



Mobile Money for the Unbanked

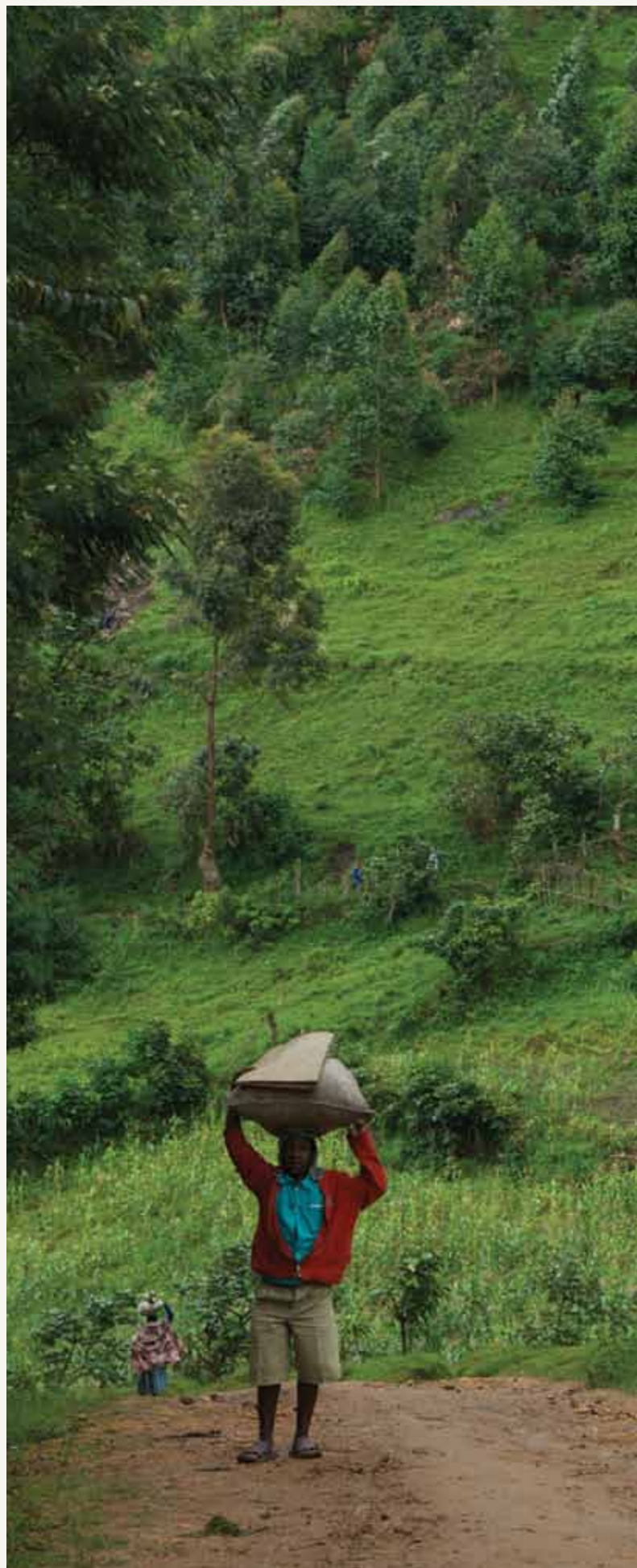
Mobile Money: Enabling regulatory solutions

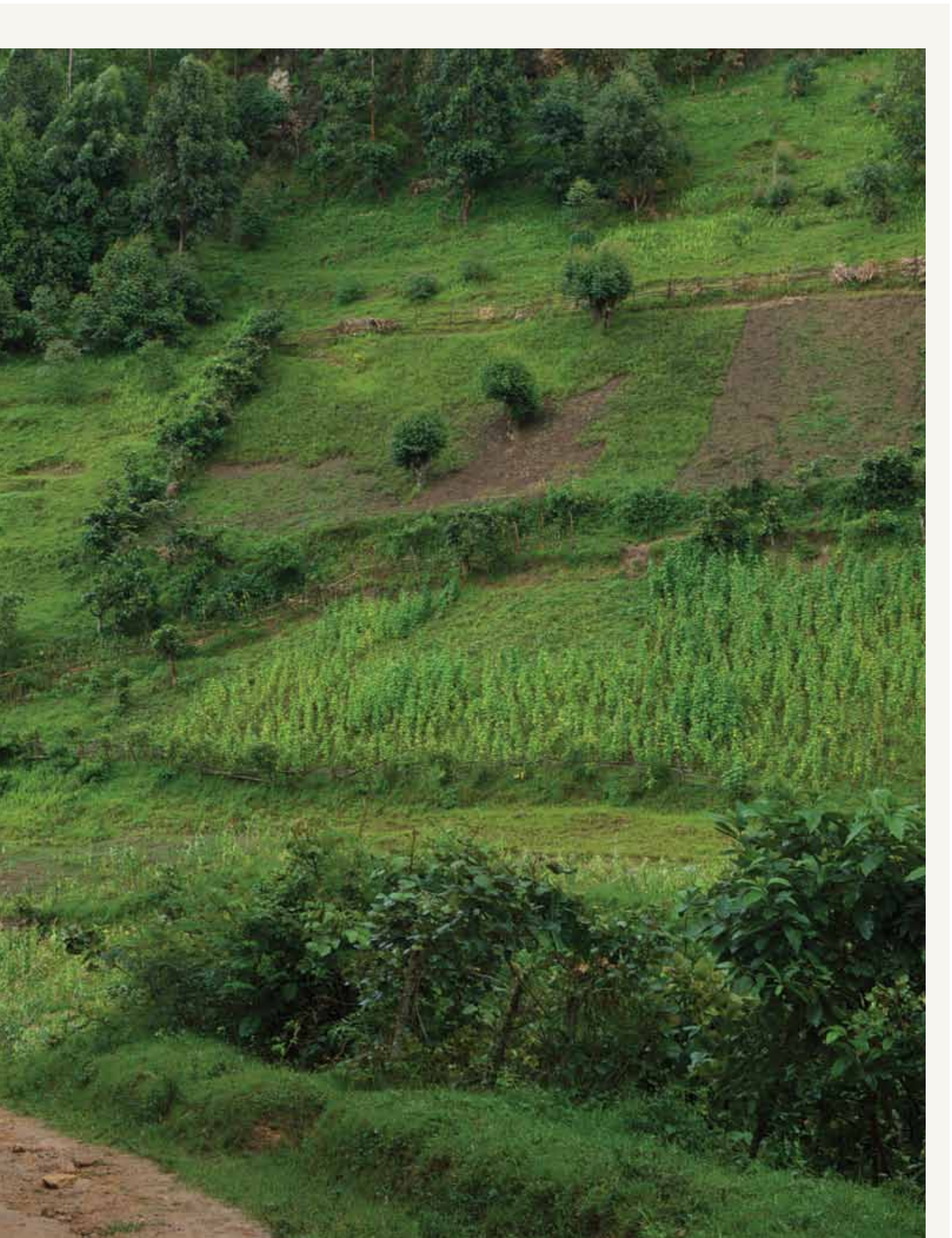
Simone di Castri
February 2013



Contents

1 – 2	Executive summary
3 – 10	Introduction
11 – 14	1. Why should regulators establish an open and level playing field?
15 – 17	2. How is customer money being safeguarded?
18 – 23	3. What customer due diligence measures are appropriate for mobile money?
24 – 28	4. How can distribution risks be mitigated while still allowing providers to leverage third party networks?
29 – 30	5. How can mobile money customers be given more protection?
31 – 33	6. How should policy makers and providers engage on interoperability?
34	Conclusions
35 – 36	Endnotes





Executive summary

The full potential of mobile money has not yet been realised, with 2.5 billion people in developing countries still lacking a viable alternative to the cash economy and informal financial services. 1.7 billion of them have mobile phones, but the mobile money industry has found it challenging to launch and scale services for the unbanked because yet many policy and regulatory environments are not genuinely enabling.

The aim of this paper is to provide a useful tool for regulators and mobile money providers to engage more effectively. It elaborates commonly held positions in the mobile industry on some key policy and regulatory issues, backed up by evidence.¹

As awareness grows that financial exclusion is a source of risk for the financial system, the global Standard Setting Bodies (SSBs) are embracing the goal of full financial inclusion, recognising that it reinforces the objectives of financial stability, integrity, and consumer protection. Mobile money can contribute to all of these objectives, driving economic and social growth through a cash-lite economy and digital pathways to financial inclusion. Therefore, we argue that the proposed regulatory reforms should not simply be items on the regulator's financial inclusion agenda. They should also become central to national strategies for improving financial stability and integrity, protecting financial consumers, and guarding the financial system against the risks of the widespread use of cash.

The basic proposition for mobile money to succeed is to create an open and level playing field that allows non-bank mobile money providers, including mobile network operators (MNOs), into the market. Anecdotal evidence, commercial lessons, and international regulatory principles all defend opening the market to providers with different value propositions. The prudential regulations of non-bank mobile money providers effectively mitigate the risk of mobile money customers losing the money they have stored in the system. The challenges of anti-money laundering and combating the financing of terrorism (AML/CFT) compliance can be addressed by promoting risk-based know-your-customer (KYC) procedures. There are also cost-effective regulatory solutions in place to develop and set up distribution networks and accelerate customer adoption.

When both banks and non-bank providers, especially MNOs, are allowed to launch mobile money deployments, and when there are effective and proportionate mechanisms in place to manage the unique risks of this industry, mobile money has the capacity to significantly expand financial inclusion – through lower transaction costs, improved access to underserved areas, and higher levels of customer convenience.

What would a digital financial inclusion environment and a cash-lite economy look like? Customers of small businesses would be able to keep electronic records of their transactions, banks would use the ubiquitous distribution networks of third parties to deliver credit products, third parties would play a role in educating consumers, and microfinance institutions (MFIs) would have access to a new group of customers that are already using digital transactions thanks to tailored KYC procedures and other efforts.

The countries that embrace the reforms discussed in this paper will ultimately be the ones driving innovation in mobile financial services and building inclusive, secure, and efficient financial sectors.



Introduction

This paper aims to provide support to regulators and mobile money providers that want to engage in collaborative discussions on the regulatory reforms that are necessary to develop mature, innovative, and deep financial systems.

Mobile money is becoming a powerful tool for building more inclusive, stable, and secure financial sectors. The potential of mobile technology to improve people's lives is growing exponentially as mobile network operators (MNOs) expand digital connectivity and bring more people in emerging markets into the mobile network.

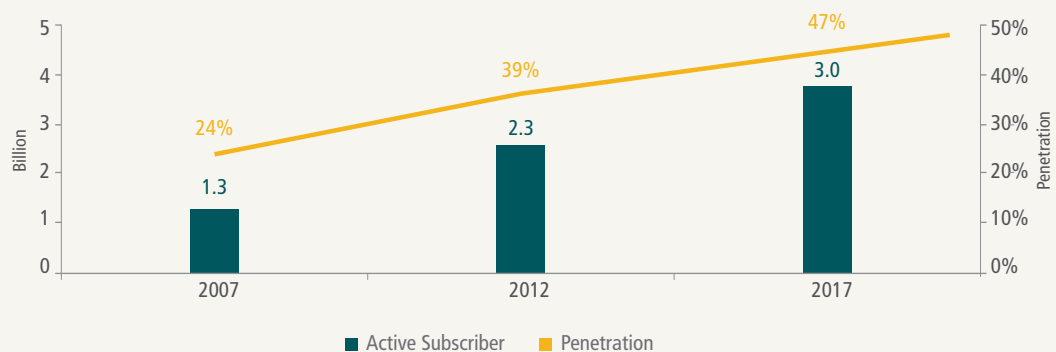
The potential of mobile money is clear:

- There were 5.9 billion active mobile connections worldwide in 2012. The number of GSM mobile connections doubled in the last four years in Africa and South East Asia, and more than tripled in South Asia. The total number of unique mobile subscribers is 3.2 billion (46% of the world's population) and is forecast to grow to 4 billion in five years.¹
- Of the 2.5 billion people in the world who still lack access to the financial system,² 1.7 billion have mobile phones.³
- MNOs are much more experienced than banks in building and managing large, low-cost distribution networks in unserved areas. The largest MNO in a developing country has 100–500 times more airtime reseller outlets than banks have branches.⁴

With 2.5 billion people in the world still lacking access to basic financial services, the challenge is to overcome the risks and costs of cash-based transactions and find alternatives to informal ways of making payments and transferring and storing money. Over 150 mobile money deployments⁵ are already extending the reach of the formal financial sector, providing low-cost products and new entry points for the unbanked through mobile phones and networks of cash-in and cash-out (CICO) agents. Commercial players, especially MNOs, are driving this movement.

Yet, relatively few mobile deployments are reaching scale. Both internal factors (such as the level of investment in mobile money and organisational structures, and customer acquisition and distribution strategies) and external factors (such as the level of mobile penetration, different socio-economic factors, competition, and the regulatory architecture) may hamper the success of a deployment. While all external factors influence the design and implementation of a mobile money service, only regulation seems to pose challenges too great for a service to overcome.⁶ Anecdotal evidence suggests there are markets in which regulatory barriers do not allow mobile money businesses to set up effective distribution networks or to register, identify, and activate clients, all of which is constricting business, creating major disincentives to investments, and delaying the generation of positive cash flow, making it too burdensome to address operational challenges.⁷

Figure 1: Mobile in the developing world



1 "GSMA Announces New Global Research that Highlights Significant Growth Opportunity for the Mobile Industry," Press release, 18 October 2012, <http://www.gsma.com/newsroom/gsma-announces-new-global-research-that-highlights-significant-growth-opportunity-for-the-mobile-industry>.

2 The Global Financial Inclusion (Global Findex) Database, <http://econ.worldbank.org>.

3 CGAP, GSMA, and McKinsey & Company "Mobile Money Market Sizing Study." The figure is reported in Mark Pickens (2009), "Window on the Unbanked: Mobile Money in the Philippines," CGAP Brief. Available at http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/br_mobile_money_philippines_d_30.pdf.

4 Claire Alexandre, Ignacio Mas, and Dan Radcliffe. (2010), "Regulating New Banking Models that can Bring Financial Services to All," Bill & Melinda Gates Foundation paper, August 2010. Available at http://www.papers.ssrn.com/sol3/papers.cfm?abstract_id=1664644.

5 GSMA Mobile Money for the Unbanked (MMU) Deployment Tracker, data retrieved on 12 January 2012, <http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-the-unbanked/>.

6 See Claire Pénicaut (2013), "State of the Industry: Results from the 2012 Global Mobile Money Adoption Survey," GSMA, London, UK. Available at <http://gsma.com/mmu>.

7 Paul Leishman (2011), "Is There Really any Money in Mobile Money?," GSMA Mobile Money for the Unbanked position paper. Available at <http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/oneyinmobilemoneyfinal63.pdf>.

A level playing field to leave the choice to usersⁱⁱ

“From the regulator’s perspective, the concerns involved in allowing mobile operators to offer payment services can be easily addressed. In fact, there is not a trade-off between the participation of financial intermediaries and mobile operators. [...] In the end, by allowing all types of participants, the financial regulator leaves the market to figure out what works best, and the customers will benefit from the result.”

Narda Sotomayor
Head of the Microfinance Analysis Department
Superintendencia de Banca, Seguros y AFP, Peru

An enabling policy and regulatory framework creates 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. Unfortunately, ineffective policies and cumbersome regulatory barriers have had a negative effect on the development of mobile money and the expansion of financial inclusion in many new markets.

Drawing on examples from various country experiences and on data, information, and lessons gleaned by the GSMA and by other institutions such as the Bank for International Settlements (BIS), the Financial Action Task Force (FATF), CGAP, the World Bank, and the World Economic Forum (WEF), this paper discusses how to apply established policy practices and regulatory principles to mobile money regulations.⁸

Given the progress that has been made in a number of markets towards creating more enabling policies for financial inclusion, the templates for regulatory reform do not need to be created from scratch. We present options for creating an enabling regulatory framework for digital financial inclusion, and a rationale for adopting policies that would meet widespread demand for more convenient and secure formal financial services while simultaneously increasing the stability, integrity, and safety of the financial system. The identified solutions can be used to draft a regulatory template for mobile money that could be applied to reforms in many markets.⁹ This paper also argues that these reforms should not simply be consigned to the regulator’s financial inclusion agenda. Building an enabling regulatory framework for mobile money and financial inclusion should also become an integral part of national strategies to improve financial stability and integrity, to protect financial consumers, to secure the financial system against the risks of an informal cash-based economy, and to foster economic growth and job creation.¹⁰

The paper is organised into the following sections:

Section 1 presents evidence from established mobile money markets, high-level commercial considerations, and regulatory arguments that are relevant to the policy maker’s choice of the business models to permit. The main point of reference for the regulatory arguments is the Bank for International Settlements (BIS), which recommends adopting established best practices in financial services regulation. The paper details why, from a commercial point of view, non-banks (especially MNOs) are well suited to building a sustainable mobile money business and expanding, in a rapid and sound way, the range of services a customer can access. This effectively creates an ‘on-ramp’ for digital financial inclusion that can be leveraged by other providers as well, such as banks and insurance providers.¹¹

Section 2 discusses how clear and simple rules applied to non-bank mobile money providers can mitigate liquidity and solvency risks. Customer protection measures begin with safeguarding funds in one or more banks (diversification of e-float fund holdings), imposing restrictions on its use by the provider, and insulating funds from institutional risks to ensure funds are available when customers want to redeem them against electronic value. Unencumbered liquid assets must normally be equal to the electronically-issued value, which is a much heavier prudential requirement typically required of banks and makes minimum capital requirements unnecessary. In the event of provider insolvency, the regulator can also detail clear procedures. Permitting the provider to pay customers interest on stored value is likely to promote the adoption of the service and have a positive effect on financial inclusion.

8 Particularly important are the core principles and other publications of the relevant standard-setting bodies (SSBs): the Basel Committee on Banking Supervision (BCBS), the Committee on Payment and Settlement Systems (CPSS), and the Financial Action Task Force (FATF).

9 We also acknowledge that the opportunities offered within the local country context should always be taken into account. For example, in a number of countries, the local regulatory framework has provided a high level of flexibility that the regulator has used to minimize the cost of regulations and maximize its impact.

10 See the next box on the benefits of mobile money from a policy perspective, and Section 3.

11 Dan Radcliffe and Rodger Voorhies (2012), “A Digital Pathway to Financial Inclusion,” Bill & Melinda Gates Foundation paper. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2186926.

Section 3 discusses the ways in which mobile money helps to reduce the risk of money laundering and terrorist financing, namely, by lowering the rate of financial exclusion and enhancing financial integrity through electronic transactions that can be monitored and traced more easily than cash. It is recommended that regulators implement the Financial Action Task Force (FATF) recommendations, design risk-based know-your-customer (KYC) regimes that allow for simplified customer due diligence (CDD) based on the specific risk that each product offers, and leverage operational and transactional mitigation measures. Misapplying these recommendations with onerous identification requirements will slow the uptake of mobile money.

Section 4 discusses how mobile money providers can outsource customer registration, cash collection, and disbursement activities to third parties¹² most effectively. Building an efficient distribution network is one of the main challenges for the provider – e.g., there is evidence that any delay in signing up a new customer and activating the mobile money account reduces customer activation. One of the main issues is setting limits on the qualifications and the types of agents and other third parties that can provide mobile money services, which should be done carefully to avoid restricting outreach. Making the provider liable for both the actions that an agent or third party executes on its behalf and in executing in the execution of the principal/ third party contract with the mobile money providers, guarantees that the provider will set up and monitor the distribution of its products properly. Provider liability should also make the regulator comfortable with allowing legal agreements govern most aspects of the distribution of mobile money products, particularly the recruitment of third parties. In this case, a notification regime can provide the same protection as an authorisation regime, and can allow third parties to open customer accounts or handle cash-in and cash-out transactions.

Section 5 addresses the importance of transparent customer relationships, the need for customers to have effective and straightforward recourse and complaint mechanisms, the opportunity to introduce protection of the stored value through insurance, and privacy issues related to mobile money. Mobile money is striking a balance between innovative financial access and an acceptable minimum level of consumer protection. Tailored guidance from the regulator can help mobile money providers to improve transparency with their customers and prevent third party fraud.

Section 6 discusses the need for providers and policy makers to work together on the design and implementation of an interoperable environment, ensuring that interoperability brings value to the customer, makes commercial sense for the providers involved, is set up at the right time, and that regulatory and implementation risks are identified and mitigated.

Crafting a regulatory definition of mobile money

There is currently no standard regulatory definition of mobile money and electronic money (e-money) suitable for global use. However, countries that have developed their own definitions tend to echo several common elements. This paper uses the following definition of mobile money:

Mobile money is 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;
- mirrored by the value stored in an account(s) usually open in one (or more) bank(s); 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.

¹² The term “third party” is used in this paper to refer to any third party that acts as the primary customer interface on behalf of the mobile money provider, whether or not there is a legal contract that states that the service provider is legally accountable to the customer for the acts of the third party (see Section 4.1). In some countries, the term “agent,” “correspondent,” or “facilitator” is used.



The benefits of mobile money from a policy perspective

The policy debate around financial services for the poor has developed quickly since the first mobile phone-based money transfer services were launched in the mid-2000s. Today, policy makers and regulators recognise that mobile connectivity can help to extend the reach of the financial sector, but it is still not widely agreed how to construct a regulatory environment that enables this technology to reach its full potential. Finding answers is critical for both policy makers and the regulator. Mobile money has the capacity to a) make the financial sector more inclusive, stable and efficient, b) preserve its integrity, and c) improve convenience and safety for financial consumers. The Global Partnership for Financial Inclusion (GPII) points out that financial inclusion, stability, integrity, and consumer protection (“I-SIP objectives”) are mutually reinforcing public policy objectives that must be viewed collectively rather than independently in order to optimise the linkages among them.ⁱⁱⁱ Mobile money strengthens the connections between these objectives.

Mobile money has additional advantages from a public policy perspective. A variety of public sector authorities have begun to step up efforts to join the digital revolution by digitising government-to-people (G2P)^{iv} payments and conditional cash transfers, and channelling them to mobile wallets. Other efforts include more efficient tax identification and collection. Digital transfers and payments are making criminal activity more difficult since cash-based transactions are more vulnerable to opportunistic crime. Cost savings from printing, replacing, and transporting cash along the value chain are also significant.

Mobile money for financial inclusion

In some markets, mobile money is already reaching huge numbers of low-income and previously unbanked customers, moving millions of households (mostly low-income) from a cash-only economy into the formal financial system. In Kenya, Madagascar, Tanzania, and Uganda, where MNOs are allowed to offer mobile money services, the number of mobile money accounts is already higher than the number of bank accounts.^v M-PESA, the payment and transfer service operated by Safaricom, is now used by 18 million Kenyans (only 7 million have bank accounts) and processes an astounding US\$1.6 billion in payments every month. Four years after M-PESA was launched (in 2007), 86% of Kenyan households and more than 70% of Kenya’s poor and unbanked households had at least one M-PESA user.^{vi} Mobile money creates important changes in the lives of the poor: relying solely on cash keeps many people

Financial exclusion and AML/CFT risks

“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
President, Financial Action Task Force (FATF)

excluded from the formal economy, while mobile money provides a convenient and safe alternative to informal financial services and cash-based assets (see below for examples of the cost of cash).^{vii}

Mobile money also plays a critical role in any national financial inclusion strategy. **It not only reduces dependency on cash by enabling digital payments through a mobile device, but also provides a platform for customers to access a much broader range of financial services.** The complex infrastructure (mobile connectivity + networks for cash-in^{viii} and cash-out services^{ix} + mobile money account) that people use to transact and store their money electronically can be used by a range of financial institutions to offer other services and products, which improves efficiency and competition in the financial sector.^x

Mobile money for financial stability

According to the GPFI, an inclusive financial sector has a more diversified and stable retail deposit base, which makes the financial system more stable overall.^{xi} **In terms of systemic risk^{xii} to the financial sector, mobile money currently poses less overall risk than banking and other payment systems.** In fact, “large numbers of clients that frequently transact small amounts [...] pose limited systemic risk because they represent such a small share of overall financial sector assets.”^{xiii} For these reasons, mobile money deployments are not subject to the same regulations and international principles of the Systemically Important Payment Systems (SIPS) (the major payment clearing systems or Real Time Gross Settlement that individual countries use). Mobile money systems are not subject to the same set of rules because it is believed that they would not endanger the rest of the economy if they failed.^{xiv} The case of M-PESA is emblematic. Even if the world’s biggest mobile money deployment were to fail completely, the regulator contends this would pose little risk to Kenya’s financial sector as a whole. In 2010 the accumulated balance of all M-PESA accounts represented just 0.2% of bank deposits by value, and although M-PESA transactions represented about 70% of all electronic transactions in the country, it only accounted for 2.3% of the total value. Even with its wide reach, M-PESA is far from posing a systemic risk.

In terms of mitigating liquidity risks,^{xv} the prudential requirements that regulators and mobile money deployments typically put in place are effective at safeguarding customers’ electronically stored value (see Sections 2 and 4). As Hannig and Jensen point out, technology-based financial inclusion services such as mobile phone banking have “idiosyncratic risk profiles that can be appropriately regulated and supervised.”^{xvi}

In the future, mobile money could play an important role in helping policy makers and households to manage crises that affect the stability of the financial system. The speed of mobile has already made it a valuable response tool in the wake of natural disasters such as the earthquakes in Rwanda^{xvii} and Haiti. Catastrophic events such as these can threaten liquidity and prompt a “run on the bank”, but mobile money has a remarkable capacity to cope with severe shocks to the local economy and curb a liquidity crisis. The time it takes for a mobile network to be restored (and used to remit money to affected areas) is significantly less than the time needed to rebuild physical infrastructure, such as land lines used for POS and ATMs, or to manage ATMs and bank branches. Governments, financial institutions, and households can use mobile money to make digital payments and rapidly move capital to areas in crisis. As digitisation expands, geospatial analysis will become an invaluable tool for governments to monitor financial flows, prevent and manage liquidity issues, and maintain financial stability.

Mobile money and inflation^{xviii}

“[I wonder] how M-PESA is linked to inflation: this is pure innovation which has simplified the way bills are paid and money transferred... but not fuelling inflation. It cannot in any way.”

Professor Benno Ndulu
Governor, Bank of Tanzania

Mobile money for financial integrity^{xix}

The risk of mobile money infrastructure being used to finance terrorism or to launder capital is very low due to the nature of mobile channels and devices, which track all transactions and localise users, and to the transaction limits that allow customers to transact relatively small amounts of money. Mobile money is a powerful tool in AML/CFT strategies to strengthen the integrity of the financial system. Digitising payments and transfers allows mobile money providers to monitor large volumes of electronic transactions efficiently, to detect patterns and profiles, and in general lower the number of transactions conducted outside the digital system, which makes it easier to identify suspicious transactions.

Financial exclusion poses significant risks to the integrity of the financial system. According to the Financial Action Task Force (FATF), “financial exclusion risks arise when persons have to seek their financial services from informal providers in the cash economy. From a FATF perspective, the risks include financial crimes committed by informal service providers, as well as threats to the integrity of formal financial services, as due diligence inquiries fail when money trails disappear in the cash economy.”^{xx} Mobile money helps to reduce these risks by bringing large numbers of users and transactions into the formal system at a relatively low cost.

Mobile money for consumer protection

Experience with mobile money to date suggests that it is a cheaper, more secure, and more reliable way to provide financial services to the poor than other alternatives in the informal economy and less suitable traditional formal financial services. In 2009, a FinAccess survey in Kenya revealed that Kenyans considered M-PESA to be the safest way to transfer money, the least expensive, the fastest, and the easiest to access. Bus/matatu and friends/family were identified as the riskiest methods.^{xxi} For consumers, the benefits of innovative mobile models seem to far outweigh the risks.^{xxii} A growing body of research is indicating that digital financial inclusion empowers and protects consumers who would otherwise be forced to rely on informal and semi-formal financial services.^{xxiii}

Consumers benefit from the security of mobile channels and devices, as well as from the business incentives providers have to build a solid reputation and drive public confidence, satisfaction, and customer adoption.^{xxiv} MNOs are particularly motivated to maintain the high reputation and customer loyalty they have established for GSM services in the vast majority of markets where they have launched mobile money deployments.

Reducing the costs (and risks) of cash

Cash is still the most prevalent payment method, but it is also the most expensive and the least secure. The European Commission (EC) has calculated that the total cost of processing all payment methods, including cash, cheques, and payment cards, is equivalent to 2%–3% of a country’s GDP. The EC estimates that cash accounts for more than two-thirds of this cost. McKinsey & Company estimates that “society spends about €200 (£180) a year per person to cover the cost of cash” and the “real” cost of cash to a retailer is 1.3% of the purchase price – comparable to a card transaction fee. The Dutch central bank, DNB, has estimated the annual cost of cash at €300 per family. The direct cost of cash management to the Nigerian banking industry was estimated to be N192 billion (approximately US\$1.9 billion) in 2012.^{xxv}

Most poor households live in a cash-based economy, relying on tangible assets such as cash, jewellery, or livestock. This creates considerable tension in their financial lives (storing their money safely, the cost of transporting physical assets, and barriers to saving) and keeps them marginalised from the formal economy.^{xxvi}

Mobile money and monetary policy

Mobile money does not create money. The use of e-money is on the rise in some countries, but not enough to have an impact on monetary supply or policy. Even if usage became much more widespread, there are mechanisms that prevent mobile money from affecting monetary policies, particularly the fact that mobile money converted by a non-bank provider is fully backed by cash held in a fully prudentially regulated institution (see Section 2.1). The Bank for International Settlement (BIS) agrees that central banks would retain control over short-term rates (see full quote below).

In the case of Kenya, for instance, in terms of monetary aggregates, economists consider mobile money stored and transferred by Safaricom customers through M-PESA to fall within “M1”, a category of money supply that includes all physical money, such as coins and currency, demand deposits, and Negotiable Order of Withdrawal (NOW) accounts. Economists use the M1 to quantify the amount of money in circulation. It is a very liquid measure of the money supply as it contains cash and assets that can be quickly converted to currency.

One of the most important functions of commercial banks is to make loans to borrowers with the deposits they have accepted. This constitutes a form of money multiplication or creation. Mobile money providers, on the other hand, are prohibited from on-lending funds entrusted to them by customers, so they do not participate in money creation or the expansion of what economists call M2. However, in most jurisdictions, they are required to deposit customers’ funds in a bank. If that bank in turn on-lends to borrowers, then the value stored as e-money will lead to money creation, but in exactly the same way as any savings mobilisation would. Intermediation, which drives money creation, will always be undertaken by licensed and supervised banks.^{xxvii}

Mobile money and monetary policy^{xxviii}

“Although electronic money has become more important in some countries, the impact of these developments on the composition of the monetary base is considered negligible thus far. Moreover, even if the usage of electronic money were to expand massively, there would still be various ways in which central banks could preserve a tight link between electronic money and central bank money and to keep control over short-term rates. Most central banks therefore judge that the influence of innovations in retail payments on monetary policy is neutral or of low importance.”

Working Group on Innovations in Retail Payments
Committee on Payment and Settlement Systems
Bank for International Settlements (BIS)

1. Why should regulators establish an open and level playing field?

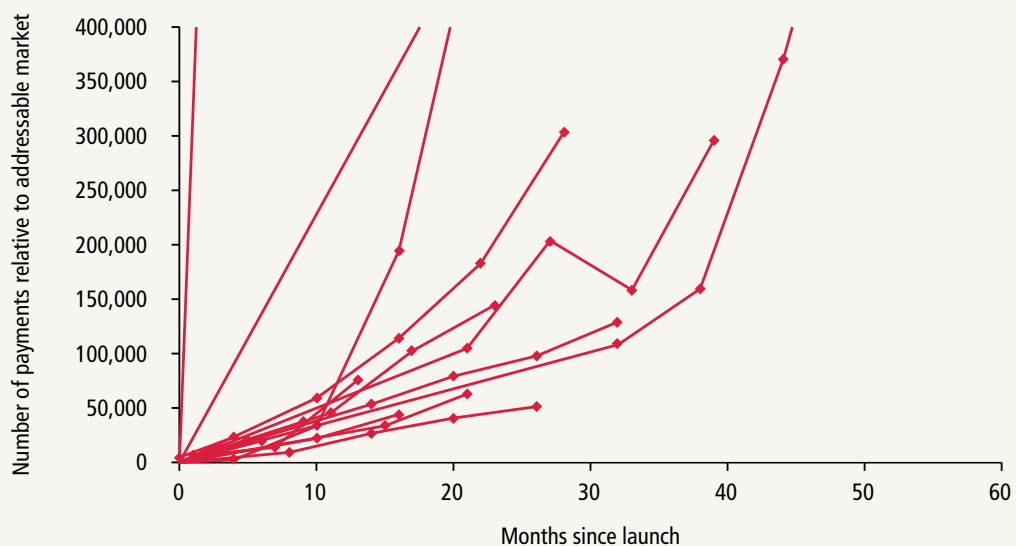
To unleash the potential of mobile money, regulators must create an open and level playing field that allows both banks and non-bank providers to offer mobile money services – particularly MNOs, which are well suited to building sustainable services and extending the reach of the formal financial sector rapidly and soundly. This would help to advance financial inclusion, stability, integrity, and consumer protection, and is consistent with the Bank for International Settlements' (BIS) international best practices in financial regulation.

1.1 Commercial lessons: opening the market to providers with different value propositions

Mobile money has grown most rapidly when both banks and non-bank payment providers such as MNOs have been allowed to directly offer mobile money services to end-user.

Globally, the overwhelming majority of mobile money customers are using services directly offered by MNOs. The chart below shows the results of the 2012 Global Mobile Money Adoption Survey, which analysed over 70 deployments around the world.¹³ The chart indicates that, in June 2012, there were 14 fast-growing mobile money deployments, revealed by the number of payments relative to the size of addressable market¹⁴ (vertical axis) and the time since launch (horizontal axis). Only two of these deployments are located outside the jurisdictions where MNOs are allowed to provide mobile money services.

Figure 2: In 10 countries 14 mobile money deployments are growing fast. Only two of these deployments are located outside the jurisdictions where MNOs are allowed to provide mobile money services.



¹³ Claire Pénicaud (2013), *cit.*

¹⁴ For MNOs, the addressable market is their GSM base; for non-MNOs, the addressable market is the number of unique mobile money subscribers in their country.

The vast majority of the fastest growing deployments are operating in markets where the regulator allows both banks and MNOs, to offer mobile money services. In four of those markets – Kenya, Madagascar, Tanzania, and Uganda – the number of mobile money accounts opened by MNOs is higher than the number of bank accounts; a clear indication that mobile money is allowing more people to access financial services than the banking industry ever has.¹⁵

In Pakistan, a market where the regulator does not permit non-banks to provide mobile money services, the number of registered and active customers is growing significantly, but the main deployment leading this growth is operated by an MNO (Telenor Pakistan) through its majority-owned subsidiary Tameer Bank, which it acquired in order to offer mobile money services. 41% of Tameer Bank / Telenor Pakistan's Easypaisa's users live on less than \$2.50 per day¹⁶

The number of countries that have enabled or are enabling the development of an open and competitive market is increasing, which is allowing MNOs to launch their deployments either directly or through wholly owned separate legal entities. A number of countries have issued enabling regulation, and in others, financial sector authorities have allowed non-bank providers to operate within an enabling monitoring framework (covering prudential, reporting, and market conduct requirements). These countries include Bolivia, Burundi, Democratic Republic of Congo, Fiji, Kenya, Madagascar, Malawi, Malaysia, Morocco, Namibia, Paraguay, Peru, the Philippines, Rwanda, Somaliland, Sri Lanka, Tanzania, Tonga, Uganda, Zambia, Zimbabwe, the eight countries of the West African Economic and Monetary Union (WAEMU), and others. Brazil and El Salvador are also working on regulations to create an open and level playing field.

There are a number of reasons why MNOs are particularly well suited to mobile money services:

- MNOs have a number of assets they can leverage to offer mobile money services. In addition to their experience with airtime distribution, the SIM card and data channel on customer handsets give users and third parties an interactive interface at a very low cost. An important intangible asset is the brand recognition and confidence that MNOs have established among customers in many countries.
- MNOs bring a number of skills that are both central to their core business and necessary for mobile money, including expertise in mass marketing and building and managing a broad distribution infrastructure.
- MNOs use mobile money to cross-sell new services to customers they already serve (their own subscribers) and to compete for customers on other networks. They are able to generate some unique forms of indirect revenue from mobile money, which should make it easier for them to launch and sustain services. These include savings from airtime distribution, reduced churn, and increased share of wallet for voice and SMS.¹⁷ Not surprisingly then, MNOs are often more keen to make investments in building and scaling mobile money services than banks and other non-banks.

Nevertheless, regulators in some countries have prohibited non-banks from issuing electronic money and offering mobile money accounts. Banks have not necessarily filled this opening in the market, however, in part because opportunities at the bottom of the pyramid require them to radically rework their business model. This is a change that many banks are reluctant to make given that the burgeoning middle class in developing countries is an attractive growth opportunity that fits into their existing business model.¹⁸ Banks also lack the same assets and incentives as MNOs.

Banks and MNOs always need to work together to offer mobile money services, and there are a wide variety of partnership opportunities.¹⁹ However, **since MNOs are usually the primary drivers of mobile money deployments, regulators that opt to allow only bank-led models are effectively forcing banks and MNOs into a type of partnership that might not make commercial and operational sense.**²⁰ These arrangements between MNOs and banks tend to have serious shortcomings and ultimately limit customer adoption. For example, a bank responsible for regulatory compliance may create obstacles to the development of mobile money if it does not fully understand how these services operate. It may take a conservative, non-risk-based position on AML/CFT requirements, and block the design of tailored CDD procedures. UNCTAD has identified examples of partner banks that have delayed MNO proposals to launch mobile money deployments because they considered mobile money products to be in competition with their products.²¹

15 Claire Pénicaud (2013), *cit.*

16 The figure refers to a study conducted 16 months after the deployment was launched. Source: <http://www.cgap.org/blog/does-branchless-banking-reach-poor-people-evidence-pakistan>. This figure is meaningful because it shows that mobile money is capable of reaching large numbers of poor and low-income households, but the vast majority of easyPaisa users do not yet have mobile money accounts. Instead, they conduct over-the-counter (OTC) transactions where the agent processes the transaction on the customer's behalf. OTC customers do not have an account and therefore no way to store, access, or accumulate funds.

17 Paul Leishman (2011), *cit.*

18 Ann-Byrd Platt (2011), "The Business Case for Branchless Banking: What's Missing?," MicroSave Briefing Note 97.

19 "It is impossible for a mobile network operator to offer mobile money without a bank: at minimum, a bank must hold the deposits which back the electronic value stored in customers' and agents' wallets. Conversely, it is impossible for a bank to offer mobile money without an operator: at minimum, an operator must provide the data channel which allows customers and agents to initiate transactions using their handsets." Neil Davidson (2011), "Mapping and Effectively Structuring Operator-Bank Relationships to Offer Mobile Money for the Unbanked," GSMA Mobile Money for the Unbanked (MMU) paper. Available at <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/mappingandeffectivestructuringfinal2643.pdf>.

20 *Ibid.*

21 United Nations Conference on Trade and Development (UNCTAD) (2012), "Mobile Money for Business Development in the East African Community. A Comparative Study of Existing Platforms and Regulations," Geneva, Switzerland.

In Sri Lanka, the regulator creates a level playing field and mobile money takes off

In 2012 the Central Bank of Sri Lanka (CBSL) completed the design of the regulatory architecture for mobile money, establishing a framework that allowed Dialog to register over 810,000 mobile money customers in 6 months.

In August 2007, the National Development Bank, a licensed commercial bank, and Dialog Axiata, the main MNO in Sri Lanka, launched a mobile money product called eZ Pay. Based on the regulatory framework, customers needed to have a bank account to sign up for the service and had to go through a burdensome process to verify their identity. Dialog partnered with another bank and a MFI, but the service never gained traction. By March 2012, Dialog had only registered 15,000 eZ Pay customers.^{xxx}

In 2011 the Central Bank issued two guidelines for regulating two distinct mobile money products: the first was an e-wallet linked to a bank account, and the second was an e-wallet that must have equivalent funds held in a custodian account by a non-bank provider, which can be a mobile operator.^{xxx}

In April 2012 Dialog was awarded a license to provide mobile money services under the Payments and Settlements System Act no. 28 of 2005. The CBSL agreed to let Dialog register clients without requiring them to have a bank account, and relaxed the KYC requirements for the due diligence of new customers. In June 2012 Dialog launched its telco-led mobile money service under the name eZ Cash (eZ Pay, the bank-led service, is still available).

The evolution of CBSL's approach created a level playing field for banks and non-bank providers, and allowed MNOs to launch their own mobile money deployments with a competitive set of products.

Thanks to the new regulatory approach, customers can activate the mobile money service simply by dialling a number from their mobile phone. Dialog can rely on the KYC information already stored in its database from the SIM card registration to verify the identities of its customers.

The maximum amount that a new eZ Cash customer can add to their e-wallet is Rs. 10,000 (US\$80). This "Classic Account" allows them to send money (up to Rs. 5,000 per each transaction), pay utility bills (up to Rs. 10,000), and to conduct other transactions such as web payments, microinsurance, microfinance, and subscription payments.

If customers want to conduct transactions over these limits, they can activate a Power Account with a top-up limit of Rs. 25,000 (US\$200) and higher transaction limits. To activate a Power Account, a customer must visit a Dialog Customer Care Centre to confirm his/her identity. As of today, 4,000 customers have signed up for a Power Account. Among eZ Cash customers, the usage rate is growing at a similar speed as the number of registrations.

In compliance with the regulatory requirements set up by the CBSL to safeguard customer money, the stored value corresponding to the value of the electronic money in circulation is held by Hatton National Bank PLC, which acts as a custodial bank for eZ Cash. Dialog's eZ Cash is further secured through a trust instrument administered by Deutsche Bank AG.^{xxxi}

eZ Cash has seen remarkable growth: by June 2012, more than 370,000 customers had signed up to eZ Cash, and in January 2013 this number reached 810,000. This growth is particularly impressive given that in June 2011, almost three years after the launch of eZ Cash, only 10,000 clients had signed up for the service.

Also, in these bank-led deployments the mobile money's already thin profit margin needs to be divided across two parties (a bank and an MNO) in a way that is acceptable to both. Such deals can sometimes be challenging to negotiate, and reduced profit margin can impede serious rollouts in some cases.

Some regulators hesitate to authorise non-bank providers because they do not offer a full range of financial services to customers. They reason that it would be better for customers to be "banked" and use a more complete suite of financial services (e.g. loans and interest-bearing savings). However, this underestimates the challenge banks face in reaching the unbanked and overlooks the fact that, in many markets, mobile money services from non-bank providers have already become the entry point for customers to make payments and transfers, to store money safely, and to access other financial services that banks and other financial institutions like insurance companies offer. As the Bill & Melinda Gates Foundation point out, "a more open (but level) playing field can help spark some more competition and innovation in financial services."²²

1.2 The regulatory context: applicable international principles

The Bank for International Settlements (BIS) has created a framework of regulatory principles that, although designed for international remittances, provides useful and relevant guidance for mobile money as well.²³

According to the BIS,²⁴ regulating solely by type of entity may reduce the effectiveness of regulations and create market distortion, and any regulation intervention should aim to create a level playing field between equivalent services rather than between different providers. In Principle n.3, the BIS rejects any form of discrimination between different types of providers that offer equivalent services based on "the nature of the provider's other lines of business."²⁵ Applying the principle of non-discrimination also promotes fair and equitable competition across the financial sector.

Regulations should instead be designed by type of service, such as payments, savings, credit, and insurance, not by the entity that provides them. The function and characteristics of each service must be assessed and regulations calibrated according to the risks it poses so that customers can use it safely and conveniently.

In 2011, the BIS released an analysis of mobile money and explicitly pointed out that the regulatory framework needs to enable entities, including non-banks, to get licenses to operate as payment service providers, e-money issuers, and/or money transfer providers. These institutions would not be allowed to invest or intermediate the funds they receive and can therefore be regulated differently than a credit-issuing institution (a bank). They should be regulated depending on the type of services they offer, in a manner proportionate to the specific risk of the service.²⁶

Enabling regulation in the Philippines

37% of municipalities in the Philippines do not have a bank branch, but 80% of people have a mobile phone. The central bank recognised a significant opportunity and developed regulation that allows MNOs to compete with banks in delivering mobile money services through a dedicated subsidiary. Competition from MNO-based remittances has not only enriched the variety of services available, it has also been an important driver in lowering the price of remittances – a critical issue in a country where remittances are an important part of the economy. External remittances alone make up 10% of GDP and internal remittances sent by individuals working in urban areas to family members in the provinces are an important part of daily life in the Philippines.

"The mere entry of **competition has improved the cost and quality of services** and that is really a big win." – Nestor Espenilla Jr, Deputy Governor of Bangko Sentral ng Pilipinas (BSP) and Chair of the Alliance for Financial Inclusion (AFI) Steering Committee.^{xxxii}

- 22 Claire Alexandre (2011), "What Can Branchless Banking Do to Advance the Field, and What Can It Not Do? From Mobile Banking to Point of Service," 2011 Global Microcredit Summit Commissioned Workshop Paper. Available at <http://www.globalmicrocreditsummit2011.org>.
- 23 According to the Committee on Payment and Settlement Systems (CPSS) at the Bank for International Settlements. See Bank for International Settlements (2012), "From Remittances to M-Payments: Understanding 'Alternative' Means of Payment Within the Common Framework of Retail Payment System Regulation," Consultative Report. Available at [http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/From_remittances_to_m-payments_consultative_report\(8-8\).pdf](http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/From_remittances_to_m-payments_consultative_report(8-8).pdf).
- 24 Bank for International Settlements (BIS) Committee on Payment and Settlement Systems and The World Bank (2007), "General principles for international remittance services." Available at <http://siteresources.worldbank.org/NEWS/Resources/GeneralPrinciplesforIntRemittances.pdf>.
- 25 *Ibid.*, p. 23.
- 26 Michael Klein and Peter Dittus (2011), "On harnessing the potential of financial inclusion." Bank for International Settlements (BIS) Working Paper n. 347. Available at <http://www.bis.org/publ/work347.htm>.

2. How is customer money being safeguarded?

27 Prudential requirements aim to maintain the integrity of the institution's capital and a certain level of liquidity. They are intended to mitigate credit and liquidity risks and might include minimum capital ratios, capital adequacy measurement systems, reserve requirements, or other measures intended to preserve the liquidity of the provider. There is a high compliance cost associated with these requirements. Typically prudential rules apply (albeit to a different extent) to all institutions that collect public deposits and mobilise retail savings in order to: a) preserve the solvency of the financial institution; b) protect depositors' and other creditors' rights; and c) minimize the impact of the insolvency of one institution on other providers and the financial system as a whole (the so-called "domino effect"). Non-bank mobile money providers are also prudentially regulated to safeguard customer funds. More stringent prudential requirements are typically required when customer funds are intermediated, such as in banking (see footnote 32).

Non-prudential rules regulate the operational aspects of a financial institution, including conduct of business (customer relationships and the protection of their assets), competition, fraud and crime prevention, and governance. Examples of non-prudential rules include the regulation of interest rates, disclosure of contractual terms and conditions, limits to foreign ownership, the functions and requirements of directors and managers, internal structure and organization, reporting, and statements. Non-prudential regulation is commonly described as all the rules that govern financial activities other than those covered by prudential regulation.

28 Slightly different approaches have been taken by regulators that, rather than requiring the entire e-money float to be held in a bank, have allowed it to be invested in low-risk securities such as government bonds.

29 Michael Tarazi and Paul Breloff (2010), "Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds," CGAP Focus Note 63. Available at <http://www.cgap.org/sites/default/files/CGAP-Focus-Note-Nonbank-E-Money-Issuers-Regulatory-Approaches-to-Protecting-Customer-Funds-Jul-2010.pdf>

30 See <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000821047&dateTexte=>

31 See Banque Centrale du Congo, Instruction n.24/2011.

32 Financial intermediation is business conducted or services offered by a financial intermediary (typically a bank, but a non-bank financial institution) that accepts money from individuals or entities with capital surpluses and then lends it (directly through loans or indirectly through capital markets) to individuals or entities with capital deficits to earn a profit. Several risks can be associated with financial intermediation, such as interest rate risk, market risk, credit risk, off-balance-sheet risk, foreign exchange risk, country or sovereign risk, technology risk, operational risk, liquidity risk, and insolvency risk.

Certain risks posed by licensed non-bank mobile money providers can be successfully mitigated through prudential requirements that safeguard funds entering the system and meet customer demand to cash out electronic value.

Based on the arguments laid out in the previous section (which build on the positions of the BIS), mobile money regulation should be designed around the specific risks of the products on offer, and these risks can be mitigated without compromising the business models that drive these product offerings.

This section discusses how, in jurisdictions where non-bank mobile money providers are licensed, certain risks posed by this business model have been successfully mitigated through prudential requirements aimed at safeguarding funds entering the system and meeting customer demand for "cashing out" electronic value.

2.1 Prudential requirements for safeguarding customer money

A key prudential requirement²⁷ typically imposed by regulators to ensure a customer's money is available when the customer wants to redeem it is that the non-bank mobile money provider maintains liquid assets equal in value to the amount of money issued electronically.

One common approach is to require assets to be ring-fenced and held in a bank account. The funds can be deposited in one or several commercial banks (the latter is required in Afghanistan) that are fully prudentially regulated. In this way, any amount that passes through the mobile money system is backed 100% by the pooled account or accounts.²⁸

CGAP has noted that these requirements are more stringent than those imposed on deposit-taking financial institutions, "which are typically subject to reserve requirements mandating only some small portion of overall deposits to be kept in liquid form – typically cash – to satisfy potential depositor claims."²⁹

Customer funds are usually pooled and held by the bank(s) in the name of the issuer. Therefore, some regulators have also required that the funds backing mobile money stored value are protected from institutional risks, such as claims made by creditors in cases of issuer bankruptcy. This protection is guaranteed by establishing a "trust" or fiduciary agreement, under which funds are held on behalf of the clients. The concept of a trust originally was developed in common law jurisdictions, but recently some countries with a civil law legal tradition have adopted similar concepts. France, for example, passed a law establishing the concept of "*la fiducie*" in 2007,³⁰ and this concept is referenced in the Central Bank of Congo's e-money regulation as a mechanism to ensure that customers can recover their funds in the event of issuer failure.³¹

The risk of mobile money customers losing the money they have stored in the system is mitigated if:

- 100% of the cash backing mobile money is held in a fully prudentially regulated institution, such as a bank or an MFI, or in more than one institution (depending on the stage of development of the deployment);
- the non-bank mobile money provider does not intermediate the funds;³² and
- customer funds are isolated from the issuer's funds and protected from claims by the issuer's creditors.

Table 1. Examples of requirements for safeguarding customer money.^{xxxiii}

Afghanistan	Funds must be held in a local currency in licensed banks.
Namibia	Funds must be unencumbered and kept in pooled deposit accounts. In exceptional circumstances, a provider may request a waiver, provided that 100% of outstanding funds are set aside and that these funds are protected against loss and creditors' claims.
Democratic Republic of Congo	Issued e-money value must be matched by an equivalent sum held in a ring-fenced bank account.
Kenya (draft)	Funds must be unencumbered and kept in banks or any other liquid asset permitted by the central bank.
Philippines	Must maintain unencumbered liquid assets in the form of bank deposits, certain government securities, or any other liquid asset permitted by the central bank.
WAEMU (BCEAO)	Funds must be deposited in banks, invested in central government or central bank securities, or invested in other approved corporate securities. Total value of assets held as securities may not exceed 10 times the provider's capital.
European Union	Funds must be deposited in banks or invested in low-risk liquid assets (such as securities issued by governments and certain corporate entities). Alternatively, providers may take out sufficient insurance to cover any deficiency.

2.2 Minimum capital requirements

Minimum capital requirements are not necessary to ensure that mobile money providers have sufficient assets to cover customer claims in the event of insolvency or financial instability. In fact, non-bank mobile money providers do not require this buffer because the e-float is backed fully by the amount deposited in the pooled account.

In banking regulation, a minimum capital requirement is a prudential rule with three functions:

- 1) It stipulates what assets the provider must hold as a minimum requirement to insure creditors (including depositors) from insolvency risk and minimise subsequent system disruptions (guarantee function).
- 2) It ensures that the institution can cover operational costs such as the infrastructure, management information system (MIS), and start-up losses to reach a viable scale (organisational function).
- 3) It aims to set a cost that creates a barrier to market entry for new institutions that want to pursue the business initiative (selective function).

In terms of mobile money, these requirements should be evaluated based on the characteristics of the business and how certain risks are mitigated through other prudential requirements.

The first function should take into account that non-bank mobile money providers are already subject to the highest level of prudential regulation possible – a 100% reserve requirement – which makes a minimum capital requirement unnecessary.

The second function does not take into account that established banks and MNOs launch the vast majority of mobile money deployments and cover the operational and start-up costs with their investment capital. However, in some markets, high minimum capital requirements can increase compliance costs to a level that makes the business case difficult even for larger companies to justify.

The third function should take into account that mobile money is a new sector and policy makers do not want to deter smaller companies from entering the market, which would hinder competition and innovation. In fact, new market entrants can contribute greatly to the development of mobile money products and mobile technology (software, user interfaces, networks, etc.). Rather than imposing a minimum capital requirement, regulators may want to conduct a deeper review of the license applications of small players before granting a license. This way, the regulator can examine, for example, the features of the provider's technology platform and its consumer protection policies, and screen out ill-equipped, unsustainable players.

Table 2. Minimum capital requirements for mobile money deployments.^{xxxiv}

Nominal \$USD					
Afghanistan	Namibia	EU	WAEMU (BCEAO)	Kenya (draft)	Philippines
200,000	320,000	430,000	550,000	650,000	2 million
As multiple of PPP GDP/Per Capita					
EU	Namibia	Afghanistan	Kenya (draft)	WAEMU (BCEAO)	Philippines
15x	52x	234x	417x	494x	619x

Finally, “don’t licence what you can’t supervise” is an important principle in all areas of the financial sector. In terms of mobile money, it should be recognised that mobile money oversight, unlike banking or MFI oversight, requires limited onsite supervision and can be conducted primarily offsite and electronically (which requires less resources).

Given that other prudential requirements already satisfy the guarantee function, that mobile money requires significant upfront investment from providers, and that innovation and competition should be encouraged in this new sector, lowering or even eliminating minimum capital requirements should be considered, particularly for those providers that target underserved areas and clientele. Also, when establishing a minimum capital requirement it is important to look not only at the nominal value, but also its value as a multiple of the GDP per capita adjusted for purchasing power parity (PPP) (see Table 2).

2.3 Interest-bearing mobile money accounts

In a paper written for the World Economic Forum, CGAP’s Ehrbeck and Tarazi (2011) argue that mobile money accounts, which already provide a safe place to store value, should be able to offer poor users the full benefits and security of a savings account³³. Considering that 75% of Ugandans who saved cash in 2009 lost some of their savings,³⁴ and that the country’s banking sector is not yet meeting the needs of most unbanked customers, an e-money account accessed through a mobile device or nearby third party would be a convenient, safe, and desirable option for many. Ehrbeck and Tarazi also suggest that **non-bank mobile money providers should be allowed to pay interest on an e-float linked to a customer’s account balance** because this would provide a strong incentive for unbanked people to join the formal financial system via mobile money platforms.

Non-bank mobile money providers should be allowed to pay interest^{xxxv}

“When pressed for a reason, regulators often simply state that paying interest is a banking activity. However, definitions of banking activity typically focus on taking deposits and, in most regulations, intermediating deposits through lending. Intermediating deposits places them at risk, thereby raising systemic concerns prudential regulation is intended to mitigate. While non-bank e-money issuers are arguably taking deposits, these deposits, if totally held in a bank, are not intermediated by the issuer. Even when regulation expressly defines the payment of interest as a banking activity, it is hard to identify what risk lies in allowing non-bank issuers to pay interest.”

Tilman Ehrbeck and Michael Tarazi
Consultative Group to Assist the Poor (CGAP)

33 Tilman Ehrbeck and Michael Tarazi (2011), “Putting the Banking in Branchless Banking: Regulation and the Case for Interest-Bearing and Insured E-money Savings Accounts,” in World Economic Forum’s Mobile Financial Services Development Report, 2011. Available at http://www3.weforum.org/docs/WEF_MFSD_Report_2011.pdf.

34 Graham A.N. Wright and Leonard Mutesasira, 2001, “The Relative Risks to the Savings of Poor People,” MicroSave Research Paper. Available at http://www.microfinancegateway.org/gm/document-1.9.28889/26216_file_the_relative_risks_.pdf.

3. What customer due diligence measures are appropriate for mobile money?

Mobile money reduces the risk of money laundering and terrorist financing since electronic transactions can be monitored and traced more easily than cash. Proportional AML/CFT regimes and simplified customer due diligence (CDD) requirements are crucial for customer adoption of mobile money.

Customer due diligence (CDD) requirements are one of the major obstacles to developing and scaling mobile money deployments. Extending digital access to the formal financial system may collide with the lack of an identification system in many countries, as well as AML/CFT regimes that do not allow a proportional approach to the risks posed by mobile money products, both of which can make it too difficult for customers to sign up or too onerous (if not impossible) for providers to offer services to the unbanked.

This is one area in which financial sector regulators are making significant efforts to apply the principle of proportionality, which balances the need to preserve the integrity of the financial system with expanding financial inclusion. The scope for CDD can be limited, however, if other controls are already in place to reduce the AML/CFT risks of a mobile money service. Many regulators follow the recommendations of the Financial Action Task Force (FATF-GAFI), the global Standard-Setting Body (SSB) in this area,³⁵ considering uniform application of know-your-customer (KYC) rules to be unnecessary in light of other risk mitigation tools such as monitoring systems and transaction limits.

3.1 The risks of cash versus mobile money for money laundering (ML) and financing of terrorism (FT)

The World Bank has identified four potential vulnerabilities of mobile money services to ML/FT: anonymity, elusiveness, rapidity, and lack of oversight.³⁶ Since every payment system has some degree of ML/FT vulnerability, and because cash transactions are the predominant type of transaction in markets with the highest demand for (and success with) mobile money services, it is helpful to conduct a generic risk and vulnerability assessment of cash and mobile transactions based on the World Bank's risk factors.³⁷ The assessment will reveal that **the inherent characteristics of mobile money protect the integrity of the financial system from the risks of cash.**

- **Anonymity:** Mobile transactions are less anonymous than cash because they can be linked to a unique mobile number and transactions are recorded and traceable (by the sender's mobile number, amount, receiver's mobile number, and date). When cash is used, on the other hand, there is neither a unique identifier for the user nor a way to trace the payment. Building customer profiles, including registration information, can help to further reduce the anonymity of mobile money users.

³⁵ The Financial Action Task Force (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 proliferation of weapons of mass destruction. FATF comprises 34 member countries, most of which are developed countries.

³⁶ Pierre Chatain, Raul Hernandez-Coss, Kamil Borowik, and Andrew Zerzan (2008), "Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing," World Bank Working Paper 146. Available at http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf.

³⁷ The assessment is based on Marina Solin and Andrew Zerzan (2010), "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks," GSMA Discussion Paper. Available at <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/amlfinal35.pdf>.

- **Elusiveness:** Mobile money transactions are traceable in mobile operating systems as part of standard business practice. The telephone number of the sender and receiver, the time, and the amount of the transaction are all known to the mobile money provider, whereas cash transactions are completely elusive. Limits on mobile money amounts, balances, frequency and number of transactions, and real-time monitoring can make mobile money even more transparent and traceable.
- **Lack of oversight:** A mobile money provider offering mobile money services is usually regulated and MNOs usually have strict internal controls with regular internal and external auditing, whereas cash transactions lack oversight.

The only ML/FT vulnerability to which mobile money is more susceptible than cash is rapidity. Over a distance, mobile technology can make transactions much more rapid and effortless than cash. As described in the next section, automated internal controls for real-time monitoring, including restrictions on the frequency of transactions, transaction amounts, and total account turnovers in a given period, can allow MNOs to identify and prevent money laundering and funding of terrorist activities.

Little evidence so far of money laundering or terrorist financing using mobile money

There have been no cases of money laundering through mobile money services in countries where these services have thrived, and there have been no reports of terrorist financing. World Bank research indicates that, so far, mobile money has been of little interest to criminals or terrorists compared to other payment channels such as cash or the internet. Although no payment system can be 100% free of abuse, it is important to gather data that measures the attractiveness of a particular system to criminal activity.^{xxxvi}

3.2 AML/CFT regimes and KYC rules for low-value mobile money accounts

If mobile money is to contribute to financial inclusion, regulators have to consider that the average mobile money customer, particularly the unbanked, maintains a low account balance, conducts relatively small transactions, and, in many countries, lacks a permanent address and/or government-issued identification. The average value of peer-to-peer (P2P) transfers is US\$35 per transaction.³⁸

Whereas it is critical to ensure that services offered by mobile money providers (and their agents and third parties) are subject to proper controls, these controls should be flexible enough to include poor and unbanked customers. **If a risk assessment deems a product to be low risk, simplified KYC rules should be applied to permit alternative forms of customer identification and verification.**

Risk assessments of typical mobile money products in developing and emerging countries are likely to reveal that they are already low risk because:

- there are limits on:
 - the amount per transaction;
 - the amount that may be sent or received per day, month, and/or year; and/or
 - the maximum balance that may be stored at any time (see Table 3);
- identification is always required to conduct transactions above a minimum amount;
- a PIN or password authentication is always required to conduct a transaction on a mobile device since it verifies the identity of the registered user every time the SIM card is used for a transaction;
- the system allows every transaction to be monitored; and
- mobile phone localisation identifies the person making the transaction by recording the Mobile Station International Subscriber Directory Number (MSISDN) that is transacting.³⁹

38 Claire Pénicaut (2013), *cit.*

39 MSISDN is a number that uniquely identifies a subscription in a GSM or a UMTS mobile network.

Fiji, Indonesia, Mexico, Namibia, Pakistan, the Philippines, South Africa, and Sri Lanka (see the case study in Section 1) provide some interesting examples of KYC measures that strike a balance between financial inclusion and financial integrity goals. The next box features an example of how risk-based KYC helped financial inclusion efforts to reach scale.⁴⁰

Dialogue between the regulator and mobile money providers is typically an important part of understanding what kinds of customer identity verification are available, and which ones can be administered cost-effectively and promote customer adoption. For example, in many of the markets where mobile money is working best, digital photos and physical forms are not requirements. Also, some MNOs operating under a bank-MNO agreement face a unique problem in countries where the bank owns the license for the mobile money business and is primarily responsible for compliance, even if the the business owner⁴¹ is the MNO: the bank requires the same level of identity verification from mobile money clients as bank customers, even if this is not required by the regulator who would allow for simplified CCD for mobile money customers. This conservative approach undermines the efforts of both regulators and operators to bring unbanked people in the system.

Flexible customer identification in Fiji

In the Pacific, where a significant portion of the population lacks national IDs (driving licenses, social security cards, and passports), regulators allow alternative methods of verifying a customer's identity.

For instance, in Fiji, **the Central Bank and the Financial Intelligence Unit (FIU) have permitted mobile money providers (and their agents) to use a "referee letter" to verify a customer's identity.** The letter must include the name, date of birth, address, and occupation of the customer.

According to the Central Bank's guidelines, a "suitable referee" is a person who knows the customer, can confirm (to the mobile money provider) that the customer is who he or she claims to be, and can verify other personal details (such as the customer's occupation and residence). For customers who are minors or students, suitable referees include a school head teacher, school principal, landlord (for tertiary students who are renting), or parent or guardian. For other customers, such as those who reside in the rural areas or villages, suitable referees include: 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, or pundit); d) district officer or district advisory officer; e) official from the Fiji Sugar Corporation sector office (for sugar cane farmers and labourers); f) official from a district government agency, such as a social welfare office, police station, or health center; g) current or former employer; h) Justice of the Peace, Commissioner for Oaths, or Notary Public; i) own councillor; or j) employee of the mobile money provider.

40 Additional examples of AML/CFT requirements and CDD procedures in different jurisdictions can be found online in the GSMA's Mobile Money Regulatory Guide. See <http://www.gsma.com/mobilefordevelopment/mobile-money-regulatory-guide>

41 "Business owner" refers to the entity which assumes the bulk of the financial risk of offering the service. Neil Davidson (2011), cit.

3.3 Transaction limits

The risks of ML/FT can be mitigated with a few simple controls. The first is placing limits on the number of accounts a customer can hold, the frequency and volume of transactions that can be conducted, and the amount that can be transferred within a certain time period. These efforts may be effective if transaction amounts and volumes are very low (see Table 3). The second is monitoring transaction flows at the system level, which alerts the mobile money provider to suspicious transaction patterns (similar to ML/FT systems currently used by banks and the fraud systems used by MNOs). These measures reinforce each other because transaction limits force criminals and terrorists to split a transaction into several smaller ones and risk detection by the monitoring system. Customers who conduct frequent and large transactions, which pose a high ML/FT risk, can be required to register in person and risk being identified. Most importantly, mobile money providers should apply risk mitigation tools that are proportionate to the risks.

Table 3. Transaction limits^{xxxxvii}

Country		Single transaction limit (P2P)	Daily limit	Monthly limit	Annual limit	Deposit limits / maximum balance
Namibia:	Individual E-Money Accounts	\$470	\$470	\$2,350	\$11,750	\$1,175
Pakistan	Level 0 Accounts		\$160	\$ 60	\$1,270	\$1,060
	Level 1 Accounts		\$260	\$630	\$5,300	
Philippines:	E-Money Accounts			\$2,430		
Sri Lanka	Basic Account	\$40 P2P				\$80
		\$40 Utilities				
	Power Account	\$40 P2P				\$200
		\$200 Utilities				
Fiji	According to the regulations, there are no pre-set limits; rather, each service's limits must be approved by the Central Bank. In the case of Dialog, there are the approved limits:					
		None specified, although providers may wish to establish limits for accounts opened with only a 'referee letter' to fulfil the identification requirements. In the case of Digicel, the transaction limit established by the provider.				
		\$566	\$5,666			

Tailored CDD in Pakistan

In Pakistan, CDD requirements are proportionally lower for low-value accounts, but all clients must have a national ID card. The requirements have been designed by regulators from the State Bank of Pakistan (SBP) in close collaboration with managers at Telenor, who have used what they have learned from identifying airtime customers to design a flexible but compliant KYC approach to mobile money.

The SBP issued Branchless Banking Regulations in March 2008 that accommodated three types of branchless accounts (Level 1, Level 2, and Level 3) with different KYC requirements and transaction/balance limits. In 2011, the SBP amended the Regulations to add a Level '0' Account with more flexible KYC requirements. SBP introduced Level '0' Accounts "to bring the low income earning segment of society into the financial services loop."

With a Level '0' Account, an agent can send a customer's Digital Account Opening form, a digital photo of the customer, and an image of the customer's CNIC to the financial institution electronically (rather than sending the physical form and a copy of the customer's Computerized National Identity Card (CNIC) to the financial institution for further processing, which was required previously). The transaction and maximum balance limits on Level "0" Accounts are: Daily Limit Rs. 15,000 (US\$153), Monthly Limit Rs. 25,000 (\$256), Annual Limit Rs. 120,000 (\$1,228) and Maximum Balance Limit Rs. 100,000 (\$1,023).

It should be noted that digitising photos and application forms is a more onerous requirement than what is typical for many mobile money services. Third parties may not have the technological capabilities to reliably digitise those documents, and data networks do not cover large areas in many emerging markets. However, the loosening of existing KYC requirements for Level "0" accounts is commendable.

During the second quarter of 2012, the number of mobile banking accounts reached 1.45 million, a remarkable growth of 37%, and the number of active accounts increased by 66%. SBP attributed that growth to a 370% increase in Level '0' Accounts.

3.4 FATF Recommendations

International standards for AML/CFT promote financial integrity while simultaneously supporting the fight against crime. In 2012, the FATF revised its Recommendations to set an international standard for AML/CFT regulations⁴². Countries that do not comply with the FATF Recommendations run the risk of being blacklisted from participation in international banking. As a result, many countries have adopted strict AML/CFT laws and regulations, regardless of the particular ML/FT risks they face.

The 2012 Recommendations include a principle that promotes the same risk-based approach that the FATF had already been applying to AML/CFT regimes, asking national regulators to design and implement effective AML/CFT controls appropriate to both the specific risks posed by particular products and clients, and the national context. This risk assessment can be extended to the third party delivery channel as well.

Regulators may decide that reduced or simplified controls are sufficient to safeguard low-risk activities against abuse, and if they find that some financial services meet FATF criteria for exemption, they may even exclude those activities, either wholly or partially, from national AML/CFT regimes. Depending on the assessed level of risk of a mobile money product, the provider is required to take CDD measures, such as the following:

- Identify their customers and verify their identities using reliable and independent source documents, data, or information.
- Obtain information on the purpose and intended nature of the business relationship.
- Maintain comprehensive records of customer information and transactions.
- Monitor customer transactions and file a report with the Financial Intelligence Unit (FIU)⁴³ or other appropriate authorities if funds are suspected to be the proceeds of crime or linked to the financing of terrorism.

42 Financial Action Task Force (FATF) (2012), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," Paris, France. Available at <http://www.fatf-gafi.org>. The FATF Recommendations outline measures that countries, financial institutions, and certain other businesses and professions should adopt to counter ML/FT. Countries are advised to do the following: a) adopt laws that criminalise laundering the proceeds of crime and providing financial or material support to terrorists; b) establish a financial intelligence unit (FIU) to receive, analyse, and disseminate information regarding potential ML/FT transactions or activities; c) ensure appropriate and effective oversight of financial institutions; and d) cooperate with one another in investigating and prosecuting crimes. The FATF is currently working on financial inclusion guidance, new payment methods guidance, and the mutual evaluation questionnaire, and aim to finalise all documents by February 2013. A mutual evaluation is a peer review conducted on an ongoing basis to assess the extent to which the FATF Recommendations are being implemented. The evaluation is based on a standard questionnaire that applies to all countries and is conducted by a team of fellow regulators and IMF and World Bank staff. The challenge with the evaluation is that the questionnaire is designed by FATF members – primarily developed countries – whose representatives have limited knowledge of financial exclusion/inclusion, mobile money, and related policy and operational issues. There is a similar challenge with the evaluators, who are rarely trained in financial exclusion/inclusion and digital solutions. Whether and to what extent the mutual evaluation questionnaire will address financial exclusion as a risk for financial integrity, and would help evaluators to point out whether over-compliance with the FATF Recommendations is stifling innovation and inclusion, are still open questions.

43 "Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis." *Ibid.*, FATF Recommendation n. 29.

In its assessment of the ML/FT risks of different types of customers, countries or geographical areas, and of particular products, services, transactions or delivery channels, the FATF included examples of potentially lower risk situations in its interpretative notes on financial products and services. These examples represent appropriately defined and limited services for certain types of customers in order to increase access to financial services and promote financial inclusion.⁴⁴

Also, “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.”⁴⁵ One possible measure suggested by the FATF is verifying the identity of the customer and the beneficial owner if account transactions exceed a certain limit. This also seems to provide for some level of anonymity below a certain threshold.⁴⁶

44 *Ibid.*, Interpretative note n.17 to FATF Recommendation n. 10.

45 *Ibid.*, Interpretative note n.21 to FATF Recommendation n. 10.

46 *Ibid.*

47 The new Recommendations incorporate the views previously expressed by FATF documents. See Financial Action Task Force (FATF), Asia/Pacific Group on Money Laundering, and the World Bank (2011), “FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion.” Available at <http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf>.

48 In 2010 the GSMA proposed a risk assessment methodology based on the principles of the existing framework of the Financial Action Task Force (FATF) Recommendations, which intended to provide regulators and industry alike with a flexible and consistent means of assessing and mitigating the risk of ML/TF for mobile money services. Although the methodology is based on the previous version of the FATF Recommendations, it can still greatly contribute to the design of an assessment methodology under the 2012 framework. See Marina Solin and Andrew Zerzan (2010), *cit.*

49 Such as in Mexico or Peru. See the boxes in this section with the examples of Pakistan and Sri Lanka. Also see Table 3 and the GSMA Mobile Money Regulatory Guide at <http://www.gsma.com/mobilefordevelopment/mobile-money-regulatory-guide>. In future this will become easier because regulators will be able to look at the frameworks that have been successfully implemented at the local level, and that have been evaluated positively by the FATF mutual evaluation.

50 Bjørn S. Aamo (2012), “FATF’s focus on financial inclusion: protecting the integrity of the global financial system,” Presentation for 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. Available at <http://www.fatf-gafi.org/pages/>

51 *Ibid.*

Interpretative note n.16 to FATF Recommendation n.10

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

The FATF is adopting a more progressive approach since the objectives of financial inclusion and integrity are now recognised to be mutually reinforcing, and financial exclusion can be a risky issue to address (see the box in the Introduction for more details on the benefits of mobile money from a policy perspective).⁴⁷

To adopt simplified or reduced KYC measures, regulators must demonstrate that mobile money products pose a lower risk than traditional financial products (using a recognised methodology for their assessment).⁴⁸ Regulators are becoming more familiar with the risk-based approach, and practical guidance from the FATF and successful examples of risk-based KYC⁴⁹ would help them to design a proportional framework for CDD for low-risk products. Many regulators are still struggling to determine how to design their regulations in a way that does justice to the risk-based approach while still mitigating potential ML/FT risks. Such guidance and examples would prevent regulators from taking a conservative approach, which might guarantee full compliance and avoid a negative evaluation from assessors, but could be detrimental to the development of mobile money and financial inclusion.

According to the president of FATE, Bjørn S. Aamo, in many countries where the proportion of unbanked people is high, AML/CFT measures often undermine financial inclusion: “Local regulators and financial service providers do not take advantage of the flexibility offered by the AML/CFT Recommendations, mainly due to challenges when it comes to resources, capacity and coordination.”⁵⁰

For regulators and mobile money providers, the challenge is to give more people access to mobile money and other financial services, leaving less people exposed to the risks of informal and unregulated financial services. As Aamo suggests, “overly strict implementation and enforcement of AML/CFT safeguards have unintended effects, and prevent the access of legitimate businesses and consumers to the formal financial system.”⁵¹

Verifying customer identities in East Africa

Because there are no universal or national IDs in the East African Community (EAC), except in Kenya, financial regulators allow mobile money providers to accept a range of ID documents for the registration process. Currently, a customer’s identity can be verified with a voter’s card, driver’s license, valid passport, local village council letter or certificate, company- or employer-issued ID, government-issued ID, tax certificate, or national ID (only available in Kenya). Vodacom in Tanzania also accepts **reference identification, which allows a family member, employer, or friend with a recognized ID document to vouch for a customer’s identity during registration.**^{xxxviii}

4. How can distribution risks be mitigated while still allowing providers to leverage third party networks?

Banks and non-banks must outsource customer registration, cash collection, and disbursement activities to lower the cost of financial services, expand their reach, and thereby increase financial inclusion. Building an efficient mobile money distribution network depends on proportional and cost-effective regulation.

The development of distribution networks is one of the most difficult and strategically important issues facing a mobile money provider. Third parties⁵² act as frontline customer service representatives and, if well managed, provide vital cash-in/ cash-out (CICO) services to meet system-wide liquidity demands. The distribution network is also a vehicle for promoting products and customer awareness, registration, activation, and education.⁵³

To scale their distribution network, mobile money providers leverage retailers, rural banks, MFIs, money changers, and airtime resellers, which are ubiquitous in most countries. **Where third parties are equipped with the necessary information and communications technologies (ICTs), they can operate “at a fraction of the cost of opening and operating conventional bank branches (making it possible to reach vast new groups of poor customers profitably).”**⁵⁴

4.1 Mitigating distribution risks

The regulator might be tempted at times to restrict either the type of legal entity (commercial, non-profit, individual, or other) that is permitted to act as a third party, or the criteria that a third party must meet (e.g. a business license or minimum capital). However, it is important that limitations on the types and qualifications of agents and other third parties be crafted carefully in order to give providers discretion in setting criteria for mobile money agents, particularly in underserved areas where local retailers would be the best option.⁵⁵

Placing large compliance or financial constraints on agents hampers mobile money services from reaching scale, as they rely heavily on low-cost distribution at low-overhead agent points. Agents constantly evaluate the mobile money business against other potential uses of their capital.

Mobile money distribution^{xxxix}

“Until the cash-lite scenario is realized, financial providers need every incentive to acquire cash handling agents, agents need incentives to handle cash, and customers must have good reasons to use their local agents.”

Matu Mugo
Assistant Director, Bank Supervision Department
Central Bank of Kenya

52 See footnote 12.

53 Operational aspects of the provider/third party relationship are illustrated in Neil Davidson and Paul Leishman (2011), “Building, Incentivising and Managing a Network of Mobile Money Agents: A Handbook for Mobile Network Operators,” GSMA, London, UK. Available at <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2011/02/Agent-Networks-full.pdf>.

54 See Clara Veniard, “How Agent Banking Changes the Economics of Small Accounts,” Bill & Melinda Gates Foundation paper for the Global Savings Forum, 2010. Available at <http://www.gatesfoundation.org/financialservicesforthepeople/Documents/agent-banking.pdf>. The source of the quote is CGAP (2010), “Branchless Banking Diagnostic Template,” Washington, D.C. Available at <http://www.cgap.org/publications/branchless-banking-diagnostic-template>. The largest MNO in a developing country has 100-500 times more airtime reseller outlets than banks have branches (see Introduction), although it is best practice for non-bank mobile money providers to use this potential incrementally, selecting the best and most strategically located third parties for their mobile money business, investing in training, and ensuring they make a profit from the mobile money business.

55 CGAP (2012), *cit.*

Regulators often recognise that business decisions about the distribution network should be freely negotiated between the provider and the third party, and limit their intervention to set baseline standards for vetting third parties. In order to ease restrictions on how a third party can be used, regulators are relying increasingly on provider liability for the provision of third party financial services. Some jurisdictions require this liability to be expressly stated in the agreement between the provider and the third party.

Most regulators have opted for a light touch in regulating distribution networks because they recognise that the risks posed by mobile money distribution can be effectively monitored and mitigated by the providers (see Table 4).

Table 4: Risk mitigation and management in mobile money distribution^{xl}

Risk classification	Definition	Risk mitigation and management in mobile money distribution
Liquidity risk	The difficulty a company faces in meeting its operational needs and paying debts as they come due.	Cash managed by a third party as part of a retail business, but from a consumer perspective, the third party is not responsible for guaranteeing the liquidity of the deployment. For cash-out, liquidity problems may arise at the third party level from time to time, but customers can easily seek out another agent in such situations. From the customer perspective, a third party more closely resembles an ATM or a bank branch – if an ATM cannot disburse funds, the client would simply seek another one, while lack of liquidity at a bank branch can cause a run on the bank because the consumer might think that the bank is insolvent.
Solvency risk	The inability of a company to honour its debt commitment. An insolvent company owes more than it owns.	Insolvency at the agent level cannot endanger customer funds because of the pre-paid nature of their service.
Systemic risk	When the failure of one financial institution causes related institutions to fail, harming the entire market or entire market segment and the economy as a whole.	The insolvency of a third party is unlikely to have a knock-on effect that initially affects the distribution network and then spreads to other mobile money providers and the rest of the financial sector.
Operational risk	An adverse event or outcome caused by a company's people, systems, and processes.	Depends on the systems and controls put in place by the provider; third parties carry risks such as fraud and loss of cash, which is in the interest of the provider to address with appropriate training, contractual obligations, and surveillance. In the end, the provider is responsible for its third parties (see section 4.1).
Settlement risk	When one party fails to deliver the terms of a contract with another party at the time of settlement. Settlement risk can be the risk associated with default at settlement and any differences in the timing of the settlement.	Not if it is real time settlement.
Integrity risk	See sections 3, 4.3, and 4.4	Electronic surveillance allows traceability, and transaction amounts are limited to mitigate the risk of abuse.
Reputational risk	Refers to the trustworthiness of business. Damage to a firm's reputation can result in lost revenue or destruction of shareholder value even if the company is not found guilty of a crime.	The reputation of the third party is linked to the reputation of the MNO or the bank, and vice versa. Reputation is a key asset for providers, particularly MNOs with established customer relationships.

4.2 Liability for third parties

Making the provider liable for the acts of its third party is often the tipping point for regulators to permit the use of third parties. The provider is made liable for third party actions that are executed on the provider's behalf during the execution of the fiduciary duty included within the agency agreement. This is consistent with civil law and general regulatory principles under common law, where the provider is referred to as the "principal" and the third party as the "attorney-in-fact" or "fiduciary of the principal." If the provider is ultimately liable for third party actions or omissions, regulators will be more likely to ease restrictions on third party eligibility, location, third party due diligence, and permitting a third party to be deployed.

However, it is important to limit the **provider's liability to the actions that the third party executes on behalf of the provider and in execution of the principal/ third party contract**, and not to all actions undertaken by the third party. Certainly the provider cannot be held responsible for risks such as imposter third parties that take cash from the public without the principal's knowledge.⁵⁶

Making the provider liable for the actions that a third party executes on its behalf in execution of the principal/ third party contract, guarantees that the provider will set up and monitor the distribution of its products properly. Provider liability should also make the regulator comfortable in allowing legal agreements to govern most aspects of the distribution of mobile money products, particularly the recruitment of third parties. In this case, a notification regime can provide the same protection as an authorisation regime, and can allow third parties to open customer accounts or handle cash-in and cash-out transactions.

4.3 Third party authorisation, notification, and training

A common regulatory approach to agent recruitment is to require the provider to notify the central bank of all third parties. One option that some regulators have adopted is approving multiple third parties at a time, or "bulk approval" (as in Kenya), but this has produced significant delays and makes it difficult for mobile money providers to closely manage the growth of their agent networks. However, regulators can require the provider to apply certain standards to the third party due diligence process and retain the prerogative to inspect third parties. As the next table summarises, **a notification regime can provide the same protection as an authorisation regime, but at a lower cost for the regulator, the provider, and the customer.**

Table 5. Third party authorisation vs. notification

	Time	Flexibility	Cost
Authorisation	Requires time to submit applications and wait for the response from the regulator.	Providers cannot quickly deploy third parties to achieve scale, nor can they shut down third parties that are not performing.	Application process requires time and resources.
Notification	Only time commitment is required to locate and source third parties. Submission of third party details to regulator can be done in bulk.	Providers can quickly respond to market developments by adding and removing third parties to/from the network.	Reduced cost due to time saved in waiting for approval and minimal ongoing administrative requirements.

Well-trained third parties are very important to ensuring high quality customer experiences and protecting both the customer and the provider against various types of fraud or abuse. The regulator can also require the provider to provide training on certain issues, such as the KYC procedure and the detection of fraudulent use of mobile money services, as well as to review and preapprove some of the materials. **However, regulators typically do not have the resources to conduct training themselves, which creates a bottleneck** (see box below).

A (resolved) regulatory challenge with CICO agents in the Philippines

Until 2009, the network of locations where GCASH and Smart Money customers could convert cash into electronic value, and vice versa, was limited to (approximately) 5,000 agents, which provided an inadequately small distribution footprint within the country.

Regulation was cited as a primary reason for this limited growth. In fact, in accordance with BSP Circular 471 of 2005, non-bank agents must first attain a remittance agent license to perform cash-in/out services. To a certain extent, the rules governing how agents acquired this license posed a barrier to scaling the agent network. Prospective agents had to first submit an application form, incorporation papers, business license, and other key documents, and then attend a seminar on AML/CFT. This last requirement proved particularly burdensome for potential mobile money agents because the seminars were not widely available outside Manila and were typically held during business hours. Since 2008, the BSP has allowed providers to conduct their own training. The AML unit in the central bank ensures that the training material is up-to-date, high quality, and meets the required standards.

4.4 Third party operations: registration of new clients, activation, and cash-in/cash-out (CICO)

Third parties play an important role in the registration of new customers. However, regulators must strike a balance between complying with AML/CFT regimes on customer identification and identity verification, and allowing third parties to conduct the due diligence of customers required to open accounts and conduct transactions.

Some regulators allow third parties to conduct CDD for mobile money because they consider it a low-risk product and channel for money laundering and terrorist financing, and because deposit and transactional limits are imposed on mobile money products (such as in Pakistan, Mexico, and Peru).

During the registration process, the customer is typically asked to present an approved form of identification and fill in a registration form. In some countries, the third party is required to send the completed form and a photocopy of the ID document to the provider's offices for processing, although this requirement seriously limits the extension of services to rural areas that do not have electricity and photocopiers. If an error is made on the form, it must be sent back to the third party, and the third party must contact the customer to correct the error where possible. This can add a few days to a few weeks to the registration process, and can result in a loss of mobile money customers.

Any delay between signing up a new customer and activating the mobile money account has a negative impact on customer activation, and therefore financial inclusion.⁵⁷ A CGAP analysis indicated that customers who performed two or less transactions in their first month only had a 4% chance of being active users in their third month.⁵⁸

In fact, the procedure just described makes it impossible for a customer who has just signed up to receive help from the third party to conduct the first transactions and to become immediately familiar with the service. Alternative registration options include phone-based registration, which allows a third party to submit new user data more quickly, transfer new client data electronically, and verify and store this information centrally. In fact, most mobile money deployments send this information via Unstructured Supplementary Service Data (USSD) or SIM Toolkit (STK) to a central database and use paper forms simply as backups.

57 GSMA (2011), "Barriers to Customer Activation: A Case Study from MTN Uganda." Available at <http://www.gsma.com/mobilefordevelopment/barriers-to-customer-activation-a-case-study-from-mtn-uganda-3/>.

58 Claudia McKay, Toru Mino, and Paola de Baldomero Zazo (2012), "The Challenge of Inactive Customers," CGAP presentation. Available at <http://www.slideshare.net/CGAP/the-challenge-of-inactive-customers>.

It is very important to find solutions that allow customers to transact immediately after signing up (with defined storage and transaction thresholds), without the hurdle of pre-registration or simultaneous registration. Then, once they are more familiar with the product and want to conduct larger transactions, they can complete their registration and change the status of their accounts. Or, if they have already registered, higher thresholds could be automatically activated once their identity has been verified.

Most regulations permit third parties to process CICO transactions, enabling customers to conveniently store and access cash and convert it to electronic money.

One of the most important innovations in mobile money is the pre-payment model, which has clear roots in the airtime distribution model used throughout the developing world. When third parties facilitate cash-out transactions, they exchange cash, which is their own, for electronic value that they may later redeem for cash from the mobile money provider. Likewise, when they facilitate cash-in transactions, they exchange electronic value that they previously purchased from the mobile money provider for cash. In every case, third parties trade on their own account – they never act as custodians of cash or electronic money that belongs to users or to the mobile money provider. **This reduces the possibility that third parties will abscond with money – either cash or electronic value – that belongs to customers or to the mobile money provider.**⁵⁹

4.5 Third party exclusivity

Third party exclusivity is a matter of competition policy that should be addressed carefully with the competition authority.

While third party exclusivity can secure first-mover advantage in the early stages of market development by helping to protect the first mover's higher investments of time, energy, and money in identifying, training, and equipping third parties, ongoing exclusivity can limit the ability of other providers to establish effective distribution networks, and this could stifle competition.

To assess the significance of this issue in any particular market, certain strategic issues must be considered, such as competitors' existing market share, and the extent to which the business model relies on other distribution networks.

A regulatory challenge with cash-out third parties in Indonesia

Five years after Bank Indonesia granted the first mobile money license, the number of mobile money users and transactions in the country remains quite low. The number of mobile money agents and third parties offering cash-out services is a major constraint to growth.

According to a study released in 2009 by CGAP, IFC, and GTZ (now GIZ), the relatively small number of cash-out points can be attributed to Bank Indonesia regulations for the use of cash-out agents for mobile money issuers^{xli}. Current regulations allow mobile money issuers to use agents to upload value to mobile money accounts (cash-in). However, if a mobile money issuer wants to use agents to offer cash-out services, the third party must be licensed as a money remitter by Bank Indonesia. Therefore, non-bank mobile money providers cannot leverage their large distribution networks to provide cash-out points because each of their airtime dealers must apply for a remittance license individually. The reasonably extensive licensing requirements imposed by the regulation discourage a significant number of small airtime dealers from applying.

However, given the definition of "money remitter" and the fact that cash-out agents only convert electronic value to cash in real time, these cash-out activities should not be considered money remittance activities. Siti Hidayati, Senior Payment System Overseer at Bank Indonesia, argues that there is a strong case for critically evaluating the current regulations and to review it "recognizing that cash-out transactions are distinct from remittance activities, it is not necessary to require a remittance license for mobile money cash-out agents."^{xliii}

59 Internal control systems have been set up in which certain platforms allow agents to make fraudulent commission-generating transactions between personal and agent accounts that falsely drive up commission costs and defraud the MNO.

5. How can mobile money customers be given more protection?

Mobile money strikes a balance between creating innovative forms of financial access and offering an acceptable level of consumer protection. Tailored guidance from the regulator can help mobile money providers to improve transparency in their relationships with customers and prevent third party fraud.

The safety of mobile money relative to cash is often cited as one of the key benefits of mobile money for customers. Safeguarding customer funds held as electronically stored value and reducing opportunities for agent fraud and other harmful actions have both been analysed in previous sections. However, in addition to this, customers can be given even more protection through greater transparency, customer recourse processes, insurance protection, and privacy and data security measures. Mobile money must strike a balance between creating innovative forms of financial access and offering an acceptable level of consumer protection.⁶⁰

5.1 Transparency and customer recourse

The regulator can help to enhance consumer protection through market conduct regulation that promotes transparency. For instance, requiring agents to post applicable fees, requiring price disclosure for mobile transactions, prohibiting agents from charging extra fees without clearly disclosing them to customers, requiring contracts to be simple and include all relevant fees and charges, and requiring agents to disclose their status as an agent of a licensed institution. However, the regulator should consider the costs of implementing transparency requirements for clients that ultimately conduct low-value transactions, and guard against creating overly prescriptive or complex rules, or mandating standards and protocols for technology that are expensive or impractical in low-income areas.

In some cases, the regulator can assist the provider with templates for customer contracts and with fine-tuning the wording to ensure the customer understands their rights and obligations. This type of collaboration can expedite the launch of the service since the contract template does not need to be pre-approved.⁶¹

It is also important that customers understand and have access to effective recourse and complaint procedures for resolving errors or disputes. These should be presented in simple, plain-language, cost little or nothing to the consumer, be carried out by a trusted provider, and have convenient access points, including well-trained call centre staff.

60 A broad analysis of these issues, with perhaps more emphasis on overly comprehensive regulation of mobile money services, is in Denise Dias and Katharine McKee (2010), "Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options." CGAP Focus Note 64. Washington, D.C..

61 Simone di Castri (2011), "Empowering and Protecting Financial Consumers. Bank Negara Malaysia's Consumer and Market Conduct Framework," Alliance for Financial Inclusion (AFI) case study, Bangkok, Thailand. Available at <http://www.afi-global.org/sites/default/files/afi%20case%20study%20malaysia.pdf>.

5.2 Insurance protection

The benefits and technical feasibility of extending deposit insurance to mobile money have been clearly demonstrated in the United States, where, as long as e-float is placed in an insured depository institution, it is considered an insured deposit. For pooled custodial accounts, there is pass-through protection for each customer up to the insurance limit.

Deposit protection though insurance might be a viable solution, but before such a system is set up, it is essential to assess who will fund it, how the premiums will be determined and assessed, and what impact these premiums will have on the fees charged to customers for mobile money services.

5.3 Privacy and data security

Like other financial services, mobile money raises issues of privacy and data protection, some of which are addressed by national privacy laws, telecommunications regulation, and financial regulation, but most by everyday business practice. Data in a mobile money transaction may include payer and payee IDs, geographic location, time of day, purchased items, and the value of the transaction.⁶² Mobile money providers have internal controls to minimise unauthorised access to consumer information, as well as the loss of customer data.

Regulators and mobile money providers need to work together to understand security concerns and maintain the integrity of customer data.

MNOs have developed various systems to protect customer privacy. Typically MNOs back up their IT systems (at least) daily, and the USSD and the STK channels used to transact mobile money customer orders have so far proven to be sufficiently secure. USSD is also session-based, which leaves no traces of the transaction once the session is closed. SMS is encrypted over the SS7 links.

Customers are also responsible for protecting their password, PIN number, and other sensitive information. Consumer education can help to reduce breaches of privacy, and most mobile money providers take initiative to build customer awareness and capacity to prevent fraud by employees or third parties.

The regulator could design and enforce a wide array of privacy-related requirements and require local hosting and specific procedures for back-ups and physical site security. However, compliance costs should be properly assessed and solutions discussed with mobile money providers, which seem particularly committed to addressing security risks and challenges.

62 Matt Krueger (2011), "When payments become more," Mobile Money Exchange blog, <http://www.mobilemoneyexchange.wordpress.com/2011/06/01/smart-money-series-whenpayments-become-more>.

6. How should policy makers and providers engage on interoperability?

Service providers and policy makers should work together to understand different types of interoperability, including the benefits, costs, and risks. The role of the policy maker is to facilitate dialogue between providers, ensuring that interoperability brings value to the customer, makes commercial sense, is set up at the right time, and regulatory risks are identified and mitigated.

There is no question that both customers and mobile money providers could benefit from the interoperability of mobile money services. The question is when and how interoperability makes commercial sense for providers and creates value for customers.

The mobile money industry is still in an early stage. Only a few deployments have succeeded in attracting a significant user base; most are still focused on establishing strong foundations for building sustainable services.⁶³ Mature deployments are already starting to pursue connections with external parties, such as banks, MFIs, and external businesses. This is already being seen in the Philippines, where Globe has created bilateral agreements with several other systems, and in Kenya where Safaricom has agreements with Western Union and several banks.⁶⁴ As more deployments mature, so will the number of connections to the mobile money platform and the pursuit of interoperable solutions to keep the industry growing.

6.1 A collaborative approach to building interconnected mobile money environments

Building an effective interoperable environment is going to require service providers to engage with policy makers and regulators. The policy maker should act as a facilitator, helping providers to create the road map that they will be primarily responsible for designing and implementing. The policy maker can also assist providers with their evaluation to **ensure a) that interoperability is set up at the right time, b) that it creates value for both customers and providers, and c) that regulatory risks are identified and mitigated. Factors to be considered:**

- **Timing:**⁶⁵ The benefits of interoperability are more likely to emerge from mature mobile money deployments, such as ones with a functioning agent / third party network and an active customer base. Most regulators are cautious about intervening to encourage mobile money platforms in markets where deployments are still young.⁶⁶

63 Claire Pénicaud (2013), *cit.*

64 M-PESA is connected to 100 financial institutions, and including bill partners and everything the number of connections goes up to 500.

65 See Gunnar Camner (2012), "Expanding the Ecosystem of Mobile Money: Considerations for Interoperability," GSMA Mobile Money for the Unbanked position paper, London, UK. Available at http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Expanding-the-ecosystem-of-mobile-money.pdf.

66 For instance, the reticence of the Banque Centrale du Congo comes from its dialogue with e-money providers and assessments of developments in countries such as Pakistan and Ghana. The central bank has concluded that mandating interoperability at an early stage is likely to jeopardise market development across the DRC. Having set up an enabling regulatory framework, both policymaker and operators agree that the biggest priority for mobile money growth in the DRC is educating consumers about mobile money services and encouraging more service uptake. This position was reported by V.C. Ramazani Mwambo, Responsable de la Sous-Direction du Contrôle Permanent des Banques et Autres Institutions Financières, Banque Centrale du Congo, during the session "Breaking the barriers of mobile financial services."

- **Commercial and customer value:** Interoperability makes sense when more customers can be reached and when a greater frequency and variety of transactions can be performed. The majority of mobile money transactions are sent and received by customers within their own deployment, but allowing mobile money to flow between multiple deployments would likely increase the number and frequency of transactions across networks, as well as the addressable customer base for each deployment. It would also make it easier for third parties to leverage mobile money and grow the network of companies and organisations that offer mobile money services.

Service providers face several challenges, however, including technical solutions, commercial agreements, and operational procedures. The costs associated with these integrations must be outweighed by the commercial benefits of performing more transactions.

- **Regulatory risks:** Depending on the business model that is permitted and adopted, mobile money providers could leverage three existing assets to implement interoperable mobile money systems:⁶⁷
 - The mobile money platform (platform level): This allows mobile money to be transferred across mobile money deployments “wallet-to-wallet” and could include connections to switches, financial institutions, and companies.
 - The distribution network (distribution level): This allows transactions to be conducted across multiple distribution networks, or electronic retail payments acceptance schemes (see also Section 4.4).
 - The SIM card (customer level): This allows a customer of one MNO to use the mobile money services of any other MNO, bank, or third party.

At each of these levels, interoperability poses different costs and regulatory risks, and requires providers to enter contractual agreements that specify both joint and individual responsibilities, e.g., the responsibility to ensure minimum KYC requirements are met and monitored at the distribution level. Providers also need to come to an agreement on how to split revenues and costs, on customer fees (both the cost and the methodology), the disclosure policies, and the recourse system available to customers.

Given the sophistication of such efforts, the providers should be mindful of implementing one solution over another.

The policy maker and the regulator could help providers to assess the particular risks and costs of interoperability at the platform, distribution, and customer level. The policy maker could also help to ensure that interoperability is not removing healthy competition that drives financial inclusion (e.g. investments in distribution if third party sharing is implemented in an immature market).

67 See CGAP (2011), “Interoperability and Related Issues in Branchless Banking,” Power point presentation. Available at <http://www.slideshare.net/CGAP/interoperability-and-related-issues-in-branchless-banking-a-framework-december-2011>.

Interoperability and the role of the central banker⁶⁸ⁱⁱⁱ

“Innovations in retail payment markets can raise new questions regarding standardisation and interoperability, which most central banks promote and facilitate, e.g., by fostering the dialogue between different stakeholders or by actively contributing to the development of domestic or global standards.”

Working Group on Innovations in Retail Payments
Committee on Payment and Settlement Systems
Bank for International Settlements (BIS)

6.2 Mandating interoperability

Some financial regulators have been tempted to require providers to become interoperable. From the perspective of policy makers, the motivation to mandate interoperability seems to be to:

- lower the costs of financial services
- increase customer choice
- increase competition and break dominant positions.

It is difficult to predict for certain whether interoperability would actually lower costs and expand customer choice – the mobile money industry is still too new. CGAP and Bankable Frontier Associates (BFA) point to Ghana, where the central bank mandated that retail payments be interconnected at a relatively early stage, “as a cautionary tale of how mandated interconnection may be hard to enforce and even have limited effect.”⁶⁸ The risk of moving too early (or in the wrong way) poses two major risks to the industry as a whole:

- Compliance costs may increase, making the business case more challenging for providers.
- Implementing the technical side of interoperability can be complex and distract the operator from focusing on the basics of the service, such as building the distribution network and educating customers.

In terms of increasing competition, it is the regulator’s responsibility to ensure that any intervention aimed at breaking a monopoly or abusive dominant position does not harm the industry, create an unequal playing field for current market players, or negatively impact customers. Competition authorities usually weigh the costs and benefits of these interventions carefully. In fact, high market share does not necessarily mean that consumers are paying excessive prices, that competition and product innovation are being stifled, or that the company with high market share is abusing its power (such as through exclusionary practices). The timing and cost-effectiveness of any regulatory intervention must be appraised carefully, and **market-led solutions should always be the preferred option.**⁶⁹

68 CGAP and Bankable Frontier Associates (BFA) (2012), “Interoperability and the Pathways Towards Inclusive retail Payments in Pakistan,” Washington D.C.. Available at <http://www.cgap.org/sites/default/files/CGAP-BFA-Interoperability-and-the-Pathways-Towards-Inclusive-Retail-Payments-in-Pakistan-Jun-2012.pdf>

69 This is a position often presented by expert policy makers and regulators. Among others, Carlos López-Moctezuma, Chief Adviser to the President, Comisión Nacional Bancaria y de Valores Mexico, and chair of AFI Mobile Financial Services Working Group) and Muhammad Ashraf Khan (Director of the Agricultural and Credit Department at the State Bank of Pakistan) during the session, “Breaking the Barriers of Mobile Financial Services to Make Financial Inclusion Real” at the Alliance for Financial Inclusion (AFI) 2012 Global Policy Forum (GPF) (see <http://www.afi-global.org/news/2012/9/28/global-policy-forum-2012-breaking-barriers>); and Narda L. Sotomayor (Economist, Superintendencia de Banca, Seguros y AFP of Peru) during the GSMA Mobile Money for the Unbanked (MMU) 2012 Leadership Forum (see <http://www.gsma.com/mmu>).

Conclusions

Mobile payments and transfers are the building blocks of digital financial inclusion. Mobile money has great potential to give millions of people access to payment and transfer services, to store their money safely, and “to build low-cost ‘on-ramps’” for accessing a broader range of financial services.⁷⁰ Smart policies are decisive in enabling the development of mobile money, while short-sighted decisions of policy makers and regulators can prevent deployments from launching, becoming sustainable, and reaching scale. Those decisions also have direct impacts on the lives of millions of households in the developing world who currently rely exclusively on the cash economy or on less convenient, risky financial services. Persistent and widespread financial exclusion has also a negative effect on economic development and the stability and integrity of the financial sector.

In countries such as Ghana, Guatemala, India, Indonesia, Mexico, Nigeria, South Africa and others, central banks and other policy making institutions have emphasised their commitment to financial inclusion, but have pursued this goal with rather conservative policies. One of the hallmarks of a mature financial system is the wide availability of payment and other financial services, offered by both bank and non-bank providers that leverage their assets to meet overwhelming demand.

Given the progress that has been made in a number of markets towards creating more enabling policies for financial inclusion, the templates for regulatory reform do not need to be created from scratch. This paper has presented enabling regulatory solutions, backed by evidence and internationally recognised regulatory standards, that could be applied extensively across all markets; they simply need to be adapted to the local context, leveraging local opportunities and adjusting to the peculiarities of each jurisdiction.

An important lesson from the markets where mobile money is growing is that the precondition for developing a successful regulatory framework is to establish an open dialogue and consultative process between the regulator and the private sector. According to many regulators, establishing an open dialogue with mobile money providers is a critical step in designing enabling regulation that has a financial inclusion objective and provides effective oversight of the business. Regulators need to understand the distinctive characteristics of mobile money, including client behaviour and needs, the characteristics of products and services, the implementation challenges that providers face, and the potential solutions they can employ.⁷¹ We have seen this challenge arise most often in markets that only allow the bank-led model, even though the MNO is involved in most of the operations and is the main interface of customers.

A second key lesson is that the success of mobile money depends on creating an open and level playing field that lets non-bank mobile money providers, including MNOs, into the market. Together with effective and proportionate mechanisms in place to manage the risks, mobile money holds the promise of significantly expanding financial inclusion by lowering transaction costs, expanding access to financial services in areas out of reach of traditional financial providers, and improving convenience for customers. Beyond financial inclusion, mobile money also contributes to meeting the mutually reinforcing objectives of financial stability, integrity, and consumer protection, and to driving economic and social growth. The countries that embrace the reforms discussed in this paper will benefit most significantly from these opportunities that mobile money presents.

70 Dan Raddcliffe and Rodger Voorhies (2012), *cit.*

71 See, for example, these interviews with Sergio Da Sousa of Bank of Namibia (<http://www.gsma.com/mobilefordevelopment/mobile-money-as-an-agent-of-financial-inclusion-the-new-regulation-for-e-money-services-in-namibia-interview-with-sergio-de-sousa-bank-of-namibia>) and Nestor Espenilla and Pia Roman of Bangko Sentral ng Philipinas (<http://blip.tv/cgap>), as well as two case studies that tell the experiences of the Banque Centrale du Congo and the Banque Centrale des États de l’Afrique de l’Ouest (BCEAO), in Simone di Castrì (2012), “Building a trusted mobile money ecosystem: policy lessons from Francophone Africa,” in “The Financial Revolution in Africa: Mobile Payment Services in a New Global Age,” Foreign Policy Centre, London, UK. Available at <http://fpc.org.uk/fsblob/1518.pdf>.

Endnotes

- i The paper incorporates comments from Claire Alexandre (Vodafone), Neil Davidson (Coda Payments), Ahmed Dermish (Bankable Frontiers Associates), Lara Gidvani (Bankable Frontiers Associates), Jeremiah Grossman (Oxford Policy Management), Alex Kamara (Millicom – Tigo), Wameek Noor (CGAP / the World Bank), Sacha Polverini (The Bill & Melinda Gates Foundation), Dan Radcliffe (The Bill & Melinda Gates Foundation), Annie Smith (Digicel), Michael Tarazi (CGAP / the World Bank), and the Mobile Money for the Unbanked (MMU) team at the GSMA.
- ii Narda L. Sotomayor (2012), "Setting the Regulatory Landscape for the Provision of Electronic Money in Peru," in *Innovations*, Volume 6, Issue 4, MIT Press. Available at http://www.sbs.gob.pe/repositorioaps/0/0/fer/ddt_ano2012/DT-3-2012_Narda_Sotomayor.pdf.
- iii See Global Partnership for Financial Inclusion (GPFI) (2012), "Financial Inclusion: A Pathway to Financial Stability? Understanding the Linkages," paper for the GPFI 1st Annual Conference on "Standard Setting Bodies and Financial Inclusion: Promoting Financial Inclusion through Proportionate Standards and Guidance," Basel, Switzerland. Available at <http://www.gpfi.org>. Also see Global Partnership for Financial Inclusion (GPFI), 2011, "Global Standard Setting Bodies and Financial Inclusion for the Poor. Towards Proportionate Standards and Guidance." Available at <http://www.gpfi.org>.
- iv Government-to-person (G2P) payments include social transfers as well as wage and pension payments. Mobile-enabled G2P payments may be leveraged to increase financial inclusion.
- v Claire Pénicaut (2013), "State of the Industry: Results from the 2012 Global Mobile Money Adoption Survey," GSMA, London, UK. Available at <http://gsma.com/mmu>.
- vi Based on a longitudinal survey of 2,000 Kenyan households. See William Jack and Tavneet Suri (2011) "Risk Sharing and Transaction Costs: Evidence from Kenya's Mobile Money Revolution," Working Paper. Available at http://www.mit.edu/~tavneet/Jack_Suri.pdf.
- vii See Dan Radcliffe and Rodger Voorhies (2012), "A Digital Pathway to Financial Inclusion," Bill & Melinda Gates Foundation paper. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2186926.
- viii The process by which a customer credits an account with cash. This is usually via a third party that takes the cash and credits the customer's mobile money account.
- ix The process by which a customer withdraws cash from a mobile money account. This is usually via a third party that gives the customer cash in exchange for a transfer from the customer's mobile money account.
- x The theory of change that sees mobile money platforms as "low-cost 'on-ramps' that enable poor people to convert their physical cash into digital money and [...] to meet their financial needs in digital form" is described in Radcliffe and Voorhies (2012), *cit.*
- xi See GPFI (2012), *cit.* In the same paper, the GPFI also argues that an inclusive financial sector is likely to have greater political legitimacy and thereby decrease the risk of political and social instability, which in turn could lead to financial instability. An inclusive financial sector has the potential to enhance economic stability, which is an essential component of financial stability.
- xii Solvency risk refers to the inability of a company to honour its debt commitment. This means that an insolvent company owes more than it owns. Systemic risk refers to the failure of one financial institution that causes other interconnected institutions to fail, harms the entire market or entire market segment, and the economy as a whole.
- xiii Alfred Hannig and Stephan Jensen (2010), "Financial Inclusion and Financial Stability: Current Policy Issues," ADBI Working Paper 259. Tokyo: Asian Development Bank Institute. Available at <http://www.adbi.org/working-paper/2010/12/21/4272.financial.inclusion.stability.policy.issues/>
- xiv The international framework for the SIPS was released by the Bank for International Settlements (BIS) in 2011. See Bank for International Settlements (BIS), Committee on Payment and Settlement Systems (CPSS) (2011), "Core Principles for Systemically Important Payment Systems." Available at <http://www.bis.org/publ/cpss43.pdf>.
- xv Liquidity risk refers to the difficulty a company faces in meeting its operational needs and pay current debts as they come due.
- xvi Alfred Hannig and Stephan Jensen (2010), *cit.*, p. 23.
- xvii See Joshua Blumenstock, Marcel Faichamps and Nathan Eagle (2012), "Charity and Reciprocity in Mobile Phone-Based Giving in the Aftermath of Earthquakes and Natural Disasters." Available at <http://users.ox.ac.uk/~econ0087/earthquakes.pdf>.
- xviii Business Week, "Inflation not affected by mobile money transfers," 12 March 2012. Available at http://www.busiweek.com/index.php?option=com_content&view=article&id=2541.
- xix A full analysis of the risks of cash versus mobile transactions for money laundering (ML) and financing terrorism (FT) is detailed in Section 3.
- xx Bjørn S. Aamo (2012), "FATF's focus on financial inclusion: protecting the integrity of the global financial system," Presentation for 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. Available at <http://www.fatf-gaforpagesfatfsfocusonfinancialinclusionprotectingtheintegrityoftheglobalfinancialsystem.html>.
- xxi Central Bank of Kenya (CBK) and Financial Sector Deepening (FSD) Kenya (2009), "FinAccess National Survey 2009. Dynamics of Kenya's changing financial landscape," Nairobi, Kenya. Available at http://www.fsdkenya.org/finaccess/documents/09-06-10_FinAccess_FA09_Report.pdf.
- xxii Denise Dias and Katharine McKee (2010), "Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options," CGAP Focus Note 64, Washington, D.C.. Available at <http://www.cgap.org/sites/default/files/CGAP-Focus-Note-Protecting-Branchless-Banking-Consumers-Policy-Objectives-and-Regulatory-Options-Sep-2010.pdf>.
- xxiii See Daryl Collins, Jonathan Morduch, Stuart Rutherford, and Orlanda Ruthven (2009), "Portfolios of the Poor: How the World's Poor Live on \$2 a Day," New Jersey: Princeton University Press. This book provides evidence of struggles by the world's poor to manage their financial lives without suitable financial services, and builds a powerful case for expanding innovative and appropriate financial services to the poor.
- xxiv See section 5, for specific consideration regarding market conduct regulation and mobile money.
A full analysis of the risks of cash versus mobile transactions for money laundering (ML) and financing terrorism (FT) is detailed in Section 3.

- xxv The sources for the social cost of cash are: European Commission Staff Working Document, Annex to the proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market, Impact Assessment (2005), COM (2005) 603 final; McKinsey & Company (2007), "Reducing the Cost of Cash"; BNM's estimate is a figure cited by Professor Leo van Hove (2008), "Why Should Cash be Made More Expensive"; information about Nigeria is reported here: <http://www.thebftonline.com/feature/1806-mtn-mobile-money-helping-build-a-cashless-economy>.
- xxvi For an analysis of the cost of cash for individuals and how they could be addressed building a digital pathway to financial inclusion, see Radcliffe and Voohties (2012), *cit*.
- xxvii For more information regarding M-PESA being considered "M1", see Claire Alexandre, "10 things you thought you knew about M-PESA," 22 November 2010, <http://www.cgap.org/blog/10-things-you-thought-you-knew-about-m-pesa>.
- xxviii Bank for International Settlements (BIS), Committee on Payment and Settlement Systems (CPSS) (2012), "Innovations in Retail Payments," Report of the Working Group on Innovations in Retail Payments. Available at <http://www.bis.org/publ/cps102.pdf>.
- xxix Sri Lanka has a population of over 20 million, and Dialog has 7.5 million airtime customers.
- xxx Mobile Payments Guidelines No. 1 of 2011 for the Bank-led Mobile Payment Services, and Mobile Payments Guidelines No. 2 of 2011 for Custodian Account Based Mobile Payment Services.
- xxxi Sources: International Finance Corporation (2011), Mobile Money Study 2011 – Sri Lanka. Available at <http://www1.ifc.org/wps/wcm/connect/6a8d06004a052e158b1affd29332b51/MobileMoneyReport-SriLanka.pdf?MOD=AJPERES>. Consultative Group to Assist the Poor (CGAP) (2009), "Financial Access: South Asia: A Regional Snapshot." Available at <http://www.cgap.org/gm/document-1.9.40542/2009%20Funder%20Survey%20Regional%20SA.pdf>.
- xxxii Jeanette Thomas, "Regulation Spurs Innovation in The Philippines," CGAP blog, November 5, 2012, <http://www.cgap.org/blog/regulation-spurs-innovation-philippines>.
- xxxiii GSMA MMU Mobile Money Regulatory Guide, available at <http://www.gsma.com/mobilefordevelopment/mobile-money-regulatory-guide>.
- xxxiv GSMA MMU Mobile Money Regulatory Guide, available at <http://www.gsma.com/mobilefordevelopment/mobile-money-regulatory-guide>.
- xxxv Tillman Ehrbeck and Michael Tarazi (2011), "Putting the Banking in Branchless Banking: Regulation and the Case for Interest-Bearing and Insured E-money Savings Accounts," in World Economic Forum's Mobile Financial Services Development Report, 2011. Available at http://www3.weforum.org/docs/WEF_MFSD_Report_2011.pdf.
- xxxvi Marina Solin and Andrew Zerzan (2010), "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks," GSMA Discussion Paper. Available at <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/amfinal35.pdf>. The authors quote three studies: 1) Pierre Chatain, Raul Hernandez-Coss, Kamil Borowik, and Andrew Zerzan (2008), "Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing," World Bank Working Paper 146. Available at http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf; 2) Louis De Koker (2009), "The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa: Findings and Guidelines," Journal of Money Laundering Control, Vol. 12 No. 4. 323-339; and 3) Andrew Zerzan (2009), "New Technologies, New Risks? Innovation and Countering the Financing of Terrorism," World Bank Working Paper 174.
- xxxvii GSMA MMU Mobile Money Regulatory Guide, available at <http://www.gsma.com/mobilefordevelopment/mobile-money-regulatory-guide>.
- xxxviii United Nations Conference on Trade and Development (UNCTAD) (2012), "Mobile Money for Business Development in the East African Community. A Comparative Study of Existing Platforms and Regulations," Geneva, Switzerland.
- xxxix Matu Mugo (2011), "Regulation of Banking and Payment Agents in Kenya," in "The Fletcher School: Leadership Program for Financial Inclusion, Policy Memoranda 2011," Boston, MA, United States. Available at <http://fletcher.tufts.edu/CEME/publications/~media/Fletcher/Microsites/CEME/pubs/papers/MEMOS%20Final.pdf>.
- xl Developed in collaboration with Bankable Frontiers Associates (BFA).
- xli Mark Flaming, Klaus Prochaska, and Stefan Staschen (2009), "Diagnostic Report on the Legal and Regulatory Environment for Branchless Banking in Indonesia." Available at <http://www1.ifc.org/wps/wcm/connect/2f6874004a1b31b68f65ffdd29332b51/Tool%2B2.5e.%2BDiagnostic%2BReport%2BExample%2B-%2BIndonesia.pdf?MOD=AJPERES>
- xlii Siti Hidayati (2011), "Cash-In and Cash-Out Agents for Mobile Money in Indonesia," The Fletcher School, Leadership Program for Financial Inclusion, Policy Memoranda 2011.
- xliii BIS (2012), *cit*.



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

