Proportional risk-based AML/CFT regimes for mobile money

A framework for assessing risk factors and mitigation measures

SIMONE DI CASTRI AND JEREMIAH GROSSMAN, GSMA
RAADHIKA SIHIN, CONSULTANT
AUGUST 2015

Mobile Money for the Unbanked

The GSMA's Mobile Money for the Unbanked (MMU) programme works to accelerate the growth of commercially viable mobile money services to achieve greater financial inclusion.

For more information visit www.gsma.com/mmu

THE MMU PROGRAMME IS SUPPORTED BY THE BILL & MELINDA GATES FOUNDATION, THE MASTERCARD FOUNDATION, AND OMIDYAR NETWORK

The MasterCard Foundation

OMIDYAR NETWORK™

CONTENTS

Author biographies

This publication was written by Simone di Castri, Jeremiah Grossman, and Raadhika Sihin.

Simone di Castri is the Advocacy and Regulatory Director for the Mobile Money programme at the GSMA. He combines his legal and academic background with experience working with policy makers, regulators, financial institutions and mobile network operators in over 40 emerging markets, and supporting the development of policy and business ecosystems to increase financial inclusion, stability, integrity, and consumer protection. In his role, Simone leads a team of experts that supports mobile network operators, global standard-setters, policy makers, and regulators in addressing policy and regulatory barriers that prevent mobile financial services providers from scaling and serving low-income customers, and expanding the reach of the formal financial sector through mobile technology so millions of people can benefit from the digital opportunity and use convenient and safe financial services. He has represented the GSMA in several Financial Action Task Force (FATF) consultations, contributing to the development of the Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, and the Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services. Simone also works with the industry to improve risk mitigation and compliance policies, and oversees the implementation of the Code of Conduct for Mobile Money Providers. Before joining the GSMA, Simone worked at the Alliance for Financial Inclusion (AFI), where he helped financial sector policy makers and regulators from 40+ countries to design and implement new policies to create inclusive financial sectors. At AFI, he developed and managed the grant portfolio for Latin America and Francophone Africa, and conceived and coordinated the working group on financial consumer empowerment and market conduct regulations. Simone has also worked as Policy Analyst at the World Bank (CGAP) and as Junior Project Manager and Research Coordinator at the International Development Law Organization (IDLO). He was recently appointed member of the advisory board of the Fletcher School Leadership Program for Financial Inclusion at Tufts University and the Center for Financial Inclusion at Accion International. He is a lawyer and holds a PhD in Law and Economics from the University of Bologna.

Jeremiah Grossman is a Senior Advocacy and Regulatory Specialist for the Mobile Money programme at the GSMA. A lawyer with a Master's degree in international relations, Jerry works to promote the development of safe and enabling legal and regulatory frameworks that foster the growth of digital financial service ecosystems while protecting customers. Currently, Jerry is helping mobile network operators strengthen the foundations of their mobile money business and build partnerships to create digital ecosystems through implementation of the Code of Conduct for Mobile Money Providers. Before joining GSMA, Jerry advised central banks and international stakeholders on various legal and policy issues related to access to finance. Some examples of Jerry's prior assignments include working closely with central bank staff to develop agent banking, branchless banking, and e-money regulations in Namibia, Ethiopia, and Yemen; identifying promising global examples of digital financial services for smallholder farmers; co-authoring a digital finance handbook for USAID staff; supporting efforts to strengthen microfinance regulation and supervision in the Middle East and North Africa; and analysing regulatory frameworks for branchless banking and access to finance in Angola, Kyrgyz Republic, Lesotho, Malawi, Mozambique, Tajikistan, Tanzania, South Africa, Uganda, and Zambia.

Raadhika Sihin has a background in regulation and policy, having worked for 10 years in the South African Reserve Bank and the National Treasury of South Africa. She has broad financial sector experience with a particular focus on AML/CFT, payment systems, and financial inclusion. She represented the South African Treasury at FATF and the Eastern and Southern Africa 'Anti-Money' Laundering Group (ESAAMLG), and was the financial sector expert for India's Mutual Evaluation. She is currently serving as Vice President of Public Policy, Africa for MasterCard. In the past, she has worked as a consultant and was the Senior Policy Specialist at the Alliance for Financial Inclusion (AFI), where she led the G20 Global Partnership for Financial Inclusion (GPFI) engagement with standard-setting bodies such as the FATF. Raadhika also coordinated AFI's working group on financial integrity and contributed to the revision of the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation and to the elaboration of the FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion. She has also worked closely with ESAAMLG and AFI on their AML/CFT and financial inclusion project in Africa. She is an economist by training.

ACKNOWLEDGEMENTS:

The authors are very grateful to the peer reviewers of this work: Mercy Buku (consultant, formerly with Safaricom), Martin Crossley (Orange), Louis de Koker (Deakin University), Victor Dostov (Russian Electronic Money Association), Timothy Goodrick (KPMG, formerly with the Financial Action Task Force - FATF), Emery Kobor (United States Department of the Treasury), Jose Lapadula (Millicom), Wameek Nour (CGAP/World Bank), Sacha Polverini and Daniel Radcliffe (Bill & Melinda Gates Foundation), and to Yasmin Kamara (GSMA) for research assistance.

DISCLAIMER:

This document includes the authors' interpretation of how the Financial Action Task Force (FATF) Recommendations apply to providers of mobile money services and has not been endorsed by FATF.

Executive Summary

Mobile money services for the unbanked are expanding across developing and emerging markets. In 89 emerging markets, 261 deployments serve 103 million active mobile money customers, who perform 717.2 million transfers and payments per month worth USD 16.3 billion. These figures highlight how pervasive mobile money has become and the potential it has to contribute to more efficient and inclusive financial systems.

Mobile money services rely on widespread availability of mobile phones and networks of agents to provide cash-in and cash-out services. With these in place, mobile money services can cost-effectively address two of the major challenges of financial inclusion: convenience and affordability. Convenient and affordable access to financial services is allowing millions of unbanked and underserved people around the world to adopt low-value transfer and payment services.

This growth in financial inclusion has not introduced significant risk or compromised the integrity of the financial sector. Empirical evidence and country research by the World Bank[1] suggest that criminal abuse of mobile money has, so far, been limited.[2] While these initial results are encouraging, it is critical to monitor new technologies and payment instruments as adoption scales, in order to understand vulnerabilities and adopt up-to-date, appropriately designed anti-money laundering and combating the financing of terrorism (AML/CFT) controls so that mobile money services remain safe and secure. The aim is to have AML/CFT controls that are effective and proportional to the specific risks of these services: neither unduly burdensome nor insufficiently rigorous.

In February 2012, the Financial Action Task Force (FATF) revised its international standards on combating money laundering and the financing of terrorism and proliferation.[3] Known as the FATF Recommendations, these AML/CFT standards set the global framework for customer due diligence (CDD) and know your customer (KYC) requirements for financial institutions, including mobile money providers. Following the release of the new standards, the FATF published a set of guidance documents to help regulators, assessors, and service providers implement the Recommendations and monitor and evaluate how they are being applied using a mechanism called 'mutual evaluation'.

> *"FATF Ministers stated that financial exclusion represents a real risk to achieving effective implementation of the AML/CFT Recommendations. This formally recognizes that for FATF, financial inclusion and AML/CFT pursue mutually supportive and complementary objectives: the application of measures which enable more citizens to use formal financial services will increase the reach and the effectiveness of AML/CFT regimes."*
>
> Bjørn S. Aamo,
> Former FATF President (2012-2013)[4]

1. Pierre-Laurent Chatain, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker (2011), "Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions", The World Bank Group, Washington, D.C.
2. Recent evidence from Afghanistan suggests that some criminals have used a variety of new payment instruments and services to facilitate drug trafficking, including internet payments, mobile payments, and prepaid cards. See FATF (2014), "Financial Flows Linked to the Production and Trafficking of Afghan Opiates", FATF, Paris.
3. FATF (2012), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation".
4. Bjørn Aamo, presentation to the Global Partnership for Financial Inclusion Conference on Standard-Setting Bodies and Financial Inclusion, "Promoting Financial Inclusion through Proportionate Standards and Guidance", Basel, Switzerland, 29 October 2012.

The 2012 FATF Recommendations, guidance documents, and the FATF mandate itself constitute official recognition that financial exclusion is a money laundering and terrorist financing (ML/TF) risk, and that reducing financial exclusion is vital to achieving an effective AML/CFT system. Being able to trace transactions and money flows with account-based mobile money services (as opposed to over-the-counter services) directly addresses this risk and makes AML/CFT systems more effective at both the country and global level.

The most important change in the 2012 Recommendations is that a risk-based approach to AML/CFT is now central to implementing all of the FATF standards. The FATF requires countries to base many key elements of their AML/CFT regime design on an assessment of the specific AML/CFT risks they face with different industries, products, delivery channels, and relevant domestic conditions. The FATF allows exemptions from AML/CFT obligations in proven low-risk cases and the use of simplified CDD measures in lower risk cases — two possibilities based on the risk assessment. The FATF has repeatedly emphasised that applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the financial system. Ineffective regulation or controls may enable money launderers and terrorist financiers to abuse mobile money services, but AML/CFT controls should not inhibit access to formal financial services for low-income, rural, undocumented, or other financially excluded and underserved groups.[5]

The purpose of this paper is to:

a. **Help regulators** understand the risks posed by mobile money services and the measures mobile money service providers are taking to mitigate these risks, both of which can help inform the design of efficient and proportional AML/CFT regulations; and

b. **Help assessors** understand mobile money services and the risks and risk mitigation measures to inform the mutual evaluation process.

The paper draws on the results of a GSMA survey of 37 mobile money providers conducted between March and May 2015 (Section 5.1). The survey revealed several emerging KYC/CDD practices:

- Providers screen staff, agents, master agents, and customers before establishing a business relationship.
- Providers train staff, agents, and master agents to ensure they understand and are prepared to carry out their AML/CFT obligations.
- Providers are developing electronic systems to identify suspicious transactions and activity by customers, staff, agents, and master agents.
- Providers mitigate risks by imposing limits on the value and frequency of transactions, along with other limits on account functionality.
- A tiered approach to KYC is popular because it allows regulators to distinguish between lower risk and higher risk scenarios, thereby permitting KYC procedures to be conducted in line with the specific risks posed by different types of customers and transactions.

This paper examines various aspects of the FATF Recommendations and guidance documents to illustrate, in practical terms, what elements should be incorporated in a risk-based assessment (RBA) of mobile money products and how a proportional AML/CFT framework has been implemented in national regulations. The analysis focuses particularly on the measures mobile money providers have put in place to identify and verify the identities of their customers, monitor and track transactions, and manage suspicious transactions. It then identifies AML/CFT regulations and KYC/CDD practices that have been effective, efficient, and not too onerous

5. FATF (2013a), "Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion."

for providers and regulators to apply. Correct application of the FATF framework will allow regulators to design proportional and risk-based regulation, which is critical to enabling the development of safe and sustainable mobile money services, protecting the integrity of the financial system, and providing millions of people with access to convenient financial services.[6]

> *Governments are increasingly challenged to support the growth of these new services while mitigating the potential risks (including fraud, money laundering, and financing terrorism). Concerns have been raised about potential integrity issues that may stem from the use of mobile money. We believe these concerns deserve our careful attention—first, because we cannot afford to put this vulnerable group of people at risk; and, second, because trust in those services is key to their development. At the same time, it is important not to overestimate these risks, particularly when the alternative is financial exclusion. […] Policy makers need to do more and to be more creative, flexible, and agile while keeping in mind that pushing access to financial services should not come at the cost of financial stability and integrity. Bad and overly restrictive regulation is a major obstacle to the expansion of mobile money services to the poor. We need (1) good regulation for nonbank financial services, such as electronic money or payment system regulation; (2) smart and flexible oversight of retailers as agents for mobile money services; and (3) proportionate, risk-based anti-money laundering and combating the financing of terrorism (AML/CFT) rules.*
>
> Janamitra Devan,
> former Vice President and Head of Network, World Bank (2013-2014)[7]

6. The authors advise all readers to read the FATF documents because the discussion in this paper is generic and may not sufficiently highlight all the risks inherent in every mobile money system. The paper highlights how some operators in some countries have addressed the risks, but the authors do not endorse any example as necessarily FATF-compliant.
7. Janamitra Devan, former Vice President and Head of Network, World Bank, preface to Pierre-Laurent Chatain, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker (2011), "Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions", The World Bank Group, Washington, DC.

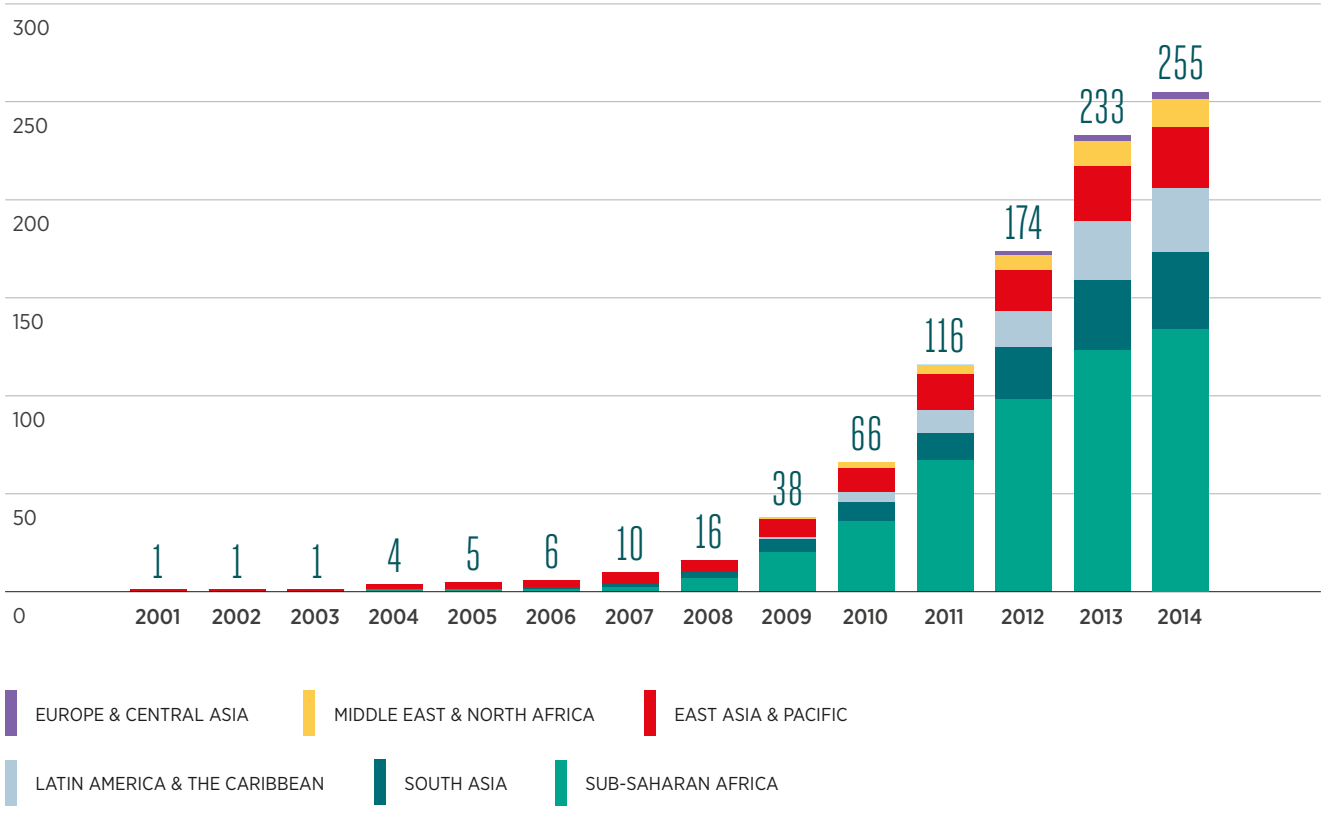
Introduction

Mobile money holds great promise for extending access to financial services to the world's 2.7 billion unbanked.[8] By improving the efficiency, convenience, and safety of payment systems, mobile money is bringing low-income households and underserved communities into the formal financial system, helping to reduce vulnerability while fostering economic growth.

Mobile money services for the unbanked are expanding across developing and emerging markets. As of December 2014, 255 deployments[9] in 89 emerging markets (see Figure 1) are serving 103 million active[10] mobile money customers, who are performing 717.2 million transfers and payments per month worth USD 16.3 billion.[11] These figures highlight how pervasive mobile money has become and its potential to contribute to more efficient and inclusive financial systems.

FIGURE 1

NUMBER OF LIVE MOBILE MONEY SERVICES BY REGION
(2001-2014; YEAR-END)



8. Unless otherwise specified, the definitions used in this document are those included in the FATF 2012 Recommendations.
9. See Figure 1. Source: GSMA, Mobile Money for the Unbanked (MMU) Deployment Tracker. Data retrieved on 1 April 2015.
10. On a 90-day basis. Total number of registered mobile money accounts worldwide was 299 million as of December 2014.
11. Transaction values for global mobile money usage in the month of December, 2014. 33.3 million unregistered customers were transacting over the counter as of June 2014. See GSMA Mobile Money for the Unbanked (2015), "State of the Industry 2014: Mobile Financial Services for the Unbanked".

Like any financial service, however, mobile money poses potential risks, including the risk of being used to support criminal activity.

The Financial Action Task Force (FATF)[12] is the main global Standard-Setting Body (SSB) for financial integrity and has a mandate to ensure the risks of money laundering (ML) and terrorist financing (TF) are addressed effectively by country regulators and financial services providers. The FATF contends that financial exclusion poses a risk to the effectiveness of an AML/CFT regime because "informal, unregulated and undocumented financial services and a pervasive cash economy can generate significant money laundering and terrorist financing risks and negatively affect AML/CFT preventive, detection and investigation/prosecution efforts."[13] Given this, the FATF has stated that financial inclusion and integrity are mutually reinforcing and complementary objectives.[14]

> *"Enlarging access to financial services for the most vulnerable parts of the population, through regulated and supervised channels, is indeed a core element to strengthen financial integrity. AML/CFT measures need to cover the largest range of transactions in order to efficiently protect the integrity of the global financial system."*
>
> Vladimir Nechaev,
> Former FATF President (2013-2014)[15]

Mobile money serves the dual objectives of financial integrity and financial inclusion in a variety of ways. By digitising financial transactions, mobile money (1) reduces the dependency of households, businesses, and governments on cash and informal financial services; (2) increases safety and convenience for customers; and (3) accelerates and expands universal access to a broad range of formal financial services, including savings, credit, insurance, and pensions. At the same time, digitising financial transactions improves record keeping and introduces functionalities to track transactions and localise customers, making it easier for law enforcement to monitor and trace illicit funds.

One of the biggest challenges to enabling the growth of mobile money and the digital finance ecosystem is designing cost-effective CDD procedures that enable universal access to mobile money services while preserving the integrity of the financial system. For the regulator, this means designing AML/CFT requirements that mitigate the risk of abuse of mobile money while still allowing customers to access and use these services safely and easily. Many low-income customers face barriers to financial services because they are unable to prove their identity through traditional means; they may live in a country that does not provide national identification documents (IDs), or they may be deprived of services where the costs of conducting CDD are too high, such as in remote areas where electricity is not available. Proportional controls are key to mitigating the risk of criminal activity on the mobile money platform while balancing the dual objectives of financial integrity and financial inclusion (see Figures 2 and 3).

12. The FATF is an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. FATF is comprised of 34 member countries, most of which are developed countries.
13. FATF (2011), "Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion", p. 15.
14. OECD, "Financial Inclusion and Financial Integrity: Complementary Policy Objectives."
15. Vladimir Nechaev, Address to the G8 Sub-Saharan Africa Public-Private Sector Dialogue on AML/CFT, Swakopmund, Namibia, 6 September 2013.

FIGURE 2

UNINTENDED NEGATIVE CONSEQUENCES OF NON-PROPORTIONAL AML/CFT REGIMES[16]

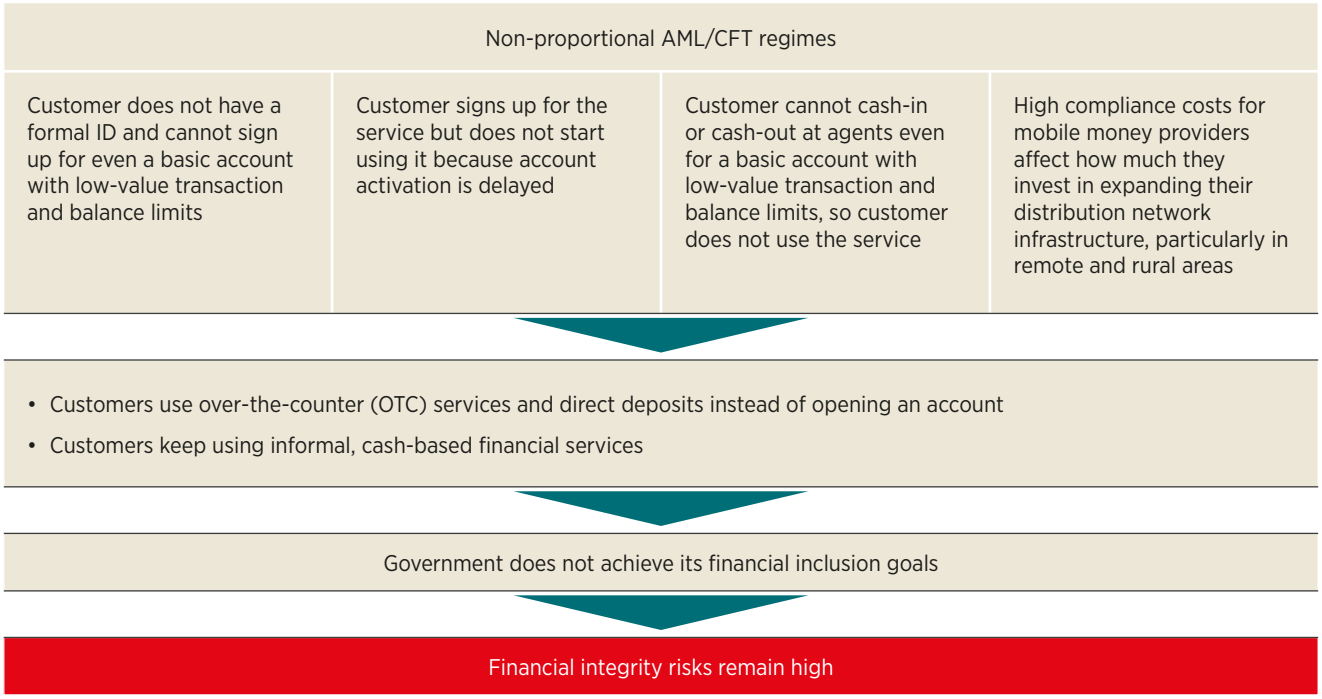
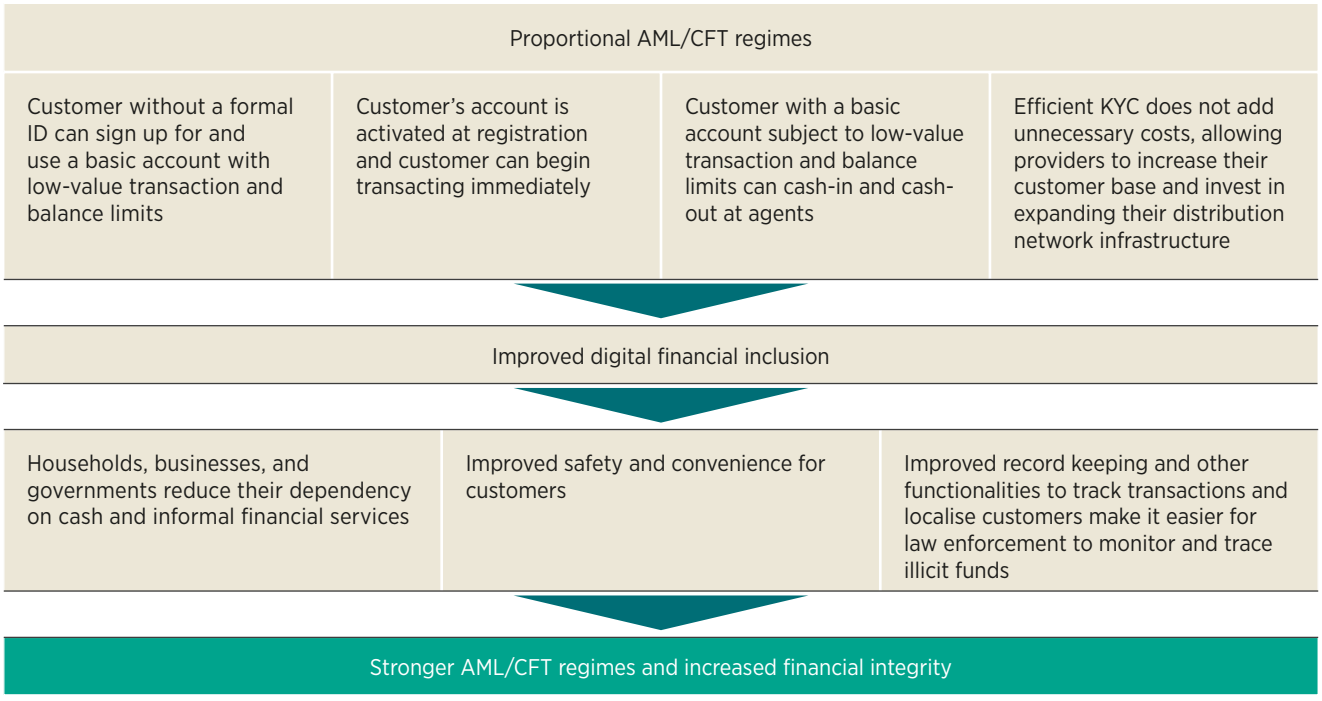


FIGURE 3

POSITIVE CONSEQUENCES OF PROPORTIONAL AML/CFT REGIMES



16. Based upon their collective experience, the authors believe the examples in Figures 2 and 3 are applicable to the vast majority of jurisdictions. The authors recognise that risks vary significantly across countries and that policymakers must consider the specific country context when developing proportional AML/CFT regimes.

An important part of this process is understanding consumer behaviour and perceptions in the intended market. For example, instantaneous account registration has a positive effect on customer activity; if customers have to wait to use the service after they register (while their identity documents are verified at the provider's headquarters), some will simply never start using it.[17]

In the most recent revision of the *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (hereinafter "FATF Recommendations"), the FATF articulates a framework that aims to detect and report transactions involving proceeds from crime or terrorist financing by designing requirements and controls proportionate to the risk of financial system abuse. This framework is very helpful for regulators looking to establish effective AML/CFT requirements that balance the objectives of financial integrity and inclusion.

The FATF requires countries seeking to meet the standards to adopt a risk-based approach, which involves (1) gathering information related to the country context, crime risk, customer groups, types of services used, customer access channels, and relation to sanctioned names; and then (2) analysing the information based upon an evaluation of the expected activity, specific risk factors, and mitigation measures. Based upon the assessment and classification of the service as *"proven low risk"*, *"lower risk"*, or *"higher risk"*, regulators can design proportional requirements and controls.

Adopting a risk-based approach means targeting resources commensurate with the level of risk of a specific service. For a regulator, this involves identifying, measuring, and evaluating different ML/TF risk factors; developing risk mitigation requirements proportionate to the risks of that specific service; imposing enhanced mitigation measures for higher-risk services; and allowing simplified measures for lower-risk customers.

For policymakers committed to promoting financial inclusion while ensuring financial integrity, a robust consultation process is essential. Only if policymakers and regulators clearly understand the key characteristics of mobile money services — including both their inherent vulnerabilities and measures mobile money providers can take to address these vulnerabilities — can they effectively assess the likely impact of proposed AML/CFT requirements on the development of mobile money services.

Outline

The purpose of this paper is to:

a. **Help regulators** understand the risks posed by mobile money services and the measures mobile money service providers have adopted to mitigate these risks, both of which can inform their efforts to design efficient and proportional AML/CFT regulations; and

b. **Help assessors** understand mobile money services and the risks and risk mitigation measures that will inform the mutual evaluation process.

The paper is organised into the following sections:

- **Section 1** defines mobile money (which is often confused with mobile banking) in the context of the AML/CFT requirements. This section discusses why a proportional approach is critical to the sustainability and viability of mobile money services, not just from a compliance point of view, but also in terms of effective customer adoption.

- **Section 2** proposes two methodological frameworks for managing the workflow of a risk-based assessment (RBA): one for regulators and one for providers. The frameworks consider the specific needs of each, as well as the outcomes the RBA must generate.

17. See Section 1.2

- **Section 3** discusses the risk of abuse of mobile money services in the absence of effective risk mitigation measures. Section 3.1 addresses the inherent vulnerabilities of mobile money products, while Section 3.2 analyses how different stakeholders may exploit these vulnerabilities.

- **Section 4** looks at international regulatory measures aimed at ensuring mobile money risks are mitigated effectively. A review of the FATF, the intergovernmental body responsible for setting AML/CFT standards and reviewing country compliance, leads into a discussion of the Recommendations most relevant to mobile money services and the application of the risk-based approach, which is a central part of the new AML/CFT architecture.

- **Section 5** describes how mobile money providers can implement appropriate risk controls to ensure financial integrity. Section 5.1 discusses the results of a global survey of 37 representatives of mobile network operators (MNOs). The results reveal emerging practices in AML/CFT compliance, the risk measures MNOs have put in place, and the challenges that remain in this nascent industry. Section 5.2 identifies the ML and TF risks of mobile money, both before and after risk controls have been implemented. This is followed by the **Conclusion** and several **Annexes**:

- **Annex 1** includes excerpts of the relevant FATF Recommendations discussed in Section 4.

- **Annex 2** provides the full results of the survey discussed in Section 5.

- **Annex 3** presents six case studies from emerging and developing markets that describe how the dual objectives of financial inclusion and integrity are being pursued by expanding access to digital financial services and developing proportional and risk-based CDD. These case studies demonstrate that success can be achieved through a combination of public and private sector collaboration, regulators who are open to innovation, and an understanding that financial inclusion and integrity are mutually reinforcing objectives. Annex 3 also includes a description of the European Union's approach to simplified customer due diligence.

1. Understanding mobile money: The importance of proportional AML/CFT

1.1 What is mobile money?

"Mobile money" refers to monetary value that is:

- available to a user to conduct transactions through a mobile device;
- accepted as a means of payment by parties other than the issuer;
- issued on receipt of funds in an amount equal to the available monetary value;
- electronically recorded; and
- redeemable for cash.

In jurisdictions where "electronic money" (or "e-money") has been defined in regulation or legislation, mobile money is a form of e-money. This definition of mobile money includes services commonly referred to as "mobile payments" or "mobile transfers": value that (1) is transferred from a mobile wallet and/or (2) accrues to a mobile wallet and/or (3) is sent using a mobile phone. Mobile payments can include non-commercial transfers between individuals, as well as transfers to pay for goods or services either at the point of sale (e.g. retail store) or remotely (e.g. bill payments). A mobile wallet is an account accessed primarily via a mobile phone.

"Mobile money" is not the same as "mobile banking" services, which mainly provide customers access to their bank accounts via a mobile phone.

A mobile money platform offers customers greater convenience and safety compared to traditional informal and cash-based alternatives. Customers can typically access the following services through mobile money (see Figure 4):

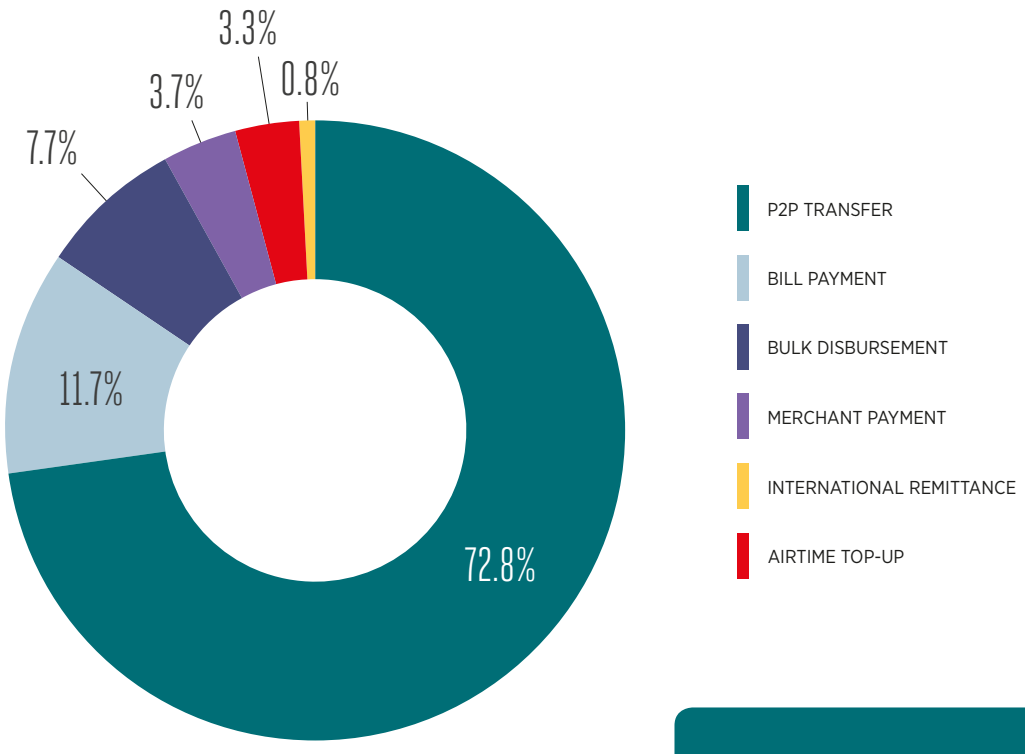
- P2P transfer: funds remitted from one person to another, where both parties are in the same country (also called domestic money transfer)
- Funds storage: the account is used as a way to store funds securely

- Merchant payments: payments to participating retailers, such as grocery stores or suppliers of household goods
- Bill payments: payments for services from utility companies, (e.g. electricity and water), other private sector companies (e.g. television, internet, insurance), or government entities (e.g. tax payments)
- Bulk disbursements: government payments (e.g. salaries or benefits) or private sector payments (e.g. salaries or goods and services)
- Airtime top-up: mobile subscribers can reload prepaid mobile credits

In some countries, mobile money customers can also transfer money to and from their bank accounts and vice versa, withdraw funds from ATMs, and/or send or receive funds internationally.

FIGURE 4

GLOBAL PRODUCT MIX OF MOBILE MONEY SERVICES BY VALUE
(AS OF DECEMBER 2014)[18]



THE AVERAGE VALUE OF A MOBILE MONEY PEER-TO-PEER (P2P) TRANSFER IS USD 45

18. GSMA (2015), cit.

1.2 Why is proportional AML/CFT regulation critical to mobile money?

To develop sustainable mobile money markets and allow the digital finance ecosystem to flourish, MNOs must be able to mitigate risk cost-effectively, maintain the integrity of the financial system, and offer inclusive services. Proportional AML/CFT requirements are critical to achieving these complementary objectives.

The CDD procedures developed by the provider to comply with KYC requirements can create obstacles to customers wishing to open an account, particularly if it is difficult for them to prove their identity (due to lack of acceptable ID) or provide other required information (e.g. proof of address). For providers, the main challenge in establishing KYC procedures for their networks of agents is ensuring CDD is not so onerous that it affects the sustainability of the business. Mobile money customers generate high volumes of low-value transactions — the average peer-to-peer (P2P) transfer is USD 45 — so compliance costs for agents and providers must be reasonable for mobile money services to be viable. In addition, CDD requirements for low-value accounts should be simple enough for agents to perform CDD on behalf of providers.

One basic proposition of an enabling regulation is that providers can use a network of agents to (1) register customers, (2) verify identity, (3) activate accounts, and (4) provide cash-in and cash-out services. The next section will analyse the most critical issues for mobile money services.

CUSTOMER REGISTRATION

To sign up for a mobile money account, a new customer typically visits a mobile money agent and provides proof of identity. However, in some countries, many potential users of the services cannot meet the identity requirements because they lack utility bills, a government-issued ID card (many countries do not have a universal national ID system), another type of acceptable photo ID (the poorest often do not have jobs that issue employee photo IDs or do not attend a school where student ID is required), or even birth records (many poor people are born at home rather than in a hospital). Customers who lack one of these IDs cannot sign up for the service unless the KYC regulation allows the service provider to accept an alternative form of identification. A 2014 global survey of both bank and non-bank providers of mobile financial services identified "onerous customer identification requirements" as one of the main barriers for the industry.[19] These findings corroborate the results of a 2013 World Bank study that found simplified KYC regimes for low-value accounts and lower-risk customers were associated with greater adoption of mobile money services,[20] as well as the results of a 2015 research paper published by the University of Chicago that identified "burdensome KYC" as a key barrier to the uptake of mobile money.[21]

Many developing countries do not have a national identification system and use other traditional methods of identifying residents. In some cases, regulators allow alternative accredited forms of ID, ranging from a voter's card or student card to a letter from a village chief or other community leader. The FATF Financial Inclusion Guidance cites several examples of acceptable IDs,[22] but cautions countries to be mindful of fraud and abusive practices. Alternative forms of identification are often only accepted for certain types of transactions and have defined thresholds and limits.

For those unable to prove their identity to open an account, a number of alternatives may be available. Depending on the country, they could be (1) left out of the formal financial system; (2) allowed to open an account with very low transaction and balance limits without verification of identity; (3) allowed to make transactions over-the-counter (OTC)[23] rather than through an account; or (4) allowed to make a direct

19. Ibid.
20. Eva Gutierrez and Sandeep Singh (2013), "What Regulatory Frameworks are More Conducive to Mobile Banking? Empirical Evidence from Findex Data", The World Bank, Washington, DC.
21. David S. Evans and Alexis Pirchio (2015), "An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most", Coase-Sandor Institute for Law and Economics, The University of Chicago Law School, Chicago.
22. FATF (2013a), 32-33.
23. An OTC transaction is similar to a wire transfer. A customer simply hands over cash to an agent who facilitates the transaction using her/his own mobile money account on the customer's behalf. OTC can be offered formally, whereby the provider deliberately chooses to implement an OTC strategy for commercial and regulatory considerations—as was the case of Easypaisa in Pakistan and of Tigo Money in Paraguay during their early years of operation, prior to introducing hybrid services. OTC can also emerge informally and organically, despite deliberate commercial and regulatory attempts to limit OTC. For example, bKash in Bangladesh (where the regulator prohibits OTC) is currently struggling with informal OTC. OTC preference matters because users of OTC services have no accounts that can be used to store funds and serve as a vehicle for the delivery of savings, insurance, or other financial products. As a result, high adoption of OTC services limits progress toward full financial inclusion. See Daniel Radcliffe, "Why aren't Pakistan's mobile money customers opening accounts?," GSMA Mobile Money for the Unbanked (MMU) blog, 4 April 2013; and Greg Chen, "Mobile Wallets: Is a Transition Underway in Bangladesh?", CGAP blog, 28 October 2013.

deposit.[24] OTC and direct deposits pose a risk to financial integrity because these transactions may occur without verification of customer identity, and a customer who does not open a mobile money account does not establish a stable "business relationship" with the provider that can be monitored over time.

VERIFICATION OF CUSTOMER IDENTITY

Some countries have established onerous procedures for recording and verifying customer identity, such as requiring agents to create digital copies of photos and application forms. In Pakistan, for example, the KYC requirements for account opening require agents to take a photo of the applicant and the ID card and send this information to bank officials, who then verify it against a database. To meet this requirement, mobile money providers must equip each agent with a ~$150 camera-enabled phone — a costly undertaking when multiplied by tens of thousands of mobile money agents. In addition, many agents lack the technological capability to reliably digitise these documents and network connectivity may be unreliable. For these reasons, only a small fraction of mobile money agents in Pakistan are equipped to register accounts. In contrast, OTC transactions only require the customer to present an ID card and hand the money to an agent. As a result, 87% of mobile money transactions in Pakistan are conducted OTC rather than through an account.[25]

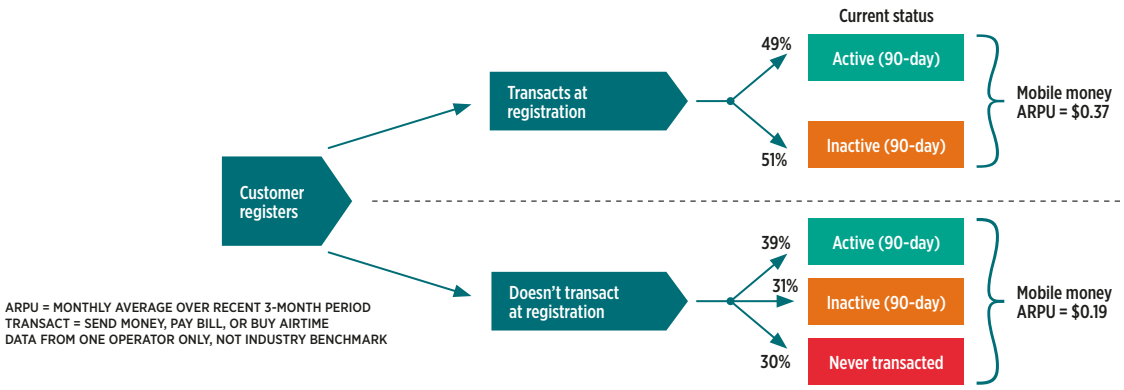
CUSTOMER ACTIVATION

To encourage active usage of mobile money accounts, prospective mobile money customers should be able to register at an agent in their community or place of work and conduct transactions immediately after registration. Any delay between signing up a new customer and activating the mobile money account has a negative impact on customer activation and, therefore, on financial inclusion.[26] GSMA research reveals a stark difference in future activity between customers who transact at the point of registration and those who do not. Customers who transact at the point of registration are more likely to be future active customers (26% more likely) and produce significantly higher mobile money average revenue per user (ARPU) (95% higher) than those who walk away after registering without transacting (see Figure 5). A CGAP analysis also found that customers who perform two or fewer transactions in the first month only have a 4% chance of being active users in the third month.[27]

Customers who are able to sign up and transact immediately can receive help from the sales agent to conduct their first transaction. This is also important because agents generate revenue right away: one commission for registering a new customer and one for the transaction. This provides an incentive for agents not only to register new customers, but also to help them become active users of the service.

FIGURE 5

THE IMPORTANCE OF GETTING CUSTOMERS ACTIVE AT REGISTRATION[28]



ARPU numbers are net of agent commissions.

24. Direct deposits are a sub-set of informal OTC. A direct deposit occurs when the customer initiating a P2P transfer hands the agent cash, but provides them with the mobile number of the recipient rather than their own. The agent deposits the funds directly into the recipient's account, circumventing the intended flow of a P2P transfer. Customers may prefer direct deposits because they are cheaper (the sender avoids the P2P transfer fee), easier, and/or the only option if they are unable to open an account. See Philip Levin, "MMU Spotlight on 'direct deposits:' An expensive nuisance for mobile money operators," GSMA Mobile Money for the Unbanked (MMU) blog, 15 April 2013; Mireya Almazán, "OTC & Mobile Money: Making Sense of the Data," GSMA Mobile Money for the Unbanked (MMU) blog, 22 January 2015.
25. Daniel Radcliffe, "Why Aren't Pakistan's Mobile Money Customers Opening Accounts?" GSMA Mobile Money for the Unbanked (MMU) blog, 4 April 2013.
26. Yasmina McCarty, "Barriers to customer activation: A case study from MTN Uganda," GSMA Mobile Money for the Unbanked (MMU) blog.
27. Claudia McKay, Toru Mino, and Paola de Baldomero Zazo (2012), "The challenge of inactive customers," CGAP presentation.
28. Philip Levin (2013), "The big payoff: Getting customers active at registration," GSMA Mobile Money for the Unbanked (MMU) blog.

2. Risk-based assessment of mobile money services: A methodology to manage the workflow

"The overall degree of risk of a particular NPPS (new payment product or service) is, in a given context, the cumulative effect of combining each of the risk factors. In addition, procedures to mitigate risk should be proportionate to the level of risk posed by the product or service. Adopting proportionality criteria allows the risks posed by a particular NPPS to be addressed, while maintaining the functionality which is aimed at customer convenience and ease of use."

FATF Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services

2.1 A methodological framework for implementing the FATF risk-based approach

Regulators must create a proper enabling framework for digital financial services to flourish and contribute to both financial inclusion and integrity. The FATF (see Section 4), the Bank for International Settlements (BIS) (see Box 1), and the World Bank[29] have provided guidance on establishing an enabling regulatory environment: regulation should be sound, clear, non-discriminatory,[30] and proportional. By doing so, regulators can create an "open and level playing field that fosters competition and innovation, leverages the value proposition of both banks and non-bank providers, attracts investments, and allows providers to focus on refining operations and promoting customer adoption."[31]

Providers must establish compliance procedures that follow the regulator's guidance, safeguard customer funds and the integrity and stability of the financial sector, and are cost-effective, thereby allowing the business to scale sustainably.

29. World Bank (2012), "From Remittances to M-Payments: Understanding 'Alternative' Means of Payment within the Common Framework of Retail Payments System Regulation", Section III.4.3.
30. Requirements should be established for the type of service offered rather than the type of service provider.
31. Simone di Castri (2013), "Mobile Money: Enabling Regulatory Solutions", GSMA, 4

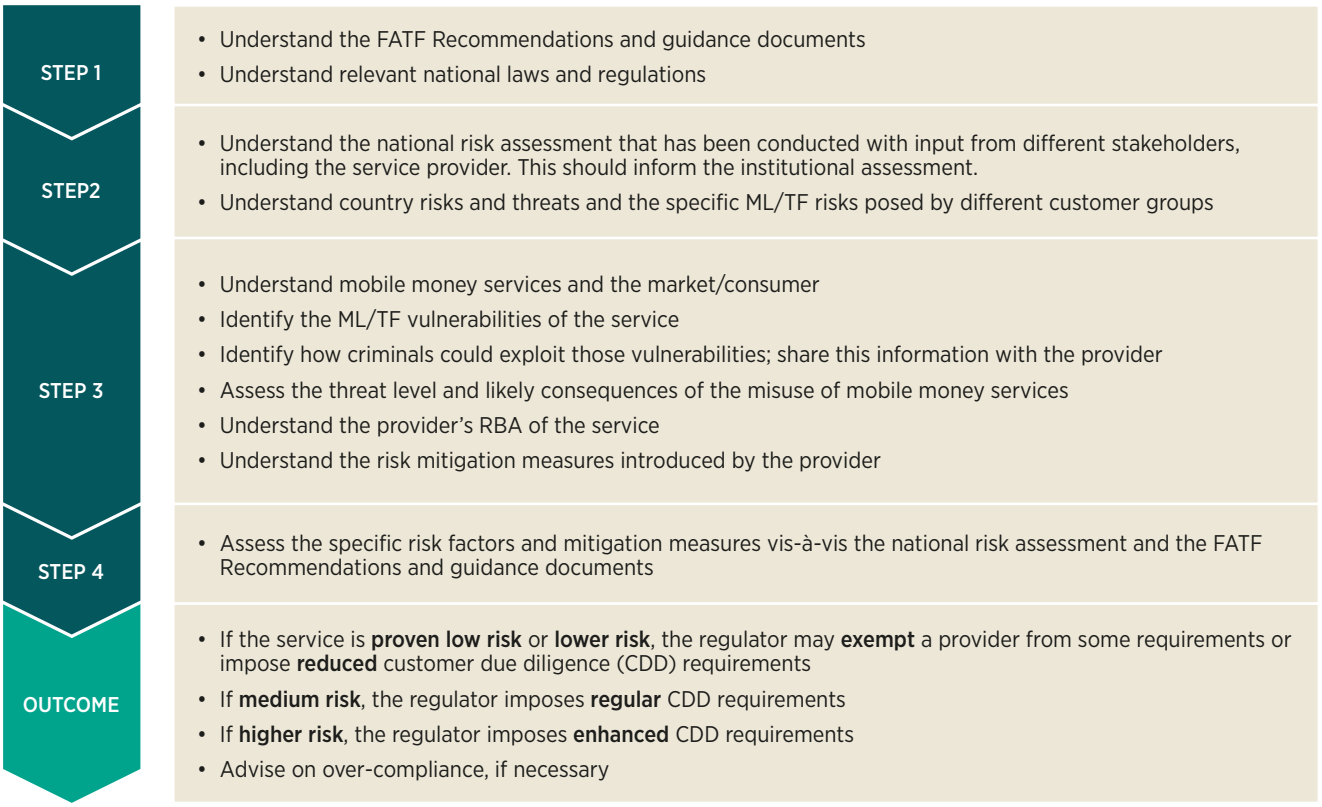
BOX 1
RELEVANT BIS PAYMENT SYSTEMS GUIDANCE

The benefits of a regulatory approach that places greater emphasis on the type of service than the provider of the service have been highlighted in multiple BIS publications. For example, in 2007, the Committee on Payment and Settlement Systems (CPSS, now called the Committee on Payments and Market Infrastructures or CPMI) and the World Bank issued General Principles for International Remittance Services. According to the General Principles, regulating solely by type of entity may reduce the effectiveness of regulations and create market distortion; any regulatory intervention should be non-discriminatory and aim to create a level playing field between equivalent services offered by different providers.[32] In 2014, the CPMI published Non-banks in Retail Payments. This report cited the need to establish a level playing field for banks and non-banks in retail payments as a key challenge for central banks and other financial sector authorities.[33]

When designing an AML/CFT regulatory regime for mobile money, stakeholders must understand the unique characteristics of mobile money services, including the inherent strengths and vulnerabilities of mobile money and the measures required to mitigate AML/CFT risks. Only then can stakeholders conduct an effective risk-based assessment that shapes and informs both regulations and operations efficiently. The methodological frameworks proposed below streamline the workflow of a risk-based assessment (RBA) for both regulators (Figure 6) and providers (Figure 7). The framework for regulators assumes regulations will be developed (or revised to align with the new FATF Recommendations) in markets where the mobile money industry is already active and deployments have already launched services with AML/CFT controls in place.

FIGURE 6

RISK-BASED ASSESSMENT OF MOBILE MONEY SERVICES: THE WORKFLOW FOR REGULATORS



32. Bank for International Settlements – Committee on Payment and Settlement Systems & The World Bank (2007), "General Principles for International Remittance Services," paras. 64, 93.
33. Bank for International Settlements – Committee on Payments and Market Infrastructures (2014), "Nonbanks in Retail Payments," Section 6.1.

FIGURE 7

RISK-BASED ASSESSMENT OF MOBILE MONEY SERVICES: THE WORKFLOW FOR SERVICE PROVIDERS

STEP 1	• Understand the FATF Recommendations and guidance documents • Understand relevant national laws and regulations
STEP2	• Understand country risks and threats and the specific ML/TF risks posed by different customer groups • Understand the national risk assessment that has been conducted with input from different stakeholders, including the serviceprovider. This should inform the institutional assessment.
STEP 3	• Understand mobile money services • Identify the ML/TF vulnerabilities of the services • Identify how criminals could exploit those vulnerabilities and the likelihood of this exploitation
STEP 4	• Assess the specific risk factors and mitigation measures vis-à-visthe FATF Recommendations and guidance documents, relevant national laws and regulations, and additional guidance provided by the regulator
STEP 5	• Introduce appropriate policies to control risks and implement risk mitigation measures
STEP 6	• Monitor risks and review the effectiveness and efficiency of controls. This is an ongoing process

3. How could mobile money services be used for money laundering and terrorist financing?

It is important to take a holistic approach when assessing the risks associated with a particular NPPS. Rather than considering the risk factors listed in the matrix one-by-one, the risks, risk mitigants, and functionality of a particular NPPS should be considered together to determine whether the product poses a high or low ML/TF risk.

FATF Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services

In a World Bank publication, Pierre-Laurent Chatain *et al*[34] assess the financial integrity risks of mobile money by determining its vulnerability to abuse and the threat of abuse by prospective criminals ("vulnerability + threat = risk"). The authors define vulnerability, threat, and risk as follows:[35]

- **Vulnerability:** An endogenous weakness in a system or sector arising from inadequate control measures. The inherent characteristics of a sector or the environment in which it operates can also create certain vulnerabilities through its product and service offering.
- **Threat:** The likelihood that ML may be attempted. The level of the threat is influenced by the overall ML environment and attractiveness to criminal elements, which could include external factors at both the national and sector level.
- **Risk:** Residual exposure to threats of ML after vulnerability is taken into consideration. Thus, risk is a function of threat and vulnerability. Although risk may be inherent to any economic sector, the degree of ML/TF risk faced by different sectors may differ.

34. Pierre-Laurent Chatain, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker (2011), cit.

35. An alternative set of definitions has been developed in the FATF RBA Guidance (FATF, 2013b, cit.), which defines "risk" as a function of three factors (threat, vulnerability, and consequence) and states that a risk assessment should include judgements on all three. According to the FATF:
    - "A **threat** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities." Therefore, risk assessments require "having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume)".
    - "The concept of **vulnerabilities** as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threat means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes".
    - "**Consequence** refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector."

    Given the complexity of such a process and the challenges in estimating "consequences," the FATF acknowledges that countries may opt for a greater focus on obtaining a comprehensive understanding of threats and vulnerabilities. For the purposes of this paper, the authors will use the definitions in Chatain et al (2011).

Applying this framework to mobile money, the authors conclude that mobile money has low vulnerability to abuse and a low threat of abuse by prospective criminals:

> *"If this framework is applied to m-money, one can argue that vulnerability is low because there are no novel weaknesses in m-money platforms. Even where national regulatory and supervisory frameworks are absent, m-money providers have internal controls and mechanisms in place. The threat from m-money is also low because the likelihood that ML may be attempted by alternative channels, such as cash, is always likely to be greater than the likelihood that m-money will be used in the attempt. In fact . . . the total costs of ML or TF through m-money, relative to other channels, are likely still greater. Hence, because risk is a function of threat and vulnerability, the risk emerging from m-money should also be comparatively low."*

Nevertheless, mobile money services have certain inherent vulnerabilities that need to be addressed through effective risk mitigation. The following sections discuss the specific vulnerabilities of mobile money and how, in the absence of proper controls, these vulnerabilities could be exploited by criminals for the purposes of money laundering or terrorist financing.

3.1 How is mobile money vulnerable to money laundering and terrorist financing?

Every financial service, and therefore every payment system, has some degree of vulnerability criminals can exploit. World Bank research and analysis suggests the abuse of mobile money could stem from four major risk factors:[36] **anonymity**, **elusiveness**, **rapidity**, and **poor oversight**.[37]

In most markets, cash is still the predominant type of transaction. To understand how mobile money services can be vulnerable to ML/TF before AML/CFT controls are put in place, it is therefore useful to compare them to the vulnerabilities of cash. Table 1 compares the inherent risk factors for cash and mobile money before AML/CFT controls are put in place.

As Table 1 indicates, mobile money is less vulnerable to ML/TF than cash with respect to three of the four major risk factors (rapidity is the one exception), even before specific AML/CFT mitigation measures have been implemented. Given that mobile money services have been deployed primarily in developing countries with a high reliance on cash, one can expect greater adoption of mobile money will reduce ML/TF risk. Implementing specific controls to mitigate ML/TF risk further reduces the risks of mobile money services (see section 5 below).

36. As new technologies develop, additional risks may be identified.

37. Pierre-Laurent Chatain, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker (2011), cit., 33. These risk categories were first identified in Pierre-Laurent Chatain, Raúl Hernandez-Coss, Kamil Borowik, and Andrew Zerzan (2008), "Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing", 13, World Bank, Working Paper No. 146, 2008, Washington, DC.

TABLE 1

COMPARATIVE RISKS OF CASH AND MOBILE MONEY BEFORE SPECIFIC AML/CFT CONTROLS FOR MOBILE MONEY ARE INTRODUCED

Risk factor	Mobile money services before specific AML/CFT controls are in place		Cash	
Anonymity: Customer's identity is unknown	**	**Vulnerabilities** • If identification processes are weak or absent, criminals may operate with a degree of anonymity and open/operate multiple accounts • If identification processes exist but verification processes are weak (e.g. lack of reliable national identification), criminals may commit identity fraud **Compensating factors** • Transactions are linked to a unique mobile number • The SIM card and customer are identified and located through the MSISDN and IMSI • Transactions recorded (sender's mobile number, amount, receiver's mobile number, date) • Transactions traced • SIM card registration records make critical information available to identify the customer • If law enforcement officials wish to identify a particular unidentified client, the provider can supply a rich source of identifying details, like voice recordings and communication and transaction patterns[38]	***	**Vulnerabilities** • Transactions are largely anonymous • There is neither a unique identifier for the user nor a way to trace the payment **Compensating factors** • None
Elusiveness: Ability to disguise amount, origin, and destination	**	**Vulnerabilities** • Sharing a single handset, SIM, and/or mobile money account makes it harder to ensure the person conducting a transaction is the registered user • Smurfing allows criminals to use a number of small transactions to hide larger sums being transferred • Ubiquity of mobile phones eliminates requirement for sender and recipient to be in the same place at the same time **Compensating factors** • Mobile money transactions are clearly traceable in a mobile operator's system as part of standard business practice • Telephone number (sending and receiving), time, and the amount of the transaction are known to the mobile operator	***	**Vulnerabilities** • Amount, origin, and destination can all be disguised **Compensating factors** • Sender and recipient (or an intermediary) must at some point be in the same place at the same time
Rapidity	***	**Vulnerabilities** • Mobile money transactions typically occur in real time, allowing for rapid transaction layering (transferring funds among multiple accounts to obscure their origin) **Compensating factors** • Mobile money transactions are clearly traceable in a mobile operator's system as part of standard business practice • Telephone number (sending and receiving), time, and the amount of the transaction are known to the mobile operator	*	**Vulnerabilities** • Limited, since cash moves relatively slowly **Compensating factors** • Transaction layering is more difficult and may require regular face-to-face interaction with bank personnel

38. Louis de Koker (2009), "Anonymous Clients, Identified Clients and the Shades In Between: Perspectives on the FATF AML/CFT Standards and Mobile Banking." Paper presented at the 27th Cambridge International Symposium on Economic Crime, Jesus College, Cambridge, UK.

Risk factor	Mobile money services before specific AML/CFT controls are in place		Cash	
Lack of oversight or poor oversight	**	**Vulnerabilities** • In some countries, mobile money service providers (and/or their agents) may not be unambiguously included as "covered institutions" under the AML/CFT law and regulations • In some countries, financial regulators directly regulate and supervise a banking partner rather than the entity providing services on the ground, and may have the best understanding of the ML and TF risks • The quality of oversight can vary between jurisdictions **Compensating factors** • Mobile money providers are regulated and supervised,[39] but the extent and quality of supervision may vary between jurisdictions	***	**Vulnerabilities** • Pure cash transactions are not subject to oversight **Compensating factors** • None

KEY:

*** INDICATES ML/TF RISK IS HIGHER

** INDICATES ML/TF RISK IS MEDIUM

* INDICATES ML/TF RISK IS LOWER

3.2 How could mobile money vulnerabilities be exploited for financial crimes?

If mobile money providers do not apply additional control measures to mitigate risk, some of the vulnerabilities of mobile money services could be exploited for financial crimes. Assessing the attractiveness of these services to criminal elements helps to evaluate the robustness of a provider's system, detect potential abuses (by measuring the degree of risk posed by the service), and identify where additional mitigation measures are needed. So far, there have been relatively few reported cases of the use of mobile money services for money laundering or terrorist financing.[40] Nevertheless, a mobile money service could be abused through exploitation of certain vulnerabilities and risk factors, as discussed in the previous section. In addition, criminals can exploit mobile money through the same mechanisms currently used to exploit other retail payment systems (such as through hacking, collaboration with insiders, etc.).

Abuses related to financial crime (for both mobile money services and most standard financial products) can occur at any of the following three stages: (1) when funds are loaded onto an account, (2) when funds are transferred, and (3) when funds are withdrawn. In the case of mobile money, opportunities for ML/TF-related crime can arise for all participants in the system: customers, merchants, employees, and agents alike. This analysis is laid out in Table 2.

39. Even in countries where the mobile money provider has not been licensed on the basis of a codified regulation, the regulator has established prudential and non-prudential requirements for the provision of the services, which always include reporting obligations that allow the regulator to monitor the system (e.g. in Kenya and Tanzania; see Simone di Castri and Lara Gidvani (2014), "Enabling mobile money policies in Tanzania: A 'test and learn' approach to enabling market-led digital financial services", GSMA case study, London; Brian Muthiora (2015), Enabling Mobile Money Policies in Kenya, GSMA case study, London.

40. See FATF (2010), "Money Laundering Using New Payment Methods", para. 23; Pierre-Laurent Chatain, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker (2011), cit.; FATF (2013), "The Role of *Hawala* and Other Similar Service Providers in Money Laundering and Terrorist Financing"; FATF (2014), "Financial Flows Linked to the Production and Trafficking of Afghan Opiates"; FATF (2015), "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant".

TABLE 2

MONEY LAUNDERING AND TERRORIST FINANCING RISKS BY DIFFERENT PARTICIPANTS IN THE SYSTEM PRIOR TO MITIGATION

Typology	Indicator of possible ML/TF and methods to identify ML/TF	Vulnerability before specific mitigants are applied
ML/TF by consumer		
Fraudulent registration	Sampling of records can identify prevalence of acceptance of fraudulent identity documents	**
Multiple registrations, multiple deposits, and transfers	Transaction patterns may indicate multiple SIM ownership. A database clean-up can be performed to identify multiple registrations	**
Transfer of service after registration	Use outside of expected geographical area, or contrary to expected profile	**
Loading with POC	Unusually large loads, frequent loads, several small transactions from one source to different users or loads just below limit	**
Use of POC to purchase from sellers	Unusually large transactions or purchase of goods/services that do not make economic sense or do not correspond to expected transaction pattern	**
POC transferred to co-conspirators	Transfers are likely to be anomalous to usual geographical transfer patterns. Frequency and value may also be irregular	**
POC pooled into single account	Pooling pattern is anomalous unless the destination is a retail outlet or an individual, group savings scheme (e.g., ROSCA, tanda, susu), or family member being supported by another family member	**
Withdrawal of POC by cash redemption	Unusually high or frequent values that would be suspicious given the profile of the users of this product	**
Funds transfer to/from a person linked to terrorism or known fraudsters	Identity information of a user matches entry on an international or national watch list or their known associates	**
ML/TF by merchant		
Complicit merchant receives POC	Unusual transaction patterns for the type of business (initial and ongoing DD of merchants should reveal any irregularities)	**
Fraudulent merchant misappropriates funds	Inability to reconcile transactions with merchant and customer account balances (transaction monitoring and regular reconciliation can help to identify such incidents)	**
ML/TF by employee		
Fraudulent registration of false accounts to facilitate ML/TF	Internal staff details cross-referenced against customer/merchant/agent account details to identify possible collusion. Improper KYC procedures discovered during periodic verification of customer identity	***
Theft of funds using internal access (e.g. false transactions, creation of e-money without depositing corresponding funds, theft from dormant accounts)	Inability to reconcile outstanding e-money liabilities and available funds; audit trails indicate failure of segregation of duties/access controls; transaction monitoring system identifies suspicious activity. Internal staff details cross-referenced against customer/merchant/agent account details to identify possible collusion	***
Employee allows known POC funds to be loaded on or withdrawn from account	Internal staff details cross-referenced against customer/merchant/agent account details to identify possible collusion. Transaction monitoring system identifies suspicious activity, including smurfing, transactions inconsistent with prior behaviour, transfer of funds to/from high-risk areas, transfer of funds to/from previously dormant accounts, employee activity on customer/merchant/agent accounts, etc	***
Employee allows customers to exceed load or withdrawal limits	Internal staff details cross-referenced against customer/merchant/agent account details to identify possible collusion. Review of audit trails identifies cases of internal approval to override established limits	***

Typology	Indicator of possible ML/TF and methods to identify ML/TF	Vulnerability before specific mitigants are applied
ML/TF by agent		
Fraudulent registration or non-compliance with KYC procedures	Mystery shopping and onsite visits by the financial service provider can indicate if the agent is compromised	***
Agent allows known POC funds to be loaded on or withdrawn from account	Transaction monitoring system identifies suspicious activity, including smurfing, transactions inconsistent with prior behaviour, transfer of funds to/from high-risk areas, transfer of funds to/from previously dormant accounts, agent activity on customer/merchant/agent accounts, etc	***
Agent does not fulfil DD obligations, intentionally or negligently	Mystery shopping and onsite visits by the financial service provider can indicate if agent is fulfilling its obligations	***
Agent allows customers to exceed load or withdrawal limits	Transaction monitoring system identifies suspicious activity, including smurfing, transactions inconsistent with prior behaviour, transfer of funds to/from high-risk areas, transfer of funds to/from previously dormant accounts, agent activity on customer/merchant/agent accounts, etc.	**

KEY:

*** INDICATES ML/TF RISK IS HIGHER

** INDICATES ML/TF RISK IS MEDIUM

* INDICATES ML/TF RISK IS LOWER

POC = PROCEEDS OF CRIME
DD = DUE DILIGENCE
ML = MONEY LAUNDERING

CUSTOMERS

ML/TF by customers could take place as part of a conventional transfer of funds that are generated from criminal activity or are intended for an ML/TF crime. False credentials could be presented at registration or could be introduced by an agent.

MERCHANTS

ML/TF by merchants is a risk because they can receive substantial volumes of payments and extract them as seemingly legitimate business revenue through the integration of legitimate and illegitimate funds. Merchants may also act as fronts for the laundering of criminal proceeds transacted by co-conspirators posing as customers.

EMPLOYEES

ML/TF by employees is a risk because employees have access to internal system resources. In the absence of effective internal controls, employees can override system controls, subvert segregation of duties requirements, and use their privileged access to cover their tracks.

AGENTS

ML/TF by agents is a risk because agents are in a position to falsify records, ignore suspicious activity that should be reported, or otherwise fail to perform their duties in a diligent manner.

4. International regulatory responses to mobile money ML and TF risk: FATF Recommendations

> The FATF recognises that applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the financial system, thereby compelling them to use services that are not subject to regulatory and supervisory oversight. AML/CFT controls must not inhibit access to formal financial services for financially excluded and unbanked persons. The FATF recognises that financial exclusion could undermine the effectiveness of an AML/CFT regime hence, financial inclusion and AML/CFT should be seen as serving complementary objectives.
>
> **FATF Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services**

4.1 What is the international framework for AML/CFT?

The FATF was established in 1989 at the G-7 Paris Summit[41] as a dedicated body for setting international standards for effective legal, regulatory, and operational procedures to combat money laundering and assess compliance (see Table 3).[42] The scope of the FATF expanded to include countering the financing of terrorism following the United Nations International Convention for the Suppression of the Financing of Terrorism and in the aftermath of September 11, 2001. The FATF's scope has since expanded again to include countering the financing of weapons of mass destruction proliferation.

The FATF Standards, while not legally binding, are enforced by peer pressure of the FATF-member countries and the member countries of the FATF-Style Regional Bodies (FSRBs). Together, the FATF and the eight FSRBs count approximately 180 countries as members. The FATF and FSRBs conduct peer assessments called "mutual evaluations" to assess compliance and effective implementation of the FATF standards at the national level. These evaluations consider both technical compliance (i.e. whether the required laws, regulations, and institutional framework are in place) and effectiveness (i.e. the extent to which AML/CFT systems are working in practice).[43]

The FATF's International Cooperation Review Group (ICRG) publicly identifies countries with strategic AML/CFT deficiencies and works with each country to develop an action plan. Initial referral to the ICRG is based primarily

41. The EU was also invited to participate.
42. The 1990 FATF report on preventing the abuse of the financial system through money laundering included 40 recommendations. At that time, FATF members were primarily OECD countries, which reconvened to assess to what extent members had implemented the recommendations. This process was the beginning of the recommendations being solidified into standards.
43. FATF (2013), "Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations," para. 2.

on the results of the jurisdiction's mutual evaluation. The FATF issues public statements three times a year updating the status of countries in the ICRG process. Countries that fail to make a high-level political commitment to address the identified deficiencies or to make progress can become subject to a FATF call on its members and other jurisdictions to apply counter-measures. Because of the new risks introduced to the financial system and the greater diligence required of financial institutions and counterparts in other countries, institutions in countries identified as having strategic AML/CFT deficiencies may lose business relationships, face increased costs, and/or slower transactions. These measures may ultimately have a negative impact on the national economy.

Therefore, while every country determines on its own when and how to adapt and implement the FATF Standards, failure to comply can have such serious economic consequences that many policy makers and regulators adopt overly conservative practices and rules to avoid the risk of punitive measures.[44] Furthermore, even when regulators provide flexibility, financial institutions are often reluctant to accept non-traditional identity documents or open accounts with simplified KYC for fear of being penalised in the event of abuse.[45] This has had an impact on the ability of mobile money providers to reach lower income, unbanked people who typically lack access to traditional identity documents and may not have a formal address. When 37 representatives of MNOs offering mobile money services were asked to identify the AML/CFT-related challenges they faced, 32% cited regulatory problems such as the lack of a risk-based regulatory approach, regulators' insufficient understanding of mobile money, and unclear guidance from regulators, while another 13% highlighted the lack of reliable government-issued IDs as a major challenge.[46]

TABLE 3

RELEVANT FATF DOCUMENTS

TITLE	RELEASED	HEREINAFTER
International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations	2012	FATF Recommendations
• Previous version: The 40 Recommendations	2003	40 Recommendations
FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment	2013	RBA Guidance
Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion	2013	Financial Inclusion Guidance
• Previous version: Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion	2011	First Financial Inclusion Guidance
Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services	2013	NPPS Guidance
• Previous version: FATF Report on Money Laundering Using New Payment Methods	2010	NPM Report
Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems	2013	Compliance & Effectiveness Methodology
Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations	2013	Mutual Evaluation Procedures
Risk-Based Approach: Guidance for Money Service Businesses	2009	MSB Guidance

44. See, e.g., FATF (2013), "Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion", para. 67.
45. Bester et al. (2008), "Implementing FATF standards in developing countries and financial inclusion: findings and guidelines", Genesis Analytics, Johannesburg.
46. GSMA (2015), Survey of AML/CFT practices (see Section 5.1).

The 2003 FATF Recommendations[47] allowed countries to implement a risk-based approach for certain aspects of AML/CFT, but there was no clarity on risk assessment and appropriate risk measures.[48] Fears of not meeting the expectations of FATF assessors and landing on a public list of non-compliant countries discouraged countries from embracing the RBA principle. The FATF began issuing guidance on the Recommendations, but these focused mainly on high-risk services.

In 2010, under the Mexican FATF Presidency, the FATF partnered with the Asia Pacific Group on Money Laundering (APG) and the World Bank to develop guidance on financial inclusion. In 2011, it issued a non-binding guidance document on AML/CFT and financial inclusion, providing support to countries and financial institutions designing AML/CFT measures that would meet national financial inclusion goals without compromising existing measures for combating crime. The main aims of the guidance were to develop a common understanding of the relevant FATF Standards for financial inclusion and to elaborate upon the flexibility of the Recommendations, especially the risk-based approach (RBA), to enable jurisdictions to craft effective and appropriate controls. As the FATF warned, "applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the financial system." This guidance focused on financial exclusion as a risk to the effectiveness and reach of AML/CFT controls, which informed the review of the Recommendations in 2012.

The FATF released the new *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (hereinafter, "FATF Recommendations") in February 2012[49] and later published:

- a revised version of the *Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (hereinafter, the "Financial Inclusion Guidance");[50]
- the new *Guidance to Assist in the Conduct of Risk Assessment at the Country or National Level* (hereinafter, the "RBA Guidance");[51] and
- the new *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services,* otherwise known as guidance on new payment products and services (hereinafter, "NPPS Guidance").[52]

This AML/CFT regime determines, at a country level, the KYC and CDD compliance requirements for mobile money providers, which the FATF Recommendations typically categorise as money or value transfer services (MVTS) providers.[53]

The 2012 Recommendations formally integrated the risk-based approach, mandating regulators to design and implement effective AML/CFT controls appropriate to the specific risks of products and services. The RBA is now mandatory for all countries and AML/CFT-regulated institutions and professions. For mobile money, this means that services assessed as "proven low risk" may benefit from full or partial exemption from AML/CFT requirements, while services assessed as "lower risk" may benefit from simplified CDD measures. Countries that designate services as "lower risk" or "proven low risk" and provide exemptions or simplified CDD measures must be able to provide assessors with evidence and analysis to support these decisions.[54]

47. FATF (2003), "The 40 Recommendations".
48. See FATF (2003), Interpretative Notes for Recommendations 10, 12, 22, 23, 24 and 25.
49. FATF (2012), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation".
50. FATF (2013a), "Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion".
51. FATF (2013b), "Guidance to Assist in the Conduct of Risk Assessment at the Country or National Level".
52. FATF (2013c), "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services".
53. "Money or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs." FATF (2012), in Glossary. Note that a mobile money provider would not be classified as an MVTS provider if it is simply providing bill payment services and not providing P2P services. See FATF (2013c), "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services", para. 123-124.
54. FATF (2013), "Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems", para. 18-19.

The NPPS Guidance determines the risk factors and mitigation measures associated with NPPS and examines how to regulate and supervise service providers. In addition, it assesses the impact of AML/CFT regulation on the NPPS market, including the potential impact on financial inclusion.

The Financial Inclusion Guidance explains why financial exclusion is an ML/TF risk and why reducing financial exclusion is vital to an effective AML/CFT system. Together with the NPPS Guidance, the Financial Inclusion Guidance document is particularly helpful for assessing the risks related to mobile money products and, eventually, simplifying the requirements of the main AML/CFT regulations for the mobile money industry.

As noted earlier, the FATF classifies non-bank mobile money providers as money or value transfer services (MVTS) providers, which means mobile money providers must comply with certain CDD measures and record keeping, monitoring, and reporting requirements. Mobile money services that contribute to financial inclusion must ensure financial integrity, for example, by placing limits on transactions and balances and using mechanisms that provide close oversight of the system. The risk-based approach is therefore an ideal framework for implementing proportional compliance requirements — inclusive and safe, but not too onerous or expensive. Table 4 illustrates how a simplified risk-based approach would apply in scenarios with different levels of risk and with control measures proportionate to different risks.

TABLE 4

EXAMPLES OF RISKS AND CONTROL MEASURES IN A SIMPLIFIED RBA

	POTENTIAL HIGHER RISK SITUATIONS	POTENTIAL LOWER RISK SITUATIONS
Customers	• Non-resident customers • Businesses that are cash intensive	• Residents only • Natural persons only
Geographical risks	• Transactions within or between countries with inadequate AML/CFT systems and/or high levels of corruption/criminal activity	• Transactions within or between countries with effective AML/CFT systems and/or low levels of corruption/criminal activity
Products	• Products permitting non-face-to-face transactions • Products permitting anonymous transactions • Products with high (or no) transaction limits	• Financial products or services that provide appropriately defined and limited services to certain types of customers, which are intended to increase financial inclusion
Examples of risk control measures (potential response to a potential risk)	• Obtaining additional information about a customer (occupation, volume of assets, source of funds, etc.) and more frequent updates	• Verifying identity after commencing a business relationship • Reducing the level of transaction monitoring based on a reasonable monetary threshold • Inferring rather than obtaining information about the purpose of the business relationship

4.2 Which FATF Recommendations are most relevant to mobile money?[55]

According to the FATF, achieving greater financial inclusion is important to protecting the financial sector from the risk of money laundering and terrorist financing. To expand access to financial services to people who would otherwise be relegated to the cash economy and informal services, it is vital for national policy makers and regulators to embrace new technologies and address emerging risks according to the principle of proportionality.[56] A balanced approach is critical to implementing cost-effective AML/CFT controls proportionate to the risks of specific financial services. This section identifies the most relevant FATF Recommendations for regulators and mobile money providers to consider.

The FATF Recommendations are grouped into seven categories: (1) risk assessments and RBA, (2) criminalisation of money laundering and forfeiture of illicit assets, (3) financing of terrorism and weapons of mass destruction proliferation, (4) preventive measures, (5) transparency and beneficial ownership of legal entities, (6) supervision of financial institutions, roles and responsibilities of law enforcement, and the role of the financial intelligence unit (FIU), and (7) international cooperation.

For the purpose of this paper, we focus on the Recommendations related to risk assessments and preventive measures, such as customer identification, record-keeping obligations, filing suspicious transaction reports (STRs), and conducting enhanced due diligence for high-risk customers such as politically exposed persons (PEPs) and their families. Excerpts from the Recommendations discussed below are included as Annex 1.

The 2012 Recommendations reinforce the FATF's commitment to proportional regulation by formalising the use of the risk-based approach (RBA) and requiring country regulators to fine-tune their requirements to the level of risk posed by specific financial services.

The current FATF Recommendations allow for simplified CDD measures proportionate to the risk of money laundering or terrorist financing. Depending on the assessed level of risk, countries may decide reduced or simplified controls are sufficient to safeguard lower risk activities against abuse. Furthermore, if a national regulator finds that some financial institutions or activities meet FATF criteria for exemption, it may even decide not to apply some of the FATF Recommendations to these institutions or activities.

With regard to mobile money, for example, a national regulator may consider applying so-called "progressive" or "tiered" KYC/CDD approaches whereby transaction/payment limits vary based on CDD: the more complete the CDD process, the higher the limits.

RECOMMENDATION 1: ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH

Recommendation 1 addresses mandatory risk assessment: the expectation that countries *"identify, assess and understand"* ML/TF risks and then apply an RBA to ensure mitigation measures are commensurate with the risks identified. In other words, higher risks require enhanced risk mitigation measures, while simplified CDD can be applied to lower risk customers, products, and services. Recommendation 1 also states that countries should require financial institutions to conduct their own risk assessments, which can also inform a national, sectoral, or thematic risk assessment. Recommendation 1 can be read with Recommendation 2 on national cooperation and coordination, which calls for the development of national, risk-based AML/CFT policies in response to the national risk assessment.

55. This section includes the authors' collective opinion of which FATF Recommendations are most relevant to mobile money. This opinion has not been endorsed by the FATF.

56. The G20 Principles for Innovative Financial Inclusion issued in 2010 promote the application of the proportionality principle as the right balance between risks and benefits by tailoring regulation to mitigate the risk of the product without imposing an undue regulatory burden that could stifle innovation: "Principle 8 on Proportionality: Build a policy and regulatory framework that is proportionate with the risks and benefits involved in such innovative products and services and is based on an understanding of the gaps and barriers in existing regulation." See G20 Financial Inclusion Experts Group (2010), "Innovative Financial Inclusion Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group."

RECOMMENDATION 10: CUSTOMER DUE DILIGENCE

Recommendation 10 expands on CDD obligations, touching on issues such as customer identification and verification of customer identity, identification in non-face-to-face scenarios, obtaining information on the purpose and intended nature of the business relationship, conducting ongoing due diligence, and monitoring the business relationship. Recommendation 10 also requires the use of a risk-based approach when applying required CDD measures.

Interpretative Note 10.11 allows financial institutions in non-face-to-face scenarios to verify the identity of a customer after the business relationship[57] is established if it is essential not to interrupt the normal course of business and risk management measures such as transaction limits are put in place.

Interpretative Note 10.17 provides examples of potentially lower risk scenarios in which a country could allow its financial institutions to apply simplified CDD. One such example is when financial institutions are offering "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes."[58] It is important to note that simplified CDD never means an absence of CDD; rather, that reduced CDD is commensurate with the lower risks posed. Interpretative Note 10.21 discusses some examples of possible simplified CDD measures (see Annex 1). One measure would be to infer the purpose and nature of the business relationship from the type of account established and/or types of transactions conducted, rather than collecting information and then implementing specific measures to satisfy this obligation. For example, *"if an account is obviously opened to enable a poor migrant to send/receive small value transfers to and from his/her country of origin through a safe, affordable and formal channel, this element of the CDD requirements could be considered fulfilled."*[59]

Simplified CDD measures may not be used if there is a suspicion of ML/TF risk or in higher risk scenarios, such as anonymous transactions or transactions involving PEPs, correspondent banking, or countries with high levels of corruption, criminal activity, or support for terrorist activities. In addition, financial institutions engaged in money transfer and those using new technologies must take certain measures to address the risks inherent in these services (see discussion of Recommendations 14–16 below).

The Financial Inclusion Guidance discusses ongoing due diligence and monitoring of the business relationship in the context of financial inclusion. For example, since monitoring in a risk-based system is primarily aimed at responding to enterprise-wide issues based on the financial institution's analysis of its major risks, regulatory authorities seeking to promote financial inclusion *"should be mindful of and give due weight to the determinations made by financial institutions, provided that these determinations are consistent with any legislative or regulatory requirements, and informed by a credible risk assessment and the mitigating measures are reasonable and adequately documented."* The Financial Inclusion Guidance also notes that technology-based service models are often easier to monitor and financial institutions applying an RBA could establish monetary or other thresholds below which an activity would be subject to reduced or limited monitoring. These thresholds should be reviewed on a regular basis to determine whether they are still appropriate to the assessed risk level. Financial institutions should also periodically assess the adequacy of all systems and processes.

RECOMMENDATION 11: RECORD KEEPING

Recommendation 11 requires financial institutions to maintain records of all transactions for at least five years so they are able to quickly provide evidence to authorities prosecuting criminal activity, if requested. Financial institutions should also keep all records related to the CDD process for at least five years after the business relationship has ended or from the date of the occasional transaction (in the absence of a business relationship).

57. The FATF does not define a business relationship, but it is commonly understood to mean an association between individuals/customers and financial institutions entered into for commercial purposes, sometimes formalised with legal contracts or agreements.
58. FATF (2012), 64, INR 10.17[b].
59. FATF (2013a), 36.

While record keeping is required for even lower risk accounts, it is important to note that no specific form of record keeping is required for CDD compliance. The Financial Inclusion Guidance states that *"[T]he record keeping requirement does not require retention of a photocopy of the identification document(s) presented for verification purposes; it merely requires that the information on that document be stored and kept for five years."*[60] Even wealthy countries such as Australia, Canada, and the United States do not impose photocopying requirements, considering it too great a risk for identity fraud and breach of privacy laws, among other reasons.[61] Moreover, different types of record keeping are allowed, from storing electronic scans of ID documents and registration forms to handwritten reference details on identity or transaction documents.

RECOMMENDATION 14: MONEY AND VALUE TRANSFER SERVICES (MVTS)

Recommendation 14 requires MVTS providers (including mobile money providers that offer P2P services) to be licensed or registered, to have effective monitoring systems, and to comply with the AML/CFT regime in accordance with Recommendation 26.[62] It also requires agents[63] to be registered or licensed by a competent authority or for a list of agents to be readily available from the provider should the authorities require it.

Providers should include their agents in their AML/CFT programmes and monitor compliance. According to the FATF, which sees agents as an extension of the principal financial institution, *"it is appropriate for regulatory supervision and oversight to focus primarily on the principal financial institution. Monitoring and supervising thousands of agents would be extremely challenging for most, if not all, countries. The oversight of agents is mainly performed by the principal financial institution"*,[64] while the authority responsible for overseeing the system limits its role to examining the provider's policies and procedures and the training and monitoring of agents by the provider.[65]

Financial institutions should conduct baseline monitoring of agents and then, based on their RBAs, determine the degree and nature of monitoring based on factors such as *"the transaction volume and values handled by the agent, the monitoring method being utilised (manual, automated, or some combination) . . . the type of activity under scrutiny . . . the products or services provided by the agent, and the agent's location."*[66]

RECOMMENDATION 15: NEW TECHNOLOGIES

Recommendation 15 requires countries and financial institutions to assess the potential ML/TF risks of developing new products and business practices, including new delivery mechanisms and the use of new and developing technologies for both new and pre-existing products. Financial institutions should conduct this risk assessment before launching new products, business practices, or technologies, and appropriate measures should be taken to manage and mitigate those risks. This initial pre-launch risk assessment will be refined and adjusted since financial institutions are required to regularly review and adapt their RBA measures.[67]

Using new technologies to develop innovative distribution channels or products does not automatically necessitate additional CDD measures. However, an additional, dedicated risk assessment is required for new products and business practices. The specific types of business relationships and transactions, the target client groups, the involvement of intermediaries, and the sophistication of the technology must all be taken into account when evaluating the risks and determining the appropriate level of CDD to be applied.[68]

60. FATF (2013a), p39.
61. FATF (2013a), p39
62. Recommendation 26 requires any institution that provides a money or value transfer service to be licensed or registered and subject to effective systems for monitoring and compliance with national AML/CFT requirements.
63. For the purpose of this paper, the term "agents" refers to individuals and legal persons or other entities participating in the distribution of mobile money services acting on behalf of (whether by contract with or under the direction of) the provider based on a legal agreement between the two parties. The FATF sees any agent as an extension of the financial services provider. Consequently, "the conduct of CDD by these agents is treated as if conducted by the principal financial institution. The customers themselves generally view the retailer as a point of access and as a representative of the principal financial institution." The principal financial institution bears ultimate responsibility for compliance with all applicable AML/CFT requirements. See FATF (2013a), 42-43; see also FATF (2012), under Definitions.
64. FATF (2013a), 44.
65. See also Recommendation 18, infra.
66. FATF (2013a), 44
67. FATF (2012), 33, INR 1.8
68. FATF (2013a), 35

RECOMMENDATION 16: WIRE TRANSFERS

Recommendation 16 requires providers to include accurate originator and beneficiary information in a wire transfer message and ensure it remains with the wire transfer throughout the payment chain. The provider must also be able to detect transactions that are missing this information and to freeze accounts if required by the United Nations Security Council (UNSC) rules. There are some practical caveats to this, however:

- For "qualifying wire transfers" (cross-border transfers above any minimum threshold that may have been established), the ordering institution is not required to verify both parties in the transfer service — just the sender's identity and information. The receiving institution can verify the beneficiary's information.

- Domestic wire transfers should include the same originator information required for cross-border transfers unless this information can be made available to the beneficiary institution and the relevant authorities through other methods. In such cases, the ordering financial institution only needs to include an account number or other unique identifier that will allow the transaction to be traced back to the sender or the beneficiary.

- Countries can adopt a minimum threshold that may not exceed USD or EUR 1,000. For cross-border wire transfers below this threshold, countries may exempt providers from verifying the name of the sender and the beneficiary, provided there is no suspicion of money laundering or terrorist financing.

The FATF (see Recommendation 20 below) also requires mobile money providers to report any suspicious transactions through suspicious transaction reports (STRs) to the FIU. Providers are required to keep all necessary records of all transactions for five years to provide transactional information to law enforcement, if necessary. The five-year requirement applies to all records collected for CDD purposes. CDD records also need to be kept up-to-date through periodic reviews.

RECOMMENDATION 18: INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES

Recommendation 18 requires financial institutions to implement AML/CFT programmes and financial groups to implement group-wide programmes, including policies and procedures for sharing information within the group. In general, these programmes should include:

- *"the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;*

- *an ongoing employee training programme; and*

- *an independent audit function to test the system."* [69]

Financial institutions should develop *"an effective internal control structure, including suspicious activity monitoring and reporting and create a culture of compliance, ensuring that staff adheres to the financial institution's policies, procedures and processes designed to limit and control risks."*[70] The FATF notes that the type and extent of these measures should be in line with the level of ML/TF risk and the size of the business.[71]

RECOMMENDATION 20: REPORTING OF SUSPICIOUS TRANSACTIONS

When a financial institution suspects funds are the proceeds of a criminal activity or related to terrorist financing, Recommendation 20 requires it to report this promptly to the country's FIU. Reporting suspicious transactions or activities is critical to a country's ability to use financial information to combat financial

69. FATF (2012), INR 18.1
70. FATF (2013a), 46.
71. FATF (2012), INR 18.1

crimes. Therefore, reporting suspicious activity is always mandatory. However, an RBA of individual financial services is still important for gauging the risk of financial crimes and allocating additional resources to higher risk areas. Financial institutions are required to develop appropriate internal monitoring systems to identify any suspicious behaviour.[72]

RECOMMENDATION 26: REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS

Recommendation 26 requires financial institutions providing a money or value transfer service to be *"licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements."*[73] Countries applying an RBA to supervision can tailor the frequency and intensity of supervision according to the ML/TF risks presented by the service and the policies, procedures, and internal controls adopted by the financial institution in question.[74]

RECOMMENDATION 34: GUIDANCE AND FEEDBACK

Recommendation 34 requires the competent authorities to establish guidelines and provide feedback to assist financial institutions in applying national AML/CFT measures, particularly for detecting and reporting suspicious transactions. The Financial Inclusion Guidance notes that *"Effective information exchange between the public and private sectors will form an integral part of a country's strategy for combating money laundering and terrorist financing while promoting financial inclusion."*[75] A positive feedback cycle is an essential part of public and private sector collaboration, as both public and private sector stakeholders have a shared goal to create a safe national financial sector.

72. See FATF (2013a), 40.
73. FATF (2012), Recommendation 18
74. FATF (2012), INR 18
75. FATF (2013a), 48.

5. Provider responses to mobile money ML and TF risk: Internal controls

In most cases, mobile money services are provided by regulated institutions that act pursuant to a regulatory and oversight framework of the competent financial sector authority. In countries where there is no law or regulation governing mobile money services (e.g. Kenya until 2014 and Tanzania), the central bank has provided space to safely launch mobile money services under its oversight by establishing provisional prudential and market conduct requirements via "Letters of No-Objection".[76]

After identifying potential vulnerabilities in the system (Section 3.1) and how these vulnerabilities can be exploited (Section 3.2), control measures can be designed to mitigate the risks while complying with relevant regulatory requirements (Section 4). Mitigation measures should be proportionate to the risk of the product.

5.1 Examples of how service providers have mitigated risks

From March to May 2015, the GSMA surveyed 37 mobile money providers to identify the CDD practices and internal risk controls they had implemented.[77] Respondents, all of which are MNO subsidiaries, represent 24 countries on five continents and include eight of the 13 largest MNO-led mobile money services worldwide. A summary of the full results of the survey is presented in Annex 2. In addition to being used in this publication, the survey results will inform the industry's ongoing efforts to strengthen AML/CFT risk mitigation practices through the GSMA's new Code of Conduct initiative (see Box 2).

The survey revealed that virtually all providers had a high level of commitment to preventing ML/TF and complying with AML/CFT requirements. The vast majority of the internal controls recommended by the FATF[78] have been implemented. This is a particularly significant result given most respondents operate in countries without a national identification system and their mobile money industry is still young and evolving. The analysis of emerging risks is therefore ongoing. The survey also revealed that the vast majority of mobile money services have been designed to mitigate and manage most ML/TF risks through limits on balances and transactions, combined with screening of staff, agents and clients and effective ongoing monitoring of staff, agents, and transactions.

76. See, for example, Simone di Castri and Lara Gidvani (2014), "Enabling mobile money policies in Tanzania: A 'test and learn' approach to enabling market-led digital financial services", GSMA case study, London.
77. The survey was conducted between March and May 2015. Survey responses were checked for clarity and internal consistency, but all information was self-reported and has not been verified independently by the GSMA. Information was reported on a confidential basis, and the report protects the confidentiality of each deployment.
78. FATF (2013a), Sec. 4.5.

BOX 2

INDUSTRY-LED AML/CFT EFFORTS: THE GSMA CODE OF CONDUCT FOR MOBILE MONEY PROVIDERS

The GSMA Code of Conduct for Mobile Money Providers is an initiative aimed at promoting the adoption of consistent risk mitigation practices by mobile money providers in critical areas of their business. The Code's eight principles address a variety of issues related to the provision of safe and sound services and the fair treatment of customers. Principle 2 addresses specific commitments related to AML/CFT:

> **Principle 2: Providers have in place effective, proportional risk-based mechanisms to prevent, detect, and report the misuse of services for the purpose of money laundering or terrorist financing (ML/TF).**
>
> **2.1 Effective policies and procedures**
> *2.1.1 Providers shall develop effective policies and procedures for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) compliance.*
>
> **2.2 Senior management commitment**
> *2.2.1 Senior management shall demonstrate their commitment to AML/CFT compliance through proper oversight.*
>
> **2.3 Appointed AML/CFT manager**
> *2.3.1 Providers shall appoint a qualified employee to promote and monitor compliance with AML/CFT-related obligations.*
>
> **2.4 Software to monitor transactions**
> *2.4.1 Providers shall create a system to monitor transactions for AML/CFT purposes.*
>
> **2.5 Risk-based KYC requirements and transaction / balance limits**
> *2.5.1 Providers shall properly identify clients and may use a risk-based KYC approach if permitted by local laws and regulations.*
> *2.5.2 Providers shall place appropriate risk-based transaction and balance limits on accounts, depending upon the strength of customer identification and verification.*
> *2.5.3 Providers shall have the ability to block account transactions under certain circumstances.*
> *2.5.4 Providers shall screen accounts using domestic and international money laundering, terrorist financing, and sanctions watch lists.*
>
> **2.6 Staff and agent AML/CFT training procedures**
> *2.6.1 Providers shall ensure that staff and agents are properly trained in AML/CFT procedures.*
> *2.6.2 Providers shall monitor staff and agent compliance with AML/CFT procedures.*
> *2.6.3 Providers shall develop clear policies and processes for addressing staff and agent AML/CFT violations.*

The Code of Conduct was publicly launched in November 2014. As of May 2015, 12 mobile network operator groups (representing 83 mobile money providers in 51 countries) had endorsed the Code.[79]

Most service providers assess the risk of a mobile money product in the initial design phase, but it is understood that not all risks can be identified at this stage and that risks need to be reviewed before a product is launched and regularly over the lifetime of the product. The following are examples of risk mitigation measures mobile money providers have undertaken.

INITIAL SCREENING OF STAFF, AGENTS, MASTER AGENTS, AND CUSTOMERS

The vast majority of providers conduct initial screening before hiring staff, contracting with an agent, or providing mobile money services to a customer (see Table 5). Merchants and agents are subject to enhanced CDD processes

79. For additional information regarding the GSMA Code of Conduct for Mobile Money providers, please refer to the GSMA website at http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-the-unbanked/code-of-conduct.

before being licensed/registered and trained, and the regulator can assist providers by sharing "blacklists" of individuals or businesses not suitable to serve as agents. Customer names can be screened quickly against national and international watch lists and flagged automatically (if these lists are provided to the industry).

TABLE 5

INITIAL SCREENING MEASURES ADOPTED BY MOBILE MONEY PROVIDERS

CATEGORY	% OF PROVIDERS WHO SCREEN	MOST COMMON SCREENING MEASURES (ADOPTED BY MOST PROVIDERS)	OTHER SCREENING MEASURES (ADOPTED BY SOME PROVIDERS)
Staff	89%	• Criminal background checks	• Reference checks • Review of academic and employment history • Review of financial information
Individual agents	100%	• Identification of business owner • Copies of business registration documents • Checking domestic and/or international watch lists	• Criminal background checks on business owner and staff • Proof of address
Master agents	100%	• Copies of business registration documents • Checking domestic and/or international watch lists • Identification of business owner and senior management • Identification of beneficial owners and controllers	• Criminal background checks on business owner and senior management • Criminal background checks on beneficial owners and controllers • Proof of address • Copies of licence (if supervised by a regulatory body)
Use of watch lists to screen customers and agents	89%	• US Office of Foreign Assets Control's Specially Designated Nationals List (US OFAC)	• Domestic list provided by financial regulator • Consolidated United Nations Security Council Sanctions List (UN) • Consolidated List of Persons, Groups and Entities subject to EU Financial Sanctions (EU) • Watch lists provided by Dow Jones • World Check by Thompson Reuters • Global politically exposed person (PEP) list
Timing and frequency of watch list screening		• Upon registration	• Periodically (daily, weekly, monthly, quarterly, or annually), or whenever there is an update to the list

AML/CFT TRAINING FOR STAFF, AGENTS, AND MASTER AGENTS

The vast majority of providers train staff, agents, and master agents on important topics related to their respective AML/CFT obligations (see Table 6). For example, providers train agents on AML/CFT regulations and CDD compliance procedures, and providers have staff who are specially trained to identify suspicious transactions and trends, as well as other triggers and red flags. Agents are trained to identify non-compliance with AML/CFT and CDD requirements and to refuse to perform transactions in the event of insufficient identification, breach of account limits, the inability of a customer to verify the source of funds, and other cases of suspicious transactions.

TABLE 6

AML/CFT TRAINING TOPICS ADDRESSED BY MOBILE MONEY PROVIDERS

CATEGORY	% OF PROVIDERS WHO TRAIN	MOST COMMON TRAINING TOPICS (ADDRESSED BY MOST PROVIDERS)	OTHER TRAINING TOPICS (ADDRESSED BY SOME PROVIDERS)
Staff	97%	• Responsibility of provider and individual staff for AML/CFT compliance and suspicious transaction reporting • Provider's policies and procedures and the role of staff with respect to these policies and procedures • How to conduct proper CDD when registering new clients • How to monitor agent compliance with AML/CFT requirements • Proper record-keeping procedures • How to identify and report suspicious activity without "tipping off"	• Relevant emerging risks and trends in ML/TF • How to communicate with agents • Awareness of what constitutes ML/TF
Individual agents	94%	• How to conduct proper CDD when registering new clients • Provider's policies and procedures and the role of staff with respect to these policies and procedures • Proper record-keeping procedures • How to identify and report suspicious activity without "tipping off"	• Relevant emerging risks and trends in ML/TF
Master agents	88%	• Provider's policies and procedures and the role of staff with respect to these policies and procedures • How to conduct proper CDD when registering new clients • Proper recordkeeping procedures • How to identify and report suspicious activity without "tipping off"	• Relevant emerging risks and trends in ML/TF
Frequency of training staff and agents		• Beginning of service and then annually thereafter	• Quarterly, every six months, or every two years

MONITORING AML/CFT COMPLIANCE OF STAFF, INDIVIDUAL AGENTS, MASTER AGENTS, AND CUSTOMERS

Virtually all surveyed providers continue to monitor staff, individual agents, master agents, and customers to ensure compliance with AML/CFT requirements and identify potential cases of money laundering or terrorist financing (see Table 7). Providers monitor agents' transaction patterns and conduct on-site inspections, sometimes using mystery shoppers. Providers have a strong incentive to ensure agent compliance, as they remain legally liable for any violations of AML/CFT requirements by their agents.

TABLE 7

AML/CFT MONITORING MEASURES USED BY MOBILE MONEY PROVIDERS

CATEGORY	% OF PROVIDERS WHO MONITOR	MOST COMMON MEASURES (USED BY MOST PROVIDERS)	OTHER MEASURES (USED BY SOME PROVIDERS)
Staff	97%	• Regularly reviewing records and transaction audit trails to assess the quality of staff compliance with AML/CFT requirements • Testing understanding of policies, procedures, and legal obligations	
Individual agents	94%	• Regularly reviewing records and transaction audit trails to assess the quality of agent compliance with AML/CFT requirements	• On-site and off-site audits (including mystery shopping) • Testing understanding of policies, procedures, and legal obligations • Regular agent conferences
Master agents	88%	• Regularly reviewing records and transaction audit trails to assess the quality of agent compliance with AML/CFT requirements	• On-site and off-site audits (including mystery shopping) • Testing understanding of policies, procedures, and legal obligations • Regular agent conferences
Type of transaction monitoring system	89%	• Have purchased a specialised automated transaction monitoring system	• In-house software solution • Manual monitoring checks • Reliance on bank partner for transaction monitoring • No formal monitoring system or did not understand the question

Most providers also use automated transaction monitoring systems to identify suspicious transactions by customers, agents, or staff. The most common methods for identifying suspicious transactions include:

- **Identification of potentially suspicious transactions:** Unusual account opening, termination, or changes to accounts; smurfing; changes in the velocity of transactions; transfer of funds to/from previously dormant accounts, etc.
- **Internal monitoring:** Monitoring internal logs and employee activity to ensure system access is limited to authorised individuals during normal business hours and their activity is appropriate.
- **Transaction logging:** Ensuring all transactions are logged with audit trails that allow reconstruction of transactions and record any attempts to modify transaction information.
- **Behaviour profiling:** Transaction analysis to develop unique behaviour profiles for customers and agents.

Some providers also employ **geographic validation** to identify suspicious behaviour, such as agents operating outside their area, transactions to/from suspicious locations, or transactions by an agent when the customer is not at the agent location.

Box 3 and Box 4 below include examples of how transaction monitoring systems operate in practice.

BOX 3

TESTIMONY FROM MOBILE MONEY PROVIDERS THAT HAVE IMPLEMENTED RISK MITIGATION MEASURES[80]

"Alerts are generated using transactional data / blacklist screening results for customers as per pre-defined rules and frequency. Investigation is carried out for each alert to assess the source and end use of funds in the wallet. Any suspicious transactions are reported to appropriate committees for views and filed with FIU if suspicion is confirmed."

"We use an in-house built software to detect suspicious and fraudulent transactions. The software allows us to screen all activities periodically, several times during the day, and to have immediate access to information, such as the average daily transaction volume — information that can be verified with the average daily transaction volume for the previous month. Also, the software automatically flags a sender or beneficiary that has transferred or received more than a specified amount in a month."

BOX 4

MINOTAUR: M-PESA'S TRANSACTION MONITORING SOFTWARE

Safaricom uses Neural Technologies' Minotaur software for AML/CFT risk management. Key features of the Minotaur mobile payments solution include:

- **KYC:** Minotaur facilitates KYC through watch list searches (external and internal) and data verification rules (e.g. ensuring proper format for national ID numbers)
- **Account activity:** Minotaur monitors and investigates all types of user activity (voice, data, and SMS) for all system users, including customers, agents, and staff. Minotaur monitors account opening, termination, and changes to accounts to identify suspicious activity. It also identifies customers with multiple accounts under the same name or possible duplicate accounts under similar names.
- **Behaviour profiling:** Minotaur conducts transaction analysis to build unique behaviour profiles for every customer and agent. These profiles are combined with account information to identify potentially suspicious activity, such as smurfing, transactions inconsistent with prior behaviour, changes in the velocity of transactions, transfer of money to/from high-risk areas, or transfer of funds to/from previously dormant accounts.
- **Geographic validation:** Minotaur tracks the location of the parties for every transaction to identify suspicious behaviour, such as agents operating outside their area, transactions to/from suspicious locations, or transactions by an agent when the customer is not at the agent location.
- **Internal monitoring:** Minotaur monitors internal logs and employee activity to ensure system access is limited to authorised individuals during normal business hours and their activity is appropriate.

Sources: Communication with Safaricom staff; Neural Technologies, Mobile Payments Fraud.

80. Source: 2013 GSMA survey of mobile money providers.

TRANSACTION, BALANCE, AND OTHER ACCOUNT FUNCTIONALITY LIMITS

Mobile money accounts are typically subject to transaction, balance, and other account functionality limits that may be established by the regulator or developed internally. Common control measures include limits on:

- the amount per transaction
- the amount that may be sent or received per day, month, and/or year
- the maximum balance that may be stored at any time

Most survey respondents also limit the use of their services geographically (within national borders)[81] and restrict the number of accounts to one per person. In most cases, this is prescribed by regulation.

> *"In a country with limitations on the type and quality of IDs and a large rural sector with no street or house markings, regulators have to be creative in the agenda on financial inclusion. Ghana's innovative 3-tiered KYC system is to ensure that everyone in the financial pyramid and certainly, at the bottom of the pyramid, can be roped into the formal financial system and can transact under a risk-based regime structured around maximum balances, daily and monthly transaction levels."*
>
> Elly Ohene-Adu (2015), Head of Banking Services & Payment Systems Oversight, Bank of Ghana[82]

Most mobile money service providers have different tiers of accounts based on proportional CDD:

- **Simplified CDD:** Used when risks are lower and controls tighter (i.e. limits on transaction values and frequency). For example, KYC may be based on the information provided at SIM registration (see Box 5) or through alternative methods of identity verification when national IDs are not available.
- **Full CDD:** Used when a customer can utilise all the features of an account with higher value and frequency limits.
- **Enhanced CDD:** Used when greater KYC is required, such as for customers with a higher risk profile (such as politically exposed persons).

BOX 5

MANDATORY SIM CARD REGISTRATION FOR PREPAID USERS[83]

Mandatory [SIM card] registration for prepaid users emerged after the introduction of registration requirements in Brazil, Germany, and Switzerland in 2003. Since then, an increasing number of governments have introduced mandatory registration requirements, prohibiting mobile operators from selling or activating prepaid SIM cards unless the purchaser presents a proof of identity and registers the SIM in their real name. As of July 2013, at least 80 countries globally (including 37 on the African continent) have mandated, or are actively considering mandating, the registration of prepaid SIM users.

81. Recently a number of countries have begun to permit low-value cross-border transfers via mobile wallets for the first time. See, e.g., Scharwatt & Williamson (2015), "Mobile money crosses borders: New remittance models in West Africa." GSMA MMU, London. In addition, the Alliance for Financial Inclusion has identified a number of issues regulators are addressing in countries where cross-border wallet-to-wallet services have been launched or are under consideration. These include harmonisation of AML/CFT requirements between different countries and compliance with cross-border KYC and record-keeping requirements, among others. See Alliance for Financial Inclusion, Mobile Financial Services: Mobile-Enabled Cross-Border Payments, Guideline Note No. 14.
82. Conversation with the authors of the paper, June 2015
83. This text is excerpted from GSMA (2013), "The Mandatory Registration of Prepaid SIM Card Users", GSMA white paper, London.

It should be noted that the FATF does not specify the exact information to be collected in the CDD process. In general, providers are required to (1) identify customers and verify their identity using reliable, independent documents or information; (2) understand the purpose of the business relationship; and (3) conduct ongoing due diligence of the business relationship.[84] The FATF therefore endorses a risk-based approach and recognises that simplified CDD may be appropriate in lower risk scenarios, such as when services with appropriate limits are offered to increase financial inclusion.[85] Providers typically record the customer's name, date of birth, address and mobile phone number, even in non-face-to-face (remote opening) scenarios where the customer is given a basic account with limited functionality until face-to-face verification is carried out.

Table 8 provides examples of tiered approaches for electronic money or mobile money services in select countries. Box 6 describes tiered approaches in Mexico and Pakistan, two countries that only permit banks to offer low-value transactional accounts.

TABLE 8

TRANSACTION AND BALANCE LIMITS FOR ELECTRONIC MONEY/MOBILE MONEY SERVICES IN SELECT COUNTRIES (IN USD)

Country		Single transaction limit (P2P)	Daily limit	Monthly limit	Annual limit	Maximum account balance
Fiji		None specified, although providers may wish to establish limits for accounts opened with only a 'referee letter' to fulfil the identification requirements. Mobile money provider Digicel has established the following limits:				
		$566	$5,666			
Ghana	***OTC (no ID)****	$48	$119	$597		
	OTC (with ID)**	$119	$477	$4,774		
	Minimum KYC		$72	$716		$239
	Medium KYC		$477	$4,774		$2,387
	Enhanced KYC		$1,194	$11,936		$4,774
Liberia	***OTC***	$100				
	Level 1		$250	$2,000		$1,000
	Level 2		$1,000	$8,000		$4,000
	Level 3		$2,000	$20,000		$10,000
Russia	***No KYC***	N/A (P2P prohibited)	$95 (withdrawals only)	$755		$285
	Simplified KYC	$285		$3,775		$1,135
	Full KYC	$11,350				$11,350
Philippines				$2,430		
Sri Lanka		No pre-set limits; the regulation requires providers to submit proposed limits for Central Bank approval. The following limits were approved for mobile money provider Dialog:				
	Dialog Basic Account	$40				$80
	Dialog Power Account	$40 for P2P, $200 for utility payment				$200

* OTC clients who lack acceptable ID must be introduced by someone with acceptable ID.
** "Acceptable ID" requirements for OTC clients are equivalent to KYC requirements for Medium KYC accounts. Minimum KYC accounts can be opened with any photo ID, while Medium KYC accounts may only be opened with a national ID, voter ID, national health insurance ID, driver's licence, or passport.

84. Financial Inclusion Guidance (2013), para. 65.
85. Financial Inclusion Guidance (2013), para. 68-74.

BOX 6
TIERED KYC FOR BANK-BASED DIGITAL FINANCIAL SERVICES

A number of countries promoting financial inclusion through tiered KYC only allow banks or similar institutions to offer mobile financial services. For example, in Mexico, both regular banks and smaller banks with lower capital requirements ("bancos nichos") can offer tiered electronic accounts. Similarly, in Pakistan, commercial banks and microfinance banks are permitted to offer branchless banking services with various tiers depending on the level of KYC performed.

Country		Single transaction limit (P2P)	Daily limit (USD)	Monthly limit (USD)	Annual limit (USD)	Maximum account balance (USD)
Mexico	Level 1			$251		
	Level 2			$1,007		
	Level 3			$3,357		
	Level 4			No limit		
Pakistan	Level 0		$147	$245	$1,176	$980
	Level 1		$245	$588	$4,902	No limit
	Level 2	Established by bank considering customer profile and bank's monitoring capacity				
	Level 3	Established by bank considering customer profile and bank's monitoring capacity				

5.2 Mobile money ML and TF risk before and after mitigation measures are applied

The next two tables consider mitigation measures in the context of an RBA to help both regulators and providers assess how CDD and other controls can be applied proportionately. The risk matrix in Table 9 is based on Table 1 of the 2013 NPPS Guidance, with additional information on mobile money-specific risk mitigation measures.[86] As the FATF points out, *"although the risk matrix applies fully for NPPS, the nature and functionality of the NPPS can vary considerably in comparison to other payment instruments (e.g. credit and debit cards), and product[s] can be tailored in different ways to allow for different uses. For this reason, the risk assessment of NPPS should be developed on a case-by-case basis, taking into consideration the specific features of the single product."*[87]

The NPPS Guidance also notes that those evaluating the risk of a specific product should take a holistic approach. Rather than considering each risk factor in isolation, parties should consider the risks, risk mitigants, and functionality of a particular product.[88] In the case of mobile money services, for example, those evaluating the risk of a particular mobile money service should consider not only the strength of CDD, but also any limits on functionality (such as transaction and balance limits) and other risk mitigation measures, such as electronic transaction monitoring systems (see Table 10).

Table 9 compares the relative risks of cash and mobile money and shows how mobile money providers can effectively mitigate the different risks identified by the FATF. While mobile money services also pose risks, most are lower than the risks of cash-based transactions once proper risk mitigation measures have been implemented.

86. See Table 1.
87. FATF (2013c), 18.
88. FATF (2013c), 18.

TABLE 9

MOBILE MONEY SERVICES RISK MATRIX

Criteria		Risk factor	Cash risk mitigation measures		Mobile money (following implementation of risk mitigation measures)	
CDD	Identification	Anonymity	None (anonymous)	***	Customers are identified.	*
	Verification	Anonymity	None (anonymous)	***	A certain level of verification is always conducted, except in countries that allow account opening without verification for accounts with very low transaction and balance limits. For accounts with greater functionality, customer identity is generally verified using reliable, independent source documents, data, or information. The strength of verification measures increases as the risk increases (risk-based approach).	*
	Monitoring	Lack of oversight	None	***	Ongoing monitoring of business relationships.	*
Record keeping		Not traceable	None, except for cross-border declarations	***	Electronic transaction records are retained and made accessible to law enforcement agencies upon request.	*
Value limits	Maximum amount stored on account / accounts per person	No limitations	None, except for cross-border declarations	***	Specific balance limits within the system. The system will not allow balances to exceed built-in thresholds.	*
	Maximum amount per transaction (incl. loading / withdrawal transactions)	No limitations	None	***	Transaction limits. The system will not allow transactions above built-in thresholds.	*
	Maximum transaction frequency	No limitations	None	***	Transaction limits. The system will not allow transactions that exceed the built-in thresholds.	*
Methods of funding		Anonymity	n/a	***	Funding can originate from anonymous sources like cash and from accounts held at regulated institutions. The risk will increase if the account holder was not properly identified.	**
Geographical limits		Elusiveness	Currency that is not universally accepted can be converted via intermediaries	**	Historically, mobile money services have tended to operate within national borders. Recently, however, a number of providers have begun to offer wallet-to-wallet transfers across borders. Mobile money transactions are clearly traceable in a mobile operator's system as part of standard business practice. Telephone number of the sender and receiver, the time, and transaction amount are all known to the mobile money provider.	**

Criteria		Risk factor	Cash risk mitigation measures		Mobile money (following implementation of risk mitigation measures)	
Usage limits	Negotiability (merchant acceptance)	Anonymity	Generally accepted	***	Merchant acceptance is still limited. In future, this risk may increase as merchant acceptance of mobile money increases. Mobile money providers can mitigate risks by monitoring and tracking mobile money transactions and by conducting enhanced due diligence on merchants.	**
	Utility	Anonymity, Rapidity	P2B, B2B, P2P, no online usage possible, limited rapidity	**	Mobile money allows funds to be transferred rapidly, but setting transaction and balance limits can mitigate this risk. In emerging markets, the average value of a P2P mobile money transaction as of December 2014 was USD 45.	**
	Withdrawal	Anonymity	n/a	***	Limits on transactions and limits on the value of withdrawals.	*
Segmentation of services	Interaction of service providers	Lack of oversight	n/a		For most mobile money services today, the entire transaction is carried out by one service provider. As digital financial services grow, multiple service providers will need to coordinate to ensure transactions are conducted properly and subjected to effective oversight.	**
	Outsourcing	Lack of oversight	n/a		For mobile money to develop in emerging markets, providers must be allowed to use agents and other entities for customer registration and activation, and to conduct cash-in and cash-out operations. Risks from outsourcing can be mitigated by holding the service provider responsible for KYC compliance and other regulatory compliance. Agents are typically trained and monitored to mitigate the risk of abuse.	**

KEY:

*** INDICATES ML/TF RISK IS HIGH

** INDICATES ML/TF RISK IS MEDIUM

* INDICATES ML/TF RISK IS LOW

CDD = CUSTOMER DUE DILIGENCE
KYC = KNOW YOUR CUSTOMER
P2P = PERSON-TO-PERSON

SOURCES: FATF (2013), NPPS GUIDANCE; AUTHORS.

Table 10 takes a closer look at specific opportunities for ML/TF-related crime in the mobile money ecosystem. It identifies various types of abuse based on the different stakeholders in the mobile money ecosystem and assesses the vulnerability of mobile money to each type of abuse, both before and after effective mitigation measures are in place. All identified risks can be significantly reduced through effective internal controls. Technological solutions and good internal controls can significantly mitigate the risks, although certain risks (particularly those related to human activity) cannot be eliminated completely.

TABLE 10

HOW ML/TF RISKS CAN BE MITIGATED

Typology	Vulnerability before mitigation	Mitigation and comments	Vulnerability after effective mitigation
ML/TF by consumer			
Fraudulent registration	**	Systems should be calibrated to detect fraudulent activity. Account monitoring systems can detect activity that seems abnormal compared to the typical behaviour of similar users in a given area. By implementing controls in other parts of the system (strict limits on value and functionality, monitoring, etc.), the risk of fraudulent registration should decrease because the system would be less attractive to criminal interests.	*
Multiple registrations	**	The number of accounts that can be held by one person is limited in many countries. SIM card registration reveals the identity of the SIM card owner and indicates whether the owner has more than one SIM card and, therefore, several mobile accounts.	*
Transfer of service after registration	**	This is a challenge with all financial services, but mobile services offer a better chance of detection because automated controls are in place to flag and/or freeze highly irregular activities. The ID requirement for transactions over a certain limit and PIN and password authentication may reduce this risk.	*
Loading with POC	**	Systems typically look for such anomalies. Services are designed to be less attractive as a channel for laundering funds: there are limits on the functionality of the mobile wallet (such as the frequency and value of transactions and maximum balance), and there are monitoring systems that track transaction flows, alerting the mobile money provider to suspicious transaction patterns. These measures reinforce each other because transaction limits force criminals and terrorists to split a transaction into several smaller ones, which would risk detection by the monitoring system. If customers wish to conduct larger transactions with high frequency, they should be obliged to submit to enhanced CDD. Mobile money services have built-in systems to prevent transactions that breach account limits and to flag unusual activity. Providers scan transactions in real time and have trained staff to identify suspicious transactions and trends. The ability to locate a mobile device and identify the registered user through the MSISDN and IMSI is an additional tool for law enforcement not available for other formal, non-mobile financial services. Agents are obligated to refuse a transaction if the transaction would breach account limits, if they cannot verify the source of funds, or if the transaction is suspicious. PIN or password authentication is required to verify the registered user of a mobile device is the person conducting the transaction on the mobile device.	*
Use of POC to purchase from sellers	**	Systems and processes will need to look for these anomalies. As noted above, most mobile money services are less prone to this type of abuse by design; transacted values are typically small and unusually high transactions would risk detection. If providers offer the ability to routinely make larger payments, systems should be designed to detect anomalous transactions that do not make economic sense.	*

Typology	Vulnerability before mitigation	Mitigation and comments	Vulnerability after effective mitigation
POC transferred to co-conspirators	**	Systems to detect anomalies will need to be put in place to monitor suspicious activities and trends. Account balance limits make this more difficult, as the POC would need to be split amongst a large number of mobile money accounts.	*
POC pooled into single account	**	Systems to detect anomalies will need to be put in place. Coupled with stringent account limits, mobile money monitoring systems are more likely to identify criminal transactions than with cash-based transactions. Monitoring systems will flag a single account receiving funds from several accounts, particularly when this does not fit the economic rationale. Account balance limits also make this more difficult, as the POC would need to be split amongst multiple mobile money accounts.	*
Withdrawal of POC by cash redemption	**	Mobile money monitoring systems can detect anomalous withdrawals. Account balance limits also make this more difficult, as the POC would need to be split amongst multiple mobile money accounts, forcing an individual to withdraw funds from an agent many times. This would likely be flagged.	*
Funds transfer to/from a person linked to terrorism	**	Known terrorists and terrorist financiers can be instantly and automatically screened by the system using international and domestic lists provided by the regulator. If a transaction is detected that could be linked to such individuals, providers freeze the matched accounts immediately and flag them for law enforcement. This is a strong deterrent.	*
ML/TF by merchant			
Complicit merchant receives POC	**	DD is an essential gateway measure when merchants are first signed up, and ongoing DD must be applied over time. Systems to detect anomalies with merchant transactions and the class of merchant are also necessary. Mystery shopping is an effective way to test the integrity of a merchant.	*
Fraudulent merchant misappropriates funds	**	Fraud cannot be entirely excluded, but sound DD processes in the initial stages and ongoing transaction monitoring should both help to reduce risk.	*
ML/TF by employee			
Fraudulent registration of false accounts to facilitate ML/TF	***	While the potential for internal fraud is always a concern, providers can take a number of measures to mitigate this risk, such as: • Initial and ongoing staff due diligence • Cross-referencing internal staff details against customer/ merchant/agent account details to identify possible collusion. • Segregation of duties and access controls • Strong user authentication mechanisms • Full system audit trails • Transaction monitoring to identify suspicious activity • Employee disciplinary policy • Periodic verification of customer account information	**

Typology	Vulnerability before mitigation	Mitigation and comments	Vulnerability after effective mitigation
Theft of funds using internal access (e.g. false transactions, creation of e-money without depositing corresponding funds, theft from dormant accounts)	***	While the potential for internal fraud is always a concern, providers can take a number of measures to mitigate this risk, such as: • Initial and ongoing staff due diligence • Cross-referencing internal staff details against customer/merchant/agent account details to identify possible collusion. • Segregation of duties and access controls • Strong user authentication mechanisms • Full system audit trails • Transaction monitoring to identify suspicious activity • Employee disciplinary policy • Regular reconciliation of outstanding e-money liabilities and funds kept to repay users	**
Allows known POC funds to be loaded on or withdrawn from account	***	Initial and ongoing staff due diligence can mitigate the risk of staff involvement in ML/TF. Transaction monitoring system should be able to identify suspicious activity, including smurfing, transactions inconsistent with prior behaviour, transfer of funds to/from high-risk areas, transfer of funds to/from previously dormant accounts, employee activity on customer/merchant/agent accounts, etc.	**
Allows customers to exceed load or withdrawal limits	***	Initial and ongoing staff due diligence can mitigate the risk of staff involvement in ML/TF. Audit trails record all cases of internal approval to override established limits (or to assign customer to a higher tier account) and identify the employee(s) responsible for such approval.	**
ML/TF by agent or retail partner			
Allows known POC to be loaded on or withdrawn from account	***	This is a vulnerable part of the payment chain and additional attention needs to be given to agents. Fit and proper criteria for agent selection (such as background checks) are important, as are enhanced due diligence, ongoing transaction reviews (including agent activity on customer/merchant/agent accounts), and periodic audits or on-site inspections. For instance, mystery shoppers can be used to test the integrity of an agent's operations. Blacklists of individuals not suited to serve as agents can be kept by the regulator and shared with all providers.	**
Agent does not fulfil due diligence obligations, intentionally or negligently	***	This is a vulnerable part of the payment chain and additional attention needs to be given to agents. Fit and proper criteria for agent selection (such as background checks) are important, as are enhanced due diligence, ongoing transaction reviews (including agent activity on customer/merchant/agent accounts), and periodic audits or on-site inspections. For instance, mystery shoppers can be used to test the integrity of an agent's operations. Blacklists of individuals not suited to serve as agents can be kept by the regulator and shared with all providers.	**
Agent allows customers to exceed load or withdrawal limits	**	System should prevent this and record incidents for follow up. Provider can implement measures to deter abuse by agents (such as using mystery shoppers) and conduct spot on-site inspections. Blacklists of individuals not suited to serve as agents can be kept by the regulator and shared with all providers.	*

KEY:

*** INDICATES ML/TF RISK IS HIGH

** INDICATES ML/TF RISK IS MEDIUM

* INDICATES ML/TF RISK IS LOW

POC = PROCEEDS OF CRIME
DD = DUE DILIGENCE
ML = MONEY LAUNDERING

A number of country case studies are included as Annex 3. These case studies provide examples of how regulators and mobile money providers have mitigated the risk of ML/TF in practice.

Conclusion

By linking the risk control measures identified in the GSMA survey to our initial analysis of the comparative risks of mobile payments and cash, general conclusions can be drawn about the degree of risk posed by mobile money services. Table 11 below shows how mobile money providers are mitigating AML/CFT risks using a variety of controls. Comparing risks between mobile money and cash transactions is particularly meaningful since cash is the main alternative to mobile money services in most emerging and developing markets. Mobile money services can be designed to strengthen financial integrity by using appropriate risk controls to mitigate the risk of money laundering and terrorist financing, while cash-based services generally remain anonymous and are difficult or impossible to trace.

TABLE 11

THE RISKS OF CASH AND MOBILE MONEY BEFORE AND AFTER AML/CFT CONTROLS ARE APPLIED

Risk factor	Mobile money			Cash	
	Before	Controls	After		
Anonymity: Customer's identity is unknown	**	• Transactions linked to a unique mobile number • Transactions recorded (sender's mobile number, amount, receiver's mobile number, date) • Transactions traced • CDD and customer profile building	*	***	• It's anonymous • There is neither a unique identifier for the user nor a way to trace the payment
Elusiveness: Ability to disguise amount, origin, and destination	**	• Mobile money transactions are clearly traceable in the mobile money provider's system as part of standard business practice • Mobile number of the sender and receiver, the time, and the amount of the transaction are all known to the mobile money provider • Limits on maximum balance and on amount, frequency and number of transactions • Real-time monitoring	*	***	• Elusive
Rapidity	***	• Real-time monitoring • Restrictions on transaction frequency • Restrictions on transaction amount and total account turnover in a given period	**	*	• Slower than mobile money
Lack of oversight or poor oversight	**	• Mobile money providers are properly regulated and supervised • MNOs put in place strict internal controls with regular internal and external auditing	*	***	• None: cash transactions lack oversight

KEY:

*** INDICATES ML/TF RISK IS HIGHLY PREVALENT

** INDICATES ML/TF RISK IS SOMEWHAT PREVALENT

* INDICATES ML/TF RISK IS LOW

Mobile money reduces dependency on cash, generates data on transactions and customers that can be shared with law enforcement, and helps to meet both financial integrity and financial inclusion objectives. The GSMA's survey found that MNOs offering mobile money services are regulated with respect to AML/CFT and are complying with AML/CFT requirements. Mobile money shifts a large proportion of low-value cash transactions to the digital platform, offering the potential for better monitoring and the ability to disrupt criminal activities. The data obtained from mobile money transactions covers the entire transaction value chain, which is useful for monitoring and tracing illegal proceeds.

In short, the benefits of mobile money outweigh the risk of abuse. This is not to say that mobile money services will never be exploited, but there is a better chance of detecting suspicious transactions and tracing criminal proceeds through electronic transactions than cash-based transactions. In addition, it is important to remember that AML/CFT regimes are not intended to prevent law-abiding people from accessing formal financial services; rather, they detect and deter criminals seeking to abuse the financial sector for money laundering or terrorist financing. Mobile money services can contribute both to financial integrity and financial inclusion if regulation is proportional and providers apply proper risk mitigation measures.

The evidence to date suggests that proportional regulatory frameworks and industry-led mitigation measures have made mobile money a relatively unattractive channel for ML/TF. Nevertheless, mobile money providers should continue to develop and adopt best practices to prevent the abuse of mobile money services. Collaboration between the public and private sectors, with a common goal of fighting crime, is an indicator of a strong AML/CFT regime. While effective AML/CFT measures must be implemented, cumbersome requirements reduce customer activation and threaten the viability of the business model. At the global level, the FATF regularly consults with private sector stakeholders (including the GSMA) to ensure the perspective of mobile money service providers is considered. At the country level, regulators and policymakers equally committed to financial inclusion and financial integrity would benefit from consulting with mobile money service providers and informing their decisions with insights and data from the industry.

Annex 1: Excerpts from the FATF Recommendations 2012

RECOMMENDATION 1. ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

RECOMMENDATION 10. CUSTOMER DUE DILIGENCE

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

i. establishing business relations;

ii. carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

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

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

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

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

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

c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

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

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

- Non face-to-face business.

. . .

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

. . .

- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

. . .

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).

- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

RECOMMENDATION 11. RECORD-KEEPING

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

RECOMMENDATION 14. MONEY OR VALUE TRANSFER SERVICES

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

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

RECOMMENDATION 15. NEW TECHNOLOGIES

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

RECOMMENDATION 16. WIRE TRANSFERS

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

RECOMMENDATION 18. INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

RECOMMENDATION 20. REPORTING OF SUSPICIOUS TRANSACTIONS

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

RECOMMENDATION 26. REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution.

Countries should not approve the establishment, or continued operation, of shell banks. For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes. Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

RECOMMENDATION 34. GUIDANCE AND FEEDBACK

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

Annex 2: Survey results

Below is a summary of the results of the GSMA's survey of mobile money providers. In a few cases, data has been omitted to ensure confidentiality.

Q1 What AML/CFT-related measures do you take to screen prospective STAFF (select all that apply)?

Answer Choices	Responses	
1. Criminal background checks	**75.68%**	28
2. None	**10.81%**	4
Other (please specify)	**29.73%**	11
Total Respondents: 37		

Q2 What AML/CFT-related measures do you take to screen prospective INDIVIDUAL AGENTS (select all that apply)?

Answer Choices	Responses	
Checking domestic and/or international watch lists (for money laundering, terrorist financing, fraud, or other sanctioned activities)	**70.27%**	26
Identification of business owner	**86.49%**	32
Criminal background checks on business owner	**18.92%**	7
Criminal background checks on staff	**16.22%**	6
Obtaining copies of business registration documents	**81.08%**	30
None	**0.00%**	0
We don't use individual agents	**2.70%**	1
Other (please specify)	**10.81%**	4
Total Respondents: 37		

Q3 What AML/CFT-related measures do you take to screen prospective MASTER AGENTS OR AGENT NETWORK MANAGERS (select all that apply)?

Answer Choices	Responses	
Checking domestic and/or international watch lists (for money laundering, terrorist financing, fraud, or other sanctioned activities)	**70.27%**	26
Identification of owners and senior management	**81.08%**	30
Identification of beneficial owners and controllers	**56.76%**	21
Criminal background checks on owners and senior management	**16.22%**	6
Criminal background checks on beneficial owners and controllers	**13.51%**	5
Obtaining copies of business registration documents	**86.49%**	32
None	**0.00%**	0
We don't use master agents or agent network managers	**5.41%**	2
Other (please specify)	**13.51%**	5
Total Respondents: 37		

Q4 What measures do you take to train STAFF regarding AML/CFT procedures and requirements (select all that apply)?

Answer Choices	Responses	
Responsibility of provider and individual staff for AML/CFT compliance and suspicious transaction reporting	**85.71%**	30
Provider's policies and procedures and the role of staff with respect with to these policies and procedures	**82.86%**	29
Relevant emerging risks and trends in ML/TF	**45.71%**	16
How to conduct proper CDD when registering new clients	**74.29%**	26
Proper record-keeping procedures	**68.57%**	24
How to identify and report suspicious activity without "tipping off"	**65.71%**	23
How to communicate with agents	**40.00%**	14
How to monitor agent compliance with AML/CFT requirements	**71.43%**	25
None	**2.86%**	1
Other (please specify)	**2.86%**	1
Total Respondents: 35		

Q5 What measures do you take to train INDIVIDUAL AGENTS regarding AML/CFT procedures and requirements (select all that apply)?

Answer Choices	Responses	
Provider's policies and procedures and the role of staff with respect to these policies and procedures	**65.71%**	23
Relevant emerging risks and trends in ML/TF	**40.00%**	14
How to conduct proper CDD when registering new clients	**68.57%**	24
Proper record-keeping procedures	**65.71%**	23
How to identify and report suspicious activity without "tipping off"	**65.71%**	23
None	**5.71%**	2
We don't use individual agents	**2.86%**	1
Other (please specify)	**8.57%**	3
Total Respondents: 35		

Q6 What measures do you take to train MASTER AGENTS OR AGENT NETWORK MANAGERS regarding AML/CFT procedures and requirements (select all that apply)?

Answer Choices	Responses	
Provider's policies and procedures and the role of staff with respect to these policies and procedures	**62.86%**	22
Relevant emerging risks and trends in ML/TF	**37.14%**	13
How to conduct proper CDD when registering new clients	**57.14%**	20
Proper record-keeping procedures	**54.29%**	19
How to identify and report suspicious activity without "tipping off"	**54.29%**	19
None	**11.43%**	4
We don't use master agents or agent network managers	**5.71%**	2
Other (please specify)	**5.71%**	2
Total Respondents: 35		

Q7 How often do you train STAFF AND AGENTS on AML/CFT procedures and requirements (select all that apply)?

	Beginning of service	Quarterly	Annually	Other (please describe below)	Total Respondents
Staff	**60.00%** 21	**2.86%** 1	**71.43%** 25	**11.43%** 4	35
Individual agents	**69.70%** 23	**27.27%** 9	**39.39%** 13	**12.12%** 4	33
Master agents or agent network managers	**68.75%** 22	**21.88%** 7	**43.75%** 14	**15.63%** 5	32
Total Respondents: 35					

Q8 What measures do you take to monitor STAFF compliance with AML/CFT procedures and requirements (select all that apply)?

Answer Choices	Responses	
Testing understanding of policies, procedures, and legal obligations	**62.86%**	22
Regularly reviewing records and transaction audit trails to assess the quality of staff compliance with AML/CFT requirements	**80.00%**	28
None	**2.86%**	1
Other (please specify)	**5.71%**	2
Total Respondents: 35		

Q9 What measures do you take to monitor INDIVIDUAL AGENT compliance with AML/CFT procedures and requirements (select all that apply)?

Answer Choices	Responses	
Testing understanding of policies, procedures, and legal obligations	**37.14%**	13
Regularly reviewing records and transaction audit trails to assess the quality of agent compliance with AML/CFT requirements	**74.29%**	26
On-site and off-site audits	**45.71%**	16
None	**5.71%**	2
We don't use individual agents	**2.86%**	1
Other (please specify)	**14.29%**	5
Total Respondents: 35		

Q10 What measures do you take to monitor MASTER AGENT OR AGENT NETWORK MANAGER compliance with AML/CFT procedures and requirements (select all that apply)?

Answer Choices	Responses	
Testing understanding of policies, procedures, and legal obligations	**28.57%**	10
Regularly reviewing records and transaction audit trails to assess the quality of agent compliance with AML/CFT requirements	**62.86%**	22
On-site and off-site audits	**37.14%**	13
None	**11.43%**	4
We don't use master agents or agent network managers	**8.57%**	3
Other (please specify)	**11.43%**	4
Total Respondents: 35		

Q11 Which watch lists do you use to screen customers and agents with respect to money laundering, terrorist financing, and sanctions (select all that apply)?

Answer Choices	Responses	
Domestic list provided by financial regulator	**42.86%**	15
Domestic list provided by another party (please describe in box below)	**14.29%**	5
Consolidated United Nations Security Council Sanctions List (UN)	**40.00%**	14
US Office of Foreign Assets Control's Specially Designated Nationals List (US OFAC)	**60.00%**	21
Consolidated List of Persons, Groups and Entities subject to EU Financial Sanctions (EU)	**25.71%**	9
None	**11.43%**	4
Other international list (please describe in box below)	**20.00%**	7
Total Respondents: 35		

Q12 When do you screen customers and agents (select all that apply)?

	Upon registration	On a regular basis (quarterly, annually, etc.) (please describe in box below)	If unusual or suspicious transactions are detected	Never	Other (please describe in box below)	Total Respondents
Customers	**71.43%** 25	**37.14%** 13	**42.86%** 15	**5.71%** 2	**5.71%** 2	35
Individual agents	**72.73%** 24	**33.33%** 11	**42.42%** 14	**3.03%** 1	**6.06%** 2	33
Master agents or agent network managers	**73.33%** 22	**30.00%** 9	**40.00%** 12	**3.33%** 1	**6.67%** 2	30
Total Respondents: 35						

Q13 What is the name of your transaction monitoring system, and who is the provider?

answers omitted to maintain confidentiality

Q14 What methods are used to monitor transactions by customers, agents, and staff (select all that apply)?

Answer Choices	Responses	
Identification of potentially suspicious transactions (e.g. unusual account opening, termination, or changes to accounts; smurfing; changes in the velocity of transactions; transfer of funds to/from previously dormant accounts).	**80.00%**	28
Behaviour profiling (transaction analysis to develop unique behaviour profiles for customers and agents).	**62.86%**	22
Geographic validation (identification of suspicious behaviour such as agents operating outside their area, transactions to/from suspicious locations, or transactions by an agent when the customer is not at the agent location).	**28.57%**	10
Transaction logging (all transactions are logged with audit trails that allow reconstruction of transactions and record any attempts to modify transaction information)	**60.00%**	21
Internal monitoring (monitoring internal logs and employee activity to ensure that system access is limited to authorised individuals during normal business hours and that their activity is appropriate).	**77.14%**	27
None	**0.00%**	0
Other (please specify)	**5.71%**	2
Total Respondents: 35		

Q15 Do you report suspicious transactions to a financial intelligence unit or similar responsible entity?

Answer Choices	Responses	
Yes (please describe in box below)	**80.00%**	28
No	**20.00%**	7
Total Respondents: 35		

Q16 In what form(s) are ACCOUNT OPENING records stored at agents and providers?

	Paper	Electronic	Both	Transaction records not stored	Total Respondents
Agents	**27.27%** 9	**9.09%** 3	**57.58%** 19	**6.06%** 2	33
Providers	**29.03%** 9	**12.90%** 4	**54.84%** 17	**3.23%** 1	31
Total Respondents: 34					

Q17 In what form(s) are TRANSACTION records stored at agents and providers?

	Paper	Electronic	Both	Transaction records not stored	Total Respondents
Agents	**15.15%** 5	**42.42%** 14	**39.39%** 13	**6.06%** 2	33
Providers	**3.33%** 1	**53.33%** 16	**43.33%** 13	**3.33%** 1	30
Total Respondents: 34					

Q18 Are you permitted to store all records in electronic form without paper copies, or are you required to keep paper

Answer Choices	Responses	
Records can be stored in electronic form without paper copies	**50.00%**	17
Paper records must be kept	**50.00%**	17
Total Respondents: 34		

Q19 For how many years must you keep account opening and transaction records?

too many answers to summarise

Q20 Please list the types of mobile money accounts/services that you offer.

Answer Choices	Responses	
Over-the-counter (OTC) services (services conducted at an agent without an account)	**48.48%**	16
Accounts with SIMPLIFIED KYC requirements and lower transaction and/or balance limits	**63.64%**	21
Accounts with REGULAR KYC requirements and transaction and/or balance limits	**72.73%**	24
Accounts with ENHANCED KYC requirements (for political exposed persons or other accounts with higher transaction and/or balance limits)	**45.45%**	15
Other (please specify)	**3.03%**	1
Total Respondents: 33		

Q21 What are the transaction and geographic limits for OVER THE COUNTER transactions (answer all that apply)?

Answer Choices	Responses	
Per transaction (US Dollars)	**95.00%**	19
Per day (US Dollars)	**85.00%**	17
Per month (US Dollars)	**75.00%**	15
Per year (US Dollars)	**65.00%**	13
Only domestic transactions permitted (yes/no)?	**85.00%**	17
Total Respondents: 20		

Q22 What are the transaction, balance, geographic, and number of account limits for accounts with SIMPLIFIED KYC (answer all that apply)?

Answer Choices	Responses	
Per transaction (US dollars)	**100.00%**	19
Per day (US dollars)	**89.47%**	17
Per month (US dollars)	**89.47%**	17
Per year (US dollars)	**73.68%**	14
Maximum balance held on account (US dollars)	**78.95%**	15
Only domestic transactions permitted (yes/no)?	**94.74%**	18
Limit of one account per person (yes/no)?	**94.74%**	18
Total Respondents: 19		

Q23 What are the transaction, balance, geographic, and number of account limits for accounts with REGULAR KYC (answer all that apply)?

Answer Choices	Responses	
Per transaction (US dollars)	**90.00%**	18
Per day (US dollars)	**85.00%**	17
Per month (US dollars)	**75.00%**	15
Per year (US dollars)	**55.00%**	11
Maximum balance held on account (US dollars)	**70.00%**	14
Only domestic transactions permitted (yes/no)?	**80.00%**	16
Limit of one account per person (yes/no)?	**85.00%**	17
Total Respondents: 20		

Q24 What are the transaction, balance, geographic, and number of account limits for accounts with ENHANCED KYC (answer all that apply)?

Answer Choices	Responses	
Per transaction (US dollars)	**85.71%**	12
Per day (US dollars)	**78.57%**	11
Per month (US dollars)	**78.57%**	11
Per year (US dollars)	**64.29%**	9
Maximum balance held on account (US dollars)	**64.29%**	9
Only domestic transactions permitted (yes/no)?	**85.71%**	12
Limit of one account per person (yes/no)?	**85.71%**	12
Total Respondents: 14		

Q25 For over-the-counter transactions, what customer identity information must be recorded (select all that apply)?

Answer Choices	Responses	
Name	**91.30%**	21
Date of birth	**56.52%**	13
Place of birth	**26.09%**	6
Mobile phone number	**86.96%**	20
SIM number	**8.70%**	2
Photograph of customer	**13.04%**	3
National registration/ID number	**78.26%**	18
Current residential address	**34.78%**	8
None	**4.35%**	1
Other (please specify)	**4.35%**	1
Total Respondents: 23		

Q26 For over-the-counter transactions, which documents may be used to verify customer identity (select all that apply)?

Answer Choices	Responses	
National ID	**90.91%**	20
Social security card	**13.64%**	3
Driver's licence	**45.45%**	10
Passport	**63.64%**	14
Voting card	**27.27%**	6
Employee ID	**9.09%**	2
Student ID	**13.64%**	3
Salary slip	**0.00%**	0
Tax report	**4.55%**	1
Other government-issued ID	**18.18%**	4
Biometrics (e.g., fingerprint, retina scan)	**0.00%**	0
Attestation letter from local government official or person of appropriate standing in the community, such as a village chief	**4.55%**	1
None required	**4.55%**	1
Other (please specify)	**0.00%**	0
Total Respondents: 22		

Q27 For over-the-counter transactions, what procedures are required to verify the information provided (select all that apply)?

Answer Choices	Responses	
Basic system validation (e.g. date of birth is a valid date, all fields completed)	**47.62%**	10
Cross-checking against ID records held in mobile money system	**33.33%**	7
Verification with the ID-issuing authorities or a central database	**28.57%**	6
None required	**28.57%**	6
Other (please specify)	**0.00%**	0
Total Respondents: 21		

Q28 For each type of account, please indicate whether customers can open an account at an agent or remotely via mobile phone (select all that apply)

	Can open account at agent	Can open account remotely via mobile phone	None of the above	Total Respondents
Accounts with SIMPLIFIED KYC	**66.67%** 18	**44.44%** 12	**14.81%** 4	27
Accounts with REGULAR KYC	**84.62%** 22	**15.38%** 4	**7.69%** 2	26
Accounts with ENHANCED KYC	**57.14%** 12	**14.29%** 3	**33.33%** 7	21
Total Respondents: 32				

Q29 When opening a mobile money account, what customer identity information must be recorded (select all that apply)?

	Accounts with SIMPLIFIED KYC	Accounts with REGULAR KYC	Accounts with ENHANCED KYC
Name	**96.00%** 24	**88.89%** 24	**85.71%** 18
Name of beneficial owner	**32.00%** 8	**37.04%** 10	**57.14%** 12
Date of birth	**92.00%** 23	**88.89%** 24	**85.71%** 18
Place of birth	**40.00%** 10	**55.56%** 15	**57.14%** 12
Mobile phone number	**96.00%** 24	**100.00%** 27	**95.24%** 20
SIM number	**16.00%** 4	**25.93%** 7	**28.57%** 6
Photograph of customer	**20.00%** 5	**33.33%** 9	**38.10%** 8
National registration/ID number	**76.00%** 19	**92.59%** 25	**90.48%** 19
Business ID number	**8.00%** 2	**14.81%** 4	**28.57%** 6
Current residential address	**56.00%** 14	**62.96%** 17	**71.43%** 15
Current business address	**8.00%** 2	**14.81%** 4	**33.33%** 7
None	**0.00%** 0	**0.00%** 0	**4.76%** 1
Other (please describe in box below)	**12.00%** 3	**7.41%** 2	**9.52%** 2
Total Respondents	**25**	27	21

Total Respondents: 32

Q30 When opening a mobile money account, which documents may be used to verify customer identity (select all that apply)?

	Accounts with SIMPLIFIED KYC	Accounts with REGULAR KYC	Accounts with ENHANCED KYC
National ID	**80.77%** 21	**100.00%** 27	**90.91%** 20
Social security card	**19.23%** 5	**22.22%** 6	**18.18%** 4
Driver's licence	**38.46%** 10	**44.44%** 12	**36.36%** 8
Passport	**57.69%** 15	**66.67%** 18	**54.55%** 12
Voting card	**23.08%** 6	**29.63%** 8	**27.27%** 6
Employee or student ID	**15.38%** 4	**14.81%** 4	**13.64%** 3
Salary slip	**0.00%** 0	**0.00%** 0	**0.00%** 0
Tax report	**0.00%** 0	**0.00%** 0	**9.09%** 2
Other government- issued ID	**15.38%** 4	**22.22%** 6	**9.09%** 2
Biometrics (e.g., fingerprint, retina scan)	**0.00%** 0	**7.41%** 2	**0.00%** 0
Letter from local government official, village chief, or other trusted person	**19.23%** 5	**18.52%** 5	**13.64%** 3
None required	**19.23%** 5	**0.00%** 0	**9.09%** 2
Other (please describe below)	**3.85%** 1	**3.70%** 1	**4.55%** 1
Total Respondents	26	27	22

Total Respondents: 32

Q31 When opening a mobile money account, what procedures must be taken to verify the information provided?

	Basic system validation (e.g. date of birth is a valid date, all fields completed)	Cross-checking against ID records held in mobile money system	Verification with the ID- issuing authorities or a central database	None required	Other (please describe below)	Total Respondents
Accounts with SIMPLIFIED KYC	**66.67%** 18	**25.93%** 7	**33.33%** 9	**11.11%** 3	**3.70%** 1	27
Accounts with REGULAR KYC	**66.67%** 18	**37.04%** 10	**25.93%** 7	**3.70%** 1	**3.70%** 1	27
Accounts with ENHANCED KYC	**63.64%** 14	**31.82%** 7	**27.27%** 6	**13.64%** 3	**4.55%** 1	22

Total Respondents: 32

Q32 How can customers with mobile money accounts identify themselves prior to transacting (select all that apply)?

	PIN, password, or passcode	Biometrics	Not required	Other (please describe below)	Total Respondents
Accounts with SIMPLIFIED KYC	**96.00%** 24	**0.00%** 0	**4.00%** 1	**0.00%** 0	25
Accounts with REGULAR KYC	**96.30%** 26	**0.00%** 0	**3.70%** 1	**0.00%** 0	27
Accounts with ENHANCED KYC	**100.00%** 20	**0.00%** 0	**0.00%** 0	**0.00%** 0	31
Total Respondents: 32					

Q33 Who assumes primary responsibility for promoting and monitoring compliance with AML/CFT-related obligations?

Answer Choices	Responses	
Specialised AML/CFT manager (often referred to as a Money Laundering Reporting Officer)	**59.38%**	19
General risk officer	**9.38%**	3
Legal/compliance officer	**21.88%**	7
Other (please specify)	**9.38%**	3
Total Respondents: 32		

Q34 What challenges do you face with respect to AML/CFT regulation in your country (if none, enter "None" below)?

answers omitted to maintain confidentiality

Q35 Please share any suggestions regarding this survey or GSMA's work on AML/CFT regulatory issues (if none, enter "None" below).

answers omitted to maintain confidentiality

Q36 Please provide the following demographic information.

answers omitted to maintain confidentiality

Q37 How many active mobile money account holders (active within 90 days, excluding OTC clients) do you have?

Answer Choices	Responses	
Fewer than 100,000	**19.35%**	6
100,000 - 500,000	**29.03%**	9
500,000 – 1 million	**16.13%**	5
Over 1 million	**35.48%**	11
Total Respondents: 31		

Q38 When was your mobile money service launched (month and year)?

answers omitted to maintain confidentiality

Q39 We often find it valuable to follow up with providers. May we contact you with any questions?

Answer Choices	Responses	
Yes	**93.55%**	29
No	**6.45%**	2
Total Respondents: 31		

Annex 3: Country Case Studies

The following case studies profile the progressive measures taken by the Democratic Republic of Congo (DRC), Fiji, Kenya, the Philippines, Sri Lanka, and Tanzania to balance AML/CFT and financial inclusion. Mobile money has significant potential in these predominantly cash-based societies, where geographical barriers, lack of infrastructure, and other challenges make it difficult to deliver traditional financial services. Each country's authorities have adapted their approach to the national context.

The DRC, Sri Lanka, and Tanzania have all applied a tiered approach to their target market. Fiji has aligned SIM card registration and KYC requirements for mobile money to create an efficient system for identifying customers. The Philippines, a pioneer in mobile money, advocates a tiered approach with delayed identity verification.

These emerging regulatory practices have been successful in these nascent markets, where risk management is still evolving. Kenya is best known for M-Pesa, which has served as a catalyst for many other innovative financial services both within Kenya and around the world. However, this case study discusses M-Shwari, a suite of banking products that builds on M-Pesa. Kenya's experience demonstrates (1) how mobile money and other financial services can complement each other to create an inclusive financial ecosystem; and (2) how smart (proportional) KYC requirements can be designed to use information from the mobile money service to facilitate access to additional financial services.

Following the case studies from these developing country markets, the Annex concludes with a description of the approach to risk-based CDD in the European Union.

1. DEMOCRATIC REPUBLIC OF CONGO[89]

The DRC, a predominantly cash-based society, holds significant promise for mobile money. With 31% mobile penetration,[90] mobile money can be a valuable tool for the country's people, only 11% of whom used formal financial services as of 2014.[91] Recognising this untapped potential, the Banque Central du Congo (BCC) issued Directive #24 in November 2011, which allows non-bank electronic money (e-money) issuers to offer transformational financial services.

The maximum value that can be stored in a mobile money account is USD 3,000. There is a maximum daily transaction limit of $100-$500 (depending on the type of account) and a $2,500 monthly limit. Electronic or paper transaction records should be held for up to 10 years.

The DRC does not have a national identification system, so KYC procedures were developed based on a two-tier system for CDD (see Table 12). Tier 1 account holders can transact up to $100 (or other amount set by the operator below the legal limit of $500) without full due diligence. CDD is based on the MSISDN and IMSI: when customers sign up for an entry-level mobile money account, they self-certify their identity and date and place of birth and the provider records their name and address. This information must match what was recorded when they registered their SIM card.

Full CDD is required to transfer up to the maximum legal limit of $500 per day. The customer's identity must be verified using a passport, voting card, driver's licence, or student card. Customers opening accounts to receive salary payments can identify themselves using a company ID card.

89. This case study includes excerpts from Simone di Castri (2014), "Enabling mobile money policies in the Democratic Republic of Congo: Leadership, pragmatism, and a participatory approach to developing a competitive market", GSMA case study, London.
90. GSMA Wireless Intelligence
91. World Bank (2015), "Financial Inclusion Data: Democratic Republic of Congo".

TABLE 12

LIMITS ON TRANSACTIONS AND BALANCES AND ACCOUNT REGISTRATION PROCEDURES IN THE DRC

	Daily transaction limit set by the provider (USD)	Monthly limit (USD)	Maximum balance (USD)	Customer due diligence (CDD)
Basic account	$100–$200 (depending upon provider)	$2,500	$3,000	Simplified KYC: Customers must self-certify their identity and date and place of birth. The verification of the MSISDN is also part of the CDD process. The information must match what was recorded at SIM card registration.
Tier 2 account	$500	$2,500	$3,000	Full KYC: Customers must register in person, complete an application form, and provide a copy of their passport, voting card, driver's licence, or student card.

The central bank holds a blacklist of individuals who are not suitable to be mobile money agents, which it shares with providers. Mobile money providers are responsible for training agents on all compliance procedures, including AML/CFT. They are also accountable for the conduct of agents on behalf of the provider. Each month, a list of agents in the distribution network is updated and sent to the BCC.

2. FIJI

By February 2014, Fiji's National Financial Inclusion Taskforce (NFIT) had achieved its target (set in 2011) to expand access to financial services to 150,000 unbanked people by 2014.[92] Established in 2010, the NFIT is made up of a combination of public sector, private sector, NGO, donor, and development partner members whose goal is to foster accessible, affordable, and appropriate financial services to all Fijians in rural and urban areas. A key part of NFIT's strategy is developing a mobile money platform that utilises Fiji's expanding mobile phone and agent networks, which are well equipped to deal with the infrastructure challenges of an archipelago nation. It is estimated that local MNOs cover more than 90% of the country.[93]

Two MNOs, Vodafone Fiji Limited and Digicel Fiji Limited, have been granted a licence from the Reserve Bank of Fiji (RBF) to offer mobile money services. When designing the regulatory requirements, the RBF was careful to ensure policies were proportional and promoted financial inclusion. In 2010, the RBF approved the extension of mobile money services to include inward international remittances. The financial intelligence unit, housed within the RBF, also worked closely with the two mobile companies in the early stages of the mobile money project to ensure they complied with the AML/CFT requirements as set out in the Financial Transactions Reporting Act (FTRA) of 2004, particularly the requirement to identify and verify customers at registration.

Guideline 4 of the FTRA[94] sets out the standard requirements for customer identification and verification and allows for exemptions and simplified due diligence in lower risk cases (referred to in Fiji as "low-risk" cases), embracing the risk-based AML/CFT approach.

A variety of documents can be used to identify and verify customers, including more formal documents such as passports and utility bills, and less formal documents such as letters of reference. At minimum, the name, address, and occupation must be verified for a low-risk customer. The customer's name can be verified using a variety of documents, including a birth certificate or letter of reference from a "suitable third party", while

92. Governor Barry Whiteside (2014), "Reserve Bank of Fiji Regional Leader in Driving National Financial Inclusion Strategy", Alliance for Financial Inclusion.
93. Fiji Sun (2013), "Moving Forward with Mobile Money." The source of the demographic data is the Fiji Bureau of Statistics, "2007 Population Census".
94. Fiji FIU (2009), "Guideline 4 – Customer Identification & Verification."

the customer's address and occupation can be verified using a utility bill, pay slip, or verification by a "suitable referee", among others (see Box 7). Low-risk customers are defined as customers who are assessed as posing a low risk of engaging in ML or TF activities, such as students, farmers, and microentrepreneurs.

BOX 7
SUITABLE REFEREES

"A 'suitable referee' is a person who knows the customer and whom the financial institution can rely on to confirm that the customer is who he or she claims to be and can verify other personal details (occupation, residential address) of the customer. Examples of suitable referees are:

i. For customers who are minors or students — school head teacher; school principal; landlords (for tertiary students who are renting); parent or guardian.

ii. For other customers, such as those who reside in the rural areas or villages –

   a. Village headman or turaga-ni-koro

   b. Roko Tui (chief administration officer) or Assistant Roko Tui or Provincial Administrator at the Provincial Office

   c. Religious leader (e.g. talatala or preacher, priest, imam of a mosque, pundit)

   d. District Officer or district advisory officer

   e. Official from the Fiji Sugar Corporation sector office (for sugar cane farmers, laborers)

   f. Official from a district government agency such as the Social Welfare Office, Police Station, Health Centers

   g. Current or former employer

   h. Justice of Peace, Commissioner for Oaths, Notary Public

   i. Town councillor

   j. Employee of the financial institution"

Source: FIU Guideline 4, Art. 12.4[95]

The Guideline also allows delayed verification when: (1) customers who do not have easy access to acceptable documentation are in the process of obtaining such documentation from relevant government agencies; or (2) the customers have some ID documents but lack other required documents, which they are willing to provide at a later date. The financial institution has the discretion to limit the number, value, and type of transactions that may be performed until verification is finalised.

FIU Policy Advisory 4/2010[96] addresses identification of customers of mobile financial services. Agents are allowed to identify and verify identities of customers on behalf of mobile money providers (referred to as "telephone service providers"). Telephone service providers are required under the *Decree on Compulsory Registration of Customers for Telephone Services* (2010) to register new and existing telephone users. They must register the telephone user's name, date of birth, and address and must obtain a copy of the photo ID

95. Fiji FIU (2009), "Guideline 4 – Customer Identification & Verification."
96. Fiji FIU (2010), "Advisory 4/2010 – Re: Identification of Customers of Telephone Financial Services."

provided by the customer at the time of registration. For customers assessed as "low risk", registration under the Decree on Compulsory Registration of Customers for Telephone Services is sufficient to meet the KYC requirements for opening a mobile money account.[97]

3. KENYA[98]

According to a FinAccess survey published in October 2013, the proportion of Kenyan adults using formal financial services has more than doubled since 2006 from 27% to 67%, reaching 80% in urban areas. Of the 18.6 million adults in the country, 5.4 million use banks while 5.2 million use informal financial services (of whom 1.5 million do not use any formal financial services). More than half of adults — 11.5 million — currently use mobile financial services, which have become the most widely used financial service in Kenya.

Originally envisaged as a mobile money transfer service, M-Pesa has evolved, allowing customers to conduct a range of transactions and access other products via the M-Pesa platform. These products include M-Shwari, which offers a suite of savings and credit products. Launched in November 2012, M-Shwari attracted 3.5 million customers in its first six months. By December 2014, 9.2 million M-Pesa customers had signed up for M-Shwari accounts, of which 4.7 million were active.

M-Shwari is offered by the Commercial Bank of Africa (CBA) in partnership with Safaricom. M-Shwari allows M-Pesa customers to access an interest-bearing savings product — effectively a bank account linked to their M-Pesa e-wallet — which pays between 2% and 5% interest per annum. M-Shwari customers also have access to short-term credit with on-demand loans of up to $235. The credit score assigned to a customer upon enrolment is based on their past usage of Safaricom products.[99] Subsequent credit scores are based on both M-Shwari and M-Pesa product usage. As of December 2014, there were $17.7 million in outstanding loans and $45.3 million in net deposits.

The CBA is responsible for KYC compliance, as per the prudential guidelines issued under the Banking Act, and uses a remote CDD model for M-Shwari, which has been critical to its success. Account opening is virtual. CBA seeks the consent of M-Pesa customers to obtain and use the information they provided to Safaricom when they opened an M-Pesa account. When they first sign up for M-Pesa, customers must show government-issued ID (national ID or passport) and complete an application form that includes their name, ID number, and address. With the customer's consent, this information is shared with CBA to open an M-Shwari account. This information is then verified against the Integrated Population Registration System (IPRS), an official database maintained by the Government of Kenya. At this point, customers can deposit up to a maximum of KES 250,000 (approx. $2,825) in their M-Shwari bank account.

Customers wishing to increase their maximum M-Shwari balance must comply with stricter KYC requirements. To be eligible to maintain a balance of up to KES 500,000 (approx. $5,650), customers must provide the bank with a copy of their legal ID in person at a Safaricom outlet, where the original ID is also verified. For those seeking a balance above KES 500,000, customers must present their original tax PIN Certificate at a Safaricom outlet, which is electronically validated using Kenya Revenue Authority records. Copies of all identification documents are stored by the CBA.

The M-Shwari CDD process is designed to be proportionate to the risks, and the simplified KYC procedure is in line with the FATF's RBA. In the case of M-Shwari, the risk of money laundering and terrorist financing is limited and well managed since M-Shwari is designed as a savings account with clear transactional limits and the following limits on functionality:

97. Fiji FIU (2010), "Advisory 4/2010 – Re: Identification of Customers of Telephone Financial Services," Art. 14-15.

98. Adapted from Simone di Castri, "Tiered risk-based KYC: M-Shwari successful customer due diligence", GSMA blog, 8 July 2013.

99. No fees or paperwork are required to apply for a loan. M-Shwari customers can dial *234*6# to find out their credit limit (maximum possible loan value). To qualify for an M-Shwari loan, a customer must be an M-Pesa subscriber for at least six months. An algorithm based on prior usage of Safaricom services (M-Pesa, Bonga Points, voice, and data) is used to determine the initial eligible loan limit. Subsequent loan limits are determined based on "regular savings" levels with M-Shwari and a customer's repayment history with M-Shwari loans. Loan disbursements are issued through M-Pesa and loan payments are made through M-Pesa. Loans can be taken for between KES 100 (USD 1.15) and KES 20,000 (USD 235), have a 30-day term, and carry a facility fee of 7.5%. Failure to pay triggers the loan to rollover (if a customer pays the loan late, the effective interest rate is much higher). This footnote uses information from Mike McCaffrey, Olivia Obiero, and George Mugweru (February 2013), "M-Shwari: Market Reactions and Potential Improvements," MicroSave Briefing Note #139.

- Deposits into M-Shwari can only be made from the customer's M-Pesa account. M-Shwari cannot be used to make transfers or payments. To do this, M-Shwari customers must move money from M-Shwari to M-Pesa and then make the transfers and/or payments, which must be within M-PESA's transactional limits of KES 1400,000 (approx. $1,500) per day.

- The only payments that go through the M-Shwari account are related to the disbursement and repayment of M-Shwari loans.

- Tiered KYC allows for graduated deposit amounts: the lower the KYC level, the lower the balance that can be held and vice versa.

4. THE PHILIPPINES

The Philippines has been a pioneer in mobile money, embracing both bank-based and non-bank-based models. A progressive central bank, the Bangko Sentral ng Pilipinas (BSP) has collaborated with the mobile industry (Globe and Smart)[100] to create an enabling environment for mobile money. In the Philippines, mobile money customers can conduct cash-in and cash-out, send and receive domestic and international remittances, transfer money, pay bills, and make loan payments. MNOs are allowed to issue e-money, and even non-bank agents can perform cash-in/cash-out, which has extended the reach of agent networks.

The BSP is known for its willingness to work with the country's mobile operators to promote financial inclusion. This financial sector reform was initiated around the same time the Philippines was placed on the FATF's Non-Cooperative Countries and Territories (NCCT) list in 2000.[101] While this made financial inclusion more challenging, the BSP used the flexibility of the FATF Recommendations to create a KYC regime that has allowed mobile money to flourish.

The BSP allows customers to be identified just once — at the commencement of the business relationship — and provides a list of 20 acceptable and credible means of identification. The SMART Money and GCash models apply this rule differently, given that SMART money is bank-based and GCash is non-bank-based. With SMART Money, KYC is conducted before the account is personalized. Customers using GCash may open an account remotely via their mobile phone or online, although they cannot withdraw or deposit funds until they undergo face-to-face CDD at an accredited shop, partner outlet, or bank.

The standard procedure for all BSP-regulated financial institutions is to formulate and implement a comprehensive and risk-based Money Laundering and Terrorist Financing Prevention Program (MLPP) covering customer identification (initial and ongoing), record keeping, covered transaction and suspicious transaction reporting, staff training, due diligence, auditing, and other topics.[102] Reduced CDD can be applied for potentially low-risk customers, which may include "an individual customer with regular employment or economically productive activity, small account balance and transactions, and a resident in the area the [financial] institution's office or branch."[103] Financial institutions applying reduced CDD can open an account with the full name, current address, date and place of birth, employment details, contact details, source of funds, and a signature, provided additional information (including permanent address, nationality, and tax/social security number) is obtained within 90 days.[104] This effectively allows the normal course of business to proceed without disruption and provides a reasonable amount of time to collect additional information to verify the customer's identity.

A good example of the BSP's flexible and practical AML/CFT approach was their response to the crisis following Typhoon Haiyan (Yolanda), which caused widespread devastation in the Philippines. For a short time, the BSP had to waive the requirement to present an ID for victims of the typhoon so transactions could be

100. Smart Communication's Smart Money was launched in the Philippines in 2001, when Smart Communications, an MNO, partnered with Banco de Oro (BDO) and a number of retail merchants that served as their agents. Globe's GCash launched in November 2004. GCash was run wholly by a subsidiary of an MNO, Globe Telecom. In 2009, Globe Telecom entered into a partnership with the Bank of the Philippine Islands and Ayala Corporation to create BPI Globe BanKO, a mobile phone-based savings bank.

101. The Philippines was removed from this list in 2005. See FATF (2007), "Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review".

102. BSP Circular 706, Art.X805.1-X805.2.

103. BSP Circular 706, Art. X806.1.a.

104. BSP Circular 706, Art. X806.1.d and Art. X806.2.a.

processed without delay.[105] The waiver was limited to a maximum of PHP 50,000 (approx. USD 1,100) per day. The waiver still required a certificate from the clients stating they were victims of the typhoon and required the BSP-covered institution to update KYC information at a later date. The BSP also required financial institutions to strictly monitor customer accounts to prevent abuse during this vulnerable time.

5. SRI LANKA[106]

The World Bank Global Findex Database reveals that, as of 2014, 83% of adults in Sri Lanka reported having an account at a formal financial institution, such as a bank, finance company, cooperative, post office, or microfinance institution.[107] In March 2014, there were 10.5 million unique mobile phone subscribers in this country of 20 million people, providing a fertile environment for mobile money to develop.

As financial inclusion was an important issue for the Central Bank of Sri Lanka (CBSL), it worked with other stakeholders to develop an enabling environment for non-banks to offer mobile money. These efforts provide an excellent example of how progressive and financial inclusion-focused policies, combined with private sector collaboration, can expand financial access through technology-enabled solutions.

In late 2011, the CBSL issued mobile payments guidelines permitting non-banks to issue electronic wallets as long as they held equivalent funds in a custodial account in one or more licensed commercial banks. Mobile wallets could be used for services like bill payments, P2P payments, B2P payments (salaries), B2B payments, retail payments, and online payments.

In April 2012, the CBSL issued a mobile money licence to Sri Lanka's largest MNO, Dialog. One year after Dialog's launch in June 2012, it had registered over 1 million mobile money accounts, of which 200,000 were active on a 30-day basis. One of the reasons for the rapid adoption of Dialog's eZ Cash service was the ability to apply tiered KYC requirements. In line with the FATF's risk-based approach, the CBSL allowed Dialog to create two types of accounts with different transaction limits corresponding to different CDD procedures:

- "Classic account": An entry-level account that customers can activate simply by dialling a number from their mobile phone. Dialog then uses the KYC information stored in its database from the customer's SIM card registration to verify his/her identity. SIM card registration requires a physical copy of the customer's original national ID card (the photocopy is later digitised and uploaded to the internal database), which is stored with the signed contract. All Sri Lankans are required to apply for their national ID card on their 16th birthday and to carry it with them at all times, so access to the national ID is not a problem. The maximum amount a customer can add to a Classic account is LKR 10,000 (approx. USD 80). The Classic account allows them to send money P2P (up to LKR 5,000 or approx. $40 per transaction), pay utility bills (up to LKR 10,000 or approx. $80 per transaction), and conduct other transactions, such as online payments or payments of microinsurance premiums, microfinance loans, or subscriptions.

- "Power" account: If customers want to conduct higher value transactions, they can activate a Power account with a maximum balance of LKR 25,000 (approx. $200) and higher transaction limits (LKR 5,000 for P2P and LKR 25,000 for bill payment). To activate a Power account, a customer must visit a Dialog Customer Care Centre to confirm his/her identity.

In April 2013, the CBSL granted Dialog permission to accept inward international remittances to the eZ Cash wallet custodian account, which is then redirected to a customer's bank account.

105. BSP Memorandum 52.

106. For additional information and references see Simone di Castri (2013), "Enabling mobile money policies in Sri Lanka: The Rise of Ez-Cash", GSMA MMU case study, London.

107. See World Bank (2014), "Financial Inclusion Data: Sri Lanka."

6. TANZANIA[108]

Tanzania is a mobile money and digital financial inclusion success story. A Financial Inclusion Insights survey conducted between September 2013 and March 2014 found that 48% of adults had used mobile money and 38% were active mobile money users.[109] In September 2014, there were 13 million active mobile money accounts with balances held in trust accounts totalling TZS 362 billion (approx. USD 161 million).[110] In the month of December 2013, mobile money deployments performed transactions worth over TZS 3 trillion (approx. $1.8 billion).[111]

The Bank of Tanzania (BOT) has adopted a proportionate AML/CFT regime that allows providers to implement tiered CDD and delegate a number of critical functions to their agents. Agents are responsible for facilitating cash withdrawals and deposits, registering users, following KYC requirements, and educating users. Since there is no national ID system in Tanzania, customers often use voter registration cards to validate their identity. Other valid forms of ID include pension cards, passports, and employee cards. Agents are required to make a copy of the ID and submit it the provider to keep on file for future customer validation. If the agent cannot retain a copy of the ID, the customer is registered as a Tier 1 customer, which limits the customer to an account with an annual throughput value of TZS 1.7 million (approx. $1,007). If a copy of the ID can be retained and is sent to the provider for verification then the customer is registered as a tier 2 customer and is eligible for an account with an annual throughput of TZS 50 million (approx. $29,600).

Agents are also required to record transactions by hand in a log book. For each transaction, the agent enters the account balance, date, agent ID, transaction ID, transaction type (customer deposit or withdrawal, agent cash rebalancing), value, and the customer's phone number, name, and ID number. Most of this information is copied from the confirmation SMS the agent receives. Customers are then asked to sign next to each transaction in the log, which helps to discourage fraud.

Even though the regulator allows providers to set up different types of accounts, Vodacom is the only operator so far that has implemented different tiers (see Table 13).

TABLE 13

M-PESA TIERED KYC IMPLEMENTED BY VODACOM

Account type	Daily transaction limit set by the provider (USD)	Monthly limit (USD)	Maximum balance (USD)	Customer due diligence (CDD)
Tier 1	TZS 1,000,000 (approx. US$ 600)	TZS 1,000,000 (approx. $600)	TZS 3,000,000 (approx. $1,775)	Customer shows ID to the agent
Tier 2	TZS 3,000,000 (approx. $1,775)	TZS 5,000,000 (approx. $2,960)	TZS 5,000,000 (approx. $2,960)	Customer shows ID to the agent, who makes a copy that the provider stores
Tier 3	TZS 12,000,000 (approx. $7,100)	TZS 50,000,000 (approx. $29,610)	TZS 1,000,000,000 (approx. $592,270)	Customer shows ID, Taxpayer Identification Number (TIN), and business licence to the agent, who makes copies that the provider stores

108. This case study includes excerpts from Simone di Castri and Lara Gidvani (2014), cit.
109. Source: Financial Inclusion Insights (2014), Survey of Tanzania.
110. Source: Bank of Tanzania (2014), "Financial Stability Report, September 2014."
111. Source: Bank of Tanzania (2014), "National Payment System Directorate Statistics."

7. EUROPEAN UNION

The Third EU Money Laundering Directive (3rd AMLD) provides the general framework governing AML/CFT in the European Union. This framework is currently being amended in line with the new FATF recommendations and a revised MLD has been proposed (see below).

The concept of Simplified Due Diligence (SDD) is included under Article 11 of the 3rd AMLD (as amended by Article 19 of the E-Money Directive). Products eligible for SDD are exempted from the legal requirement to identify and verify customers (in the absence of suspicion of ML or TF). For e-money, SDD is only permitted for (1) non-rechargeable products with a maximum balance of EUR 250 (or EUR 500 if the product can only be used domestically); (2) rechargeable products with an annual transaction limit of EUR 2,500 (users may only exceed this limit if they have redeemed more than EUR 1,000 directly from the issuer over the course of a year); or (3) rechargeable products connected to a bank account with an annual transaction limit of EUR 15,000.

The Commission has recently published a proposal for a Fourth Anti-Money Laundering Directive (4th AMLD), driven in part by revisions to the FATF Recommendations adopted in February 2012 and by various reports and assessments conducted by the Commission on the application of the 3rd AMLD (2005/60/EC).

The Directive, if adopted by the European Parliament and Council of Ministers, would repeal the 3rd AMLD and Commission Directive 2006/70, which provide examples of how simplified due diligence may be applied. The revised Directive would tighten the rules on SDD. The current approach, which allows for full exemptions to CDD requirements, was felt to be overly permissive. Under the revised Directive, financial providers would have to ascertain whether specific products or customers posed a lower risk. A number of potentially lower risk factors are set out in Annex II of the Directive, including "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes" and "products where the risk of money laundering/terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money as defined in [the E-Money Directive])." In addition, the proposal would require the European Banking Authority (and the authorities responsible for pensions and securities) to issue guidelines on the risk factors to be considered and the measures to be taken where SDD measures are appropriate.

References and bibliography

FATF DOCUMENTS

FATF (2003), "The 40 Recommendations".

FATF (2003), Interpretive Notes for Recommendations 10, 12, 22, 23, 24 and 25.

FATF (2007), "Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review".

FATF (2009), "Risk-Based Approach: Guidance for Money Service Businesses".

FATF (2010), "Money Laundering Using New Payment Methods".

FATF (2011), "Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion".

FATF (2012), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations".

FATF (2013a), "Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion".

FATF (2013b), "Guidance on National Money Laundering and Terrorist Financing Risk Assessment".

FATF (2013c), "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services".

FATF (2013d), "Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems".

FATF (2013e), "Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations".

FATF (2013f), "The Role of *Hawala* and Other Similar Service Providers in Money Laundering and Terrorist Financing".

FATF (2014), "Financial Flows Linked to the Production and Trafficking of Afghan Opiates".

FATF (2015), "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant".

ADDITIONAL RESOURCES

Alliance for Financial Inclusion (2014), Mobile financial services: Mobile-enabled cross-border payments, Guideline Note No. 14.

Mireya Almazan, "OTC & mobile money: Making sense of the data", GSMA blog, 22 January 2015.

Bangko Sentral ng Pilipinas, Circular 706.

Bangko Sentral ng Pilipinas, Memorandum 52.

Bank for International Settlements – Committee on Payment and Settlement Systems & The World Bank (2007), "General Principles for International Remittance Services", paras. 64, 93.

Bank for International Settlements – Committee on Payments and Market Infrastructures (2014), "Nonbanks in retail payments", Section 6.1.

Bank of Tanzania (2014), "Financial Stability Report, September 2014."

Bank of Tanzania (2014), "National Payment System Directorate Statistics."

Bester et al. (2008), "Implementing FATF standards in developing countries and financial Inclusion: Findings and guidelines", Genesis Analytics, Johannesburg.

Simone di Castri (2013), "Enabling mobile money policies in Sri Lanka: The rise of Ez-Cash", GSMA Mobile Money for the Unbanked (MMU) case study.

Simone di Castri (2013), "Mobile money: Enabling regulatory solutions", GSMA Mobile Money for the Unbanked (MMU) Discussion Paper.

Simone di Castri, "Tiered risk-based KYC: M-Shwari successful customer due diligence", GSMA blog, 8 July 2013.

Simone di Castri (2014), "Enabling mobile money policies in the Democratic Republic of Congo: Leadership, pragmatism, and a participatory approach to developing a competitive market", GSMA Mobile Money for the Unbanked (MMU) case study.

Simone di Castri and Lara Gidvani (2014), "Enabling mobile money policies in Tanzania: A 'test and learn' approach to enabling market-led digital financial services", GSMA Mobile Money for the Unbanked (MMU) case study.

Pierre-Laurent Chatain, Raúl Hernandez-Coss, Kamil Borowik, and Andrew Zerzan (2008), "Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing", 13, The World Bank Group, Working Paper No. 146, Washington, DC.

Pierre-Laurent Chatain, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker (2011), "Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions", The World Bank Group, Washington, DC.

Evans and Pirchio (2015), "An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries But Flounder in Most", Coase-Sandor Institute for Law and Economics, The University of Chicago Law School, Chicago.

Fiji FIU (2009), "Guideline 4 – Customer Identification & Verification".

Fiji FIU (2010), "Advisory 4/2010 – Re: Identification of Customers of Telephone Financial Services".

Fiji Sun (12 May 2013), "Moving Forward with Mobile Money".

G20 Financial Inclusion Experts Group (2010), "Innovative Financial Inclusion Principles and Report on Innovative Financial Inclusion from the Access through Innovation Sub-Group of the G20 Financial Inclusion Experts Group".

GSMA (2013), "The mandatory registration of prepaid SIM card users", GSMA white paper, London.

GSMA (2015), "State of the Industry 2014: Mobile Financial Services for the Unbanked".

Gutierrez & Singh (2013), "What Regulatory Frameworks are More Conducive to Mobile Banking? Empirical Evidence from Findex Data", The World Bank, Washington, DC.

InterMedia, (2014), "Financial Inclusion Insights Survey of Tanzania."

Louis de Koker (2009), "Anonymous Clients, Identified Clients and the Shades In Between: Perspectives on the FATF AML/CFT Standards and Mobile Banking." Paper presented at the 27th Cambridge International Symposium on Economic Crime, Jesus College, Cambridge, UK.

Louis de Koker (2013), "The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks within the New Standards Framework", Washington Journal of Law, Technology & Arts, 8 (3), 165.

Philip Levin (15 April 2013), "MMU Spotlight on 'direct deposits': An expensive nuisance for mobile money operators", GSMA Mobile Money for the Unbanked (MMU) blog.

Philip Levin (29 August 2013), "The big payoff: Getting customers active at registration", GSMA Mobile Money for the Unbanked (MMU) blog.

Mike McCaffrey, Olivia Obiero, and George Mugweru (2013), "M-Shwari: Market Reactions and Potential Improvements", MicroSave Briefing Note #139.

Yasmina McCarty, "Barriers to customer activation: A case study from MTN Uganda", GSMA Mobile Money for the Unbanked (MMU) blog.

Claudia McKay, Toru Mino, and Paola de Baldomero Zazo (2012), "The Challenge of Inactive Customers: Using Data Analytics to Understand and Tackle Low Customer Activity", CGAP presentation.

Brian Muthiora (2015), "Enabling mobile money policies in Kenya", GSMA Mobile Money for the Unbanked (MMU) case study.

OECD, "Financial Inclusion and Financial Integrity: Complementary Policy Objectives."

Daniel Radcliffe (4 April 2013), "Why aren't Pakistan's mobile money customers opening accounts?", GSMA Mobile Money for the Unbanked (MMU) blog.

Claire Scharwatt & Chris Williamson (2015), "Mobile money crosses borders: New remittance models in West Africa", GSMA Mobile Money for the Unbanked (MMU).

Marina Solin and Andrew Zerzan (2009), "Mobile money: Methodology for assessing money laundering and terrorist financing risks", GSMA Discussion Paper.

U.S. Agency for International Development (2010), "Mobile Financial Services Risk Matrix", Washington, DC.

Governor Barry Whiteside (2014), "Reserve Bank of Fiji Regional Leader in Driving National Financial Inclusion Strategy", Alliance for Financial Inclusion.

World Bank (2012), "From Remittances to M-Payments: Understanding 'Alternative' Means of Payment within the Common Framework of Retail Payments System Regulation", Section III.4.3.

World Bank (2015), "Financial Inclusion Data: Democratic Republic of Congo", Global Findex.

World Bank (2015), "Financial Inclusion Data: Sri Lanka", Global Findex.

For further information please contact
mmu@gsma.com
GSMA London Office
T +44 (0) 20 7356 0600