measures in relation to a lower-risk product but they elect to apply the same CDD measures across the board, it is appropriate to explore the extent to which this disproportionate allocation impinges on their ability to mitigate higher money laundering and terrorist financing risks—as well as the extent to which such compliance practices contribute to financial exclusion risk.

Deepening the conversation on “financial identity,” considering both its law enforcement and privacy dimensions. The landscape of financial identity at the base of the economic pyramid is changing rapidly with the spreading of mobile financial services among poor populations around the world and large-scale initiatives such as India’s Aadhaar national digital identity system.⁸⁶ These developments challenge a simple, binary understanding of an “anonymous” account or transaction versus one where a customer is “identified” and that identity is verified. As observed above, when customers move from using cash to a mobile wallet with strict limits on the amounts and frequency involved and number of other parties with whom they can transact, the money laundering and terrorist financing risk may remain low while minutely specific “financial identities” emerge,

associated with the SIM cards used. Moreover, these SIM-based financial identities, coupled with the feasibility of mapping transaction flows down to the level of specific cell phone towers and agent locations offer both providers and law enforcement new means of discerning suspicious transactions and finding perpetrators of financial crime. If readily available phone usage data and patterns, coupled with geo-tagged location data that pinpoint the whereabouts of the customer, are added to the picture, law enforcement’s capacity to identify and apprehend anyone using mobile financial services for criminal purposes increases considerably.

At the same, the data privacy dimensions of this changing landscape are a subject of fervent international debate.⁸⁷ Many of the countries standing to benefit most from the financial inclusion potential of these developments will also be among those least likely to have effective data privacy protection in place or the resources to address related newly emerging consumer risks. In countries where corruption is high, the risk of misuse of personal data may be high as well.

The policy questions triggered are complex for country-level policy makers, and even more so for multilateral bodies including FATF and those interested in financial consumer protection more broadly.⁸⁸ They also are not to be ignored.

Optimizing the linkages among financial inclusion, stability, integrity, and consumer protection. Both country-level policy makers and increasingly also international financial sector standard-setting bodies simultaneously pursue the objectives of financial inclusion, financial stability, financial integrity, and financial consumer protection.

⁸⁶ <http://www.uidai.gov.in/>

⁸⁷ See, e.g., Financial Times (2014).

⁸⁸ An example is the G20/OECD Financial Consumer Protection Task Force, which produced the G20’s High Level Principles on Financial Consumer Protection. Principle 8, Protection of Consumer Data and Privacy, provides as follows: “Consumers’ financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties). The mechanisms should also acknowledge the rights of consumers to be informed about data-sharing, to access data and to obtain the prompt correction and/or deletion of inaccurate, or unlawfully collected or processed data.” <http://www.oecd.org/daf/fin/financial-markets/48892010.pdf>

There is increasing understanding that, at the level of outcomes, these four objectives are interdependent and may be mutually reinforcing.⁸⁹ In practice, at the policy-making level, the linkages are less well known, and policy makers face choices that are often unnecessarily framed as trade-offs. Important country-level work is currently underway to deepen understanding on how policy makers can optimize the linkages among the four objectives, maximizing synergies and minimizing trade-offs and other negative outcomes.⁹⁰ In the AML/CFT context, of course, the pair-wise linkages between the objectives of inclusion and integrity loom particularly large, as they underlie the formal recognition of financial exclusion as a money laundering and terrorist financing risk in the approval by FATF Ministers of the organization's 2012–2020 mandate.⁹¹

References

Basel Committee on Banking Supervision. 2014. "Sound Management of Risks Related to Money Laundering and Financing of Terrorism." Basel Committee Document, January.

———. 2012. "Basel III Regulatory Consistency Assessment Programme." April. <http://www.bis.org/publ/bcbs216.pdf>

Byron, Rejaul Karim. 2014. "Steps against Money Laundering under Review." *The Daily Star* website, 14 February. <http://www.thedailystar.net/steps-against-money-laundering-under-review-11229>

CGAP. 2012. "Financial Inclusion and the Linkages to Stability, Integrity and Protection: Insights from the South African Experience." Washington, D.C.: CGAP. http://www.cgap.org/sites/default/files/Working-Paper-Insights-from-the-South-African-Experience-Nov-2012_0.pdf

———. 2013. International Remittances and Branchless Banking: 2013 Landscape. Slide presentation. Washington, D.C.: CGAP, 12 July. <http://www.slideshare.net/CGAP/international-remittances-through-branchless-banking>.

Chatain, Pierre, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis De Koker. 2011. "Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions." *Directions in Development*. Washington, D.C.: World Bank, February.

Corkery, Michael. 2014. "Immigrants from Latin America and Africa Squeezed as Banks Curtail International Money Transfers." *The New York Times* website, 6 July. http://dealbook.nytimes.com/2014/07/06/immigrants-from-latin-america-and-africa-squeezed-as-banks-curtail-international-money-transfers/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1

CPSS (Committee on Payment and Settlement Systems). 2012. "Innovations in Retail Payments: Report of the Working Group on Innovations in Retail Payments." Bank for International Settlements, May.

89 In November 2012, the G20 Financial Ministers and Central Bank Governors explicitly recognized the importance of the inter-relationship among these objectives, commending FATF and the other financial sector standard-setting bodies for their growing commitment "to provide guidance and to engage with the GPF to explore the linkages among financial inclusion, financial stability, financial integrity and financial consumer protection" (Communiqué of the G20 Finance Ministers and Central Bank Governors, Mexico City, 4–5 November 2012).

90 See, e.g., CGAP (2012). In its capacity as Co-Chair of the Subgroup of the GPF focused on engagement with the standard-setting bodies, the UK Department for International Development (DFID) funded CGAP as GPF Implementing Partner to conduct the rapid research initiative documented in this report, to inform the work of the Subgroup. Similar rapid research exercises on the linkages among inclusion, stability, integrity, and consumer protection have now been carried out in Pakistan and Russia as well, and reports are forthcoming.

91 Recent research by the World Bank further explores the pairwise linkage between inclusion and integrity in the context of cross-border remittances, which may be particularly timely given the recent actions by banks in the United Kingdom and other countries (see Box 5). Although this phenomenon is not new, it deserves further exploration and new evidence that could contribute to a potentially fundamental rethinking of the calibration of risks in international finance. See Todoroki, Noor, Celik, and Kulathunga (2014).

- de Koker, Louis. 2011. "Aligning Anti-Money Laundering, Combating of Financing of Terror and Financial Inclusion: Questions to Consider When FATF Standards Are Clarified." *Journal of Financial Crime*, Vol. 18, No. 4, pp. 361–86.
- FATF (Financial Action Task Force). 2011. FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. June.
- . 2012a. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations. February.
- . 2012b. Financial Action Task Force Mandate (2012–2020). April.
- . 2012c. Declaration of the Ministers and Representatives of the Financial Action Task Force, Report to G20 Leaders by the Financial Action Task Force. June. <http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20to%20G20%20Leaders%20June%202012%20.pdf>
- . 2013a. Methodology for Assessing the Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems. February.
- . 2013b. FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. February.
- . 2013c. FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment. February.
- . 2013d. Guidance for a Risk Based Approach: Prepaid Cards, Mobile Payments and Internet Based Payment Services. June.
- . 2013e. Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations. October. <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF-4th-Round-Procedures.pdf>, p. 16.
- Financial Times. 2014. "European Court of Justice rules EU data collection laws illegal." *Financial Times*, 8 April.
- Halliday, Terence C., Michael Levi, and Peter Reuter. 2014. "Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism." Urbana, Ill.: Center on Law and Globalization. http://www.lexglobal.org/files/Report_Global%20Surveillance%20of%20Dirty%20Money%201.30.2014.pdf
- IMF (International Monetary Fund). 2011. "Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)—Report on the Review of the Effectiveness of the Program." Washington, D.C.: IMF, 11 May. <http://www.imf.org/external/np/pp/eng/2011/051111.pdf>
- Isern, Jennifer, and Louis de Koker. 2009. "AML/CFT: Strengthening Financial Inclusion and Integrity." Focus Note 56. Washington, D.C.: CGAP, August.
- National Public Radio. 2014. "As Wire Transfer Options Dwindle, Somali-Americans Fear a Lost Lifeline." Morning Edition, 8 July.
- Noor, Wameek. 2013. "Anti-Money Laundering Regulation and Financial Inclusion." CGAP Blog, 15 May. <http://www.cgap.org/blog/anti-money-laundering-regulation-and-financial-inclusion>
- Pesme, Jean, and Emile Van Der Does. 2014. "Assessing the Assessors: From Form to Substance." World Bank Blog, 6 February. <https://blogs.worldbank.org/psd/assessing-assessors-form-substance>.
- Ratha, Dilip. 2005. "Remittances: A Lifeline for Development." *Finance and Development*, December. <http://www.imf.org/external/pubs/ft/fandd/2005/12/basics.htm>.

———. 2012. "Remittances: Funds for the Folks Back Home." *Finance and Development*. <http://www.imf.org/external/pubs/ft/fandd/basics/remitt.htm>

Todoroki, Emiko, Wameek Noor, Kuntay Celik, and Anoma Kulathunga. 2014. "Making Remittances Work: Balancing Financial Integrity and Inclusion." *Directions in Development*, May. Washington, D.C.: World Bank.

U.K. Parliament. 2013. Written Ministerial Statement, Money Service Businesses, HM Treasury (10 October). <http://www.parliament.uk/documents/commons-vote-office/October%202013/10%20October/2.CHANCELLOR-money-service-businesses.pdf>

Vlaanderen, Paul. 2010. FATF President's Presentation at the 3rd Windsor Global Leadership Seminar on Regulating Transformational Branchless Banking, March. <http://www.oecd.org/unitedkingdom/financialinclusionandfinancialintegritycomplementarypolicyobjectives.htm>

World Bank. 2013. Migration and Development Brief. Washington, D.C.: World Bank, April. <http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationDevelopmentBrief20.pdf>

Wright, Robin. 2008. "Stuart Levey's War." *The New York Times* website, 31 October. <http://www.nytimes.com/2008/11/02/magazine/02IRAN-t.html?pagewanted=all&r=0>

Annex I. Abbreviations

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
DNFBP	Defined Nonfinancial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSRB	FATF Style Regional Body
GPII	Global Partnership for Financial Inclusion
ICRG	FATF's International Cooperation Review Group
IMF	International Monetary Fund
KYC	Know Your Customer
MNO	Mobile Network Operator
MSB	Money Service Business
MVTS	Money or Value Transfer Service
NPPS	New Payment Products and Services
OECD	Organization of Economic Cooperation and Development
OTC	Over the Counter
P2P	Person to Person
RBA	Risk-Based Approach
UNSGSA	United Nations Secretary General's Special Advocate for Inclusive Finance for Development

Please share this Focus Note with your colleagues or request extra copies of this paper or others in this series.

CGAP welcomes your comments on this paper.

All CGAP publications are available on the CGAP Web site at www.cgap.org.

CGAP
1818 H Street, NW
MSN P3-300
Washington, DC
20433 USA

Tel: 202-473-9594
Fax: 202-522-3744

Email:
cgap@worldbank.org
© CGAP, 2014

The authors of this Focus Note are Timothy Lyman and Wameek Noor of CGAP. The authors would like to thank Louis de Koker, CGAP policy advisory consultant and professor of Law, Deakin University, Australia, and Emiko Todoroki, senior financial sector specialist, the World Bank, who served as advisers to this project and shared their valuable expertise and insights. The authors would also like to thank the Secretariat of FATF, in particular

Valerie Schilling, Aniko Hrubí, Anne-Francoise Lefevre, as well as Jean Pesme and Emily Reinhart of the World Bank's Financial Market Integrity Unit, for providing constructive comments and technical input. The authors also received valuable input from Kate Lauer and Olga Tomilova of CGAP. Michael Tarazi of CGAP provided guidance in conceptualizing and setting the context for this Focus Note.

The suggested citation for this Focus Note is as follows:
Lyman, Timothy, and Wameek Noor. 2014. "AML/CFT and Financial Inclusion: New Opportunities Emerge from Recent FATF Action." Focus Note 98. Washington, D.C.: CGAP, August.

Print: ISBN 978-1-62696-056-5
pdf: ISBN 978-1-62696-057-2

epub: ISBN 978-1-62696-058-9
mobi: ISBN 978-1-62696-059-6



MetLife Foundation
Ensuring Access. Empowering Communities.