

Policy note

Mobile financial services

Regulatory approaches to enable access



About this note

AFI's series of policy notes are made specifically for policymakers and focus on the key policy solutions that have been proven to promote financial inclusion in developing countries. Drawing on existing research, they define the policy solution, identify the critical issues for decision-makers and give practical examples from developing countries. The notes also identify policy champions who are at the forefront of implementation, and give an overview of relevant reading material.

At a glance

Mobile financial services

Mobile financial services include a diverse range of financial services that are delivered using a mobile phone. Two commonly distinguished categories are **mobile banking services**, through which a bank's clients connect to their accounts at the bank via their mobile device, and **mobile payment services**, which cover a broader range of payment services that may not be offered by a bank but always involve one.

Mobile phones are now widely available and widely used. Financial services that take advantage of this new channel can contribute greatly to financial inclusion. However, in order to serve the needs of the population while simultaneously protecting users, financial regulators must understand and assess the risks of mobile financial services arising from:

- **The channel:** when properly managed and regulated, operational risks are typically not greater than Internet banking via a PC and may be even lower if limits are established on the size and type of transactions that can be carried out with proportionate IT security controls.
- **The instrument:** while mobile financial services may provide access to existing sources of funds that are already regulated, such as bank accounts, mobile financial services may also involve creating and issuing new payment instruments such as electronic money (e-money). Regulators then face the dilemma of deciding which entities will be allowed to fulfill this role. A range of solutions has been taken in different countries, from the most conservative (limiting issuance to banks) to the most open (allowing mobile network operators and other non-bank participants to issue e-money). In terms of risk, selecting appropriate entities may be less important than whether regulators have the necessary powers to oversee the issuer.

Policy questions

Enabling M-financial services: How can regulators enable models of mobile financial services that expand financial inclusion and make the financial sector more efficient?

Mobile payment instruments: How should the issuance of new mobile payment instruments like e-money be regulated?

Channel: How should the use of the mobile phone as a channel be regulated?

Consumer protection: Do mobile financial services create new consumer protection and financial literacy challenges?

AML/CFT: What are the AML/CFT concerns in relation to mobile financial services?

Supervision: How should mobile financial services be supervised?

Interoperability: What are the implications of mandating interoperability and interconnection of mobile financial services?

Policy snapshots

A number of countries have developed innovative policy solutions to enable mobile financial services:



Mobile phones in financial inclusion

Before the arrival of mobile communications, financial institutions depended on fixed lines or satellites to connect branches, ATMs, point of sale machines, and other devices for providing services and products. Nowadays, mobile data channels provide reliable and cheaper forms of data connectivity. However, the potential of mobile communications to promote financial inclusion goes well beyond using the new communication channels to link existing devices.

The widespread use of mobile communications has created new channels, new instruments, and new business models for providing financial services to people who have traditionally been excluded from the formal financial system. In 2009, it was estimated that more than one billion people in developing countries had mobile phones but did not yet have access to formal financial services.¹ To date, about 100 million people worldwide use mobile services, most of them in Asia and Africa, and this group is growing fast.² The potential to reach even more people with mobile financial services is considerable. While the scale of mobile financial service deployments remains modest in most places outside of a few pioneering markets, there are signs of accelerating uptake in several countries. The number of people currently using mobile financial services represents only 2% of those with mobile subscriptions, and this number increased by 54% in just one year. A large number of new deployments are also being reported and tracked by the mobile industry body, GSM Association (GSMA).³

The potential of mobile phones to promote financial inclusion is widely recognized, but some questions and uncertainties remain regarding the regulatory and policy environment required to develop its potential and the implications if it succeeds. Mobile phones have enabled mobile operators to participate in the provision of certain financial services in various markets, simultaneously increasing competition and raising issues of regulatory scope. Proliferating business models and technology choices contribute to the complexity of the issues. The mobile phone itself plays two distinct roles, often simultaneously. It can be:

- **A channel** for the provision of electronic financial services, alongside other channels such as ATMs or point of sale devices, whether in the hands of the end consumer and/or new networks of agents who provide services to the final consumer on behalf of the service provider; and/or

- **A payment instrument** that enables payment instructions to be transmitted between payer and payee from and to different types of account. While the account may be a bank account which is already regulated, some services involve creating and issuing new payment instruments such as electronic money (e-money). Regulators then face the dilemma of deciding which entities will be allowed to do this.

As a channel, mobile phones decrease the costs of providing financial services to already-banked people. As a payment instrument, mobile devices enable new payment products and new business models that may involve a different role for banking institutions. This distinction has implications for the risks, and therefore the regulatory treatment, of mobile financial services.

- **Operational risks** arise from the use of mobile phones as a new channel for the delivery of financial services. These are related to the risks of electronic banking in general, but certain elements are specific to the use of the mobile device and mobile bearer channels.
- **Prudential risks** may arise with the creation of new payment instruments (such as e-money issued by non-banks) if certain conditions are not met.

Over the past decade, financial sector providers and regulators have come to identify the risks involved in offering such services and to better understand how to mitigate these risks. Regulators are increasingly recognizing the role that mobile financial services can play in transforming access to financial services and they are seeking to unlock this potential by creating enabling environments for them to grow. Understanding the risks involved allows regulators to balance these with opportunities for greater access.

This Policy Note provides a basis for understanding evolving types of mobile financial services and sets out an emerging understanding of how various policy questions are being addressed.

¹ CGAP-GSMA Mobile Money Market Sizing Study: <http://www.cgap.org/p/site/c/template.rc/1.26.10806/>.

² See Press Release of Gartner Research report, "Gartner Says Number of Worldwide Mobile Payment Users to Reach 108.6 Million in 2010," <http://www.gartner.com/it/page.jsp?id=1388914>.

³ For example, as of June 2010, GSMA Deployment Tracker reports 65 live and 85 pending mobile money deployments: see <http://www.wirelessintelligence.com/mobile-money/>.

Box A: Do mobile phones expand financial inclusion?

Mobile financial services are transformational when they allow unbanked people to enter the formal financial system. The large number of unbanked people with cell phones is often pointed to as proof of the transformational potential of mobile financial services. However, not all mobile financial service models are transformational – either in intent or outcome – and it is important to identify and analyze those business models and experiences that have been transformational and successful in expanding mobile financial services to the unbanked.

Kenya remains a leading example of the large-scale impact of financial inclusion. As many as one in two adults used mobile payment services in 2010, just three years after these services were first introduced. The proportion of users who were unbanked rose from 30% after the first year of deployment to 50% in 2009, as the service penetrated more widely and to lower income groups.⁴ M-Pesa, the main provider of mobile payment services in Kenya, has also reduced the cost and risk of domestic remittances compared to existing formal and informal options. A range of additional financial services, such as savings and credit, are currently being launched and offered on the back of the increasingly pervasive electronic retail payment systems (see Box B).

The Philippines offers another example of the potential of mobile phones as a transformational tool for financial inclusion. Mobile operators in the Philippines were early pioneers in launching mobile money services (since 2004). Although levels of active usage are below what was initially hoped, a CGAP study found that of all active mobile money users in the Philippines, one-half were unbanked and about one-quarter were considered poor by local standards.⁵ A shortage of cash-in and cash-out agents and strict KYC (Know Your Customer) procedures have perhaps prevented mobile usage from expanding further.

South Africa has also had several mobile money services active since 2005, but a 2008 study concluded that these services had not yet significantly expanded access to financial services.⁶ With few exceptions, mobile financial services linked to bank accounts have served the already largely banked population. However, overall adoption of the mobile channel has grown quickly, especially among the marginally banked or underbanked. At the end of 2009, the number of mobile financial services users in South Africa had grown to almost one-third of all banked customers in the country (twice as many as those using Internet banking).⁷

While the transformational potential of mobile financial services is significant, it will likely take time for transformational models to emerge from the shadow of less risky (and necessary) additive approaches.⁸ Regulators and providers will need to have realistic expectations about timeframes for rolling out new services.

⁴ For more information, see FinAccess National Survey 2009 (Kenya): http://www.fsdkenya.org/finaccess/documents/09-06-10_FinAccess_FA09_Report.pdf.

⁵ Mark Pickens, 2009, "Window on the Unbanked: Mobile Money in the Philippines," CGAP Brief, http://www.cgap.org/gm/document-1.9.41163/BR_Mobile_Money_Philippines.pdf.

⁶ David Porteous, 2008.

⁷ Leigh-Ann Francis, 30 April 2010, "Mobile banking set for growth explosion," <http://www2.itweb.co.za/sections/telecoms/2010/1004300141.asp?A=FIN&S=Financial&T=News&O=C>.

⁸ Additive approaches refer to financial services provided through the use of mobile phones that focus on serving the already banked population.

How it works: a definitional framework

In part because of the novelty of the field, there is no official or internationally accepted definition of **mobile financial services**.⁹ However, **mobile financial services** is commonly used as an umbrella term to describe any financial service that is provided using a mobile device. **Mobile money** is sometimes used as a substitute, although some use this term more narrowly to refer to the underlying source of value for mobile payments.¹⁰ This broad definition can be further delineated:

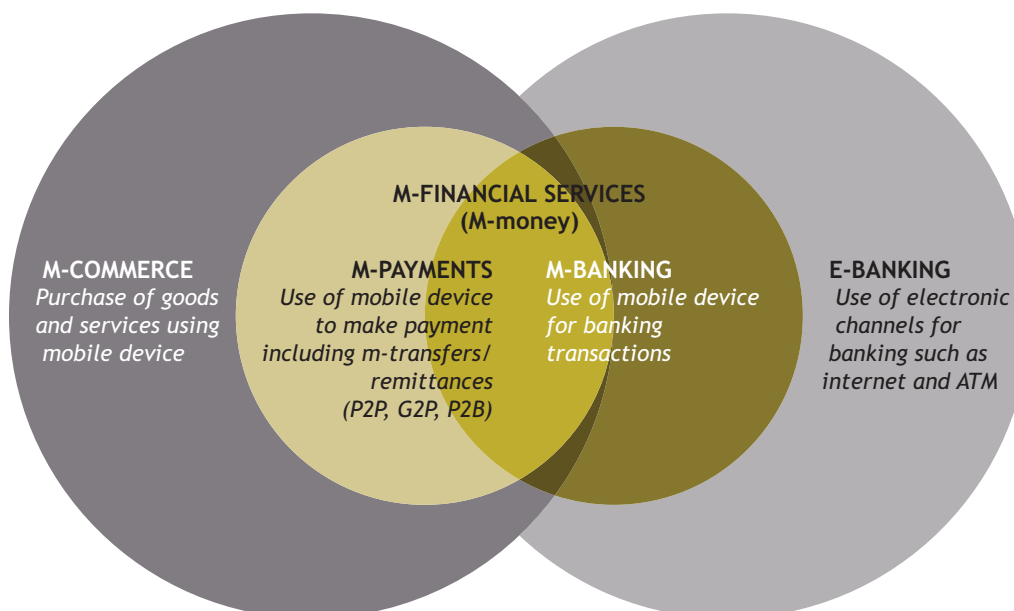
- **Mobile banking** (m-banking) is the use of a mobile device primarily as a channel to conduct transactions from one or more bank accounts. These transactions may include payments from one bank account to other bank accounts. Mobile banking services typically offer a range of informational functions as well, such as balance enquiries, simplified statements, transaction notifications, or account alerts. Mobile banking is a subset of electronic banking (e-banking), which includes Internet banking and the use of non-mobile channels such as ATMs and Point of Sale devices.
- **Mobile payment** (m-payment) is the use of a mobile device to make a payment.¹¹ M-payment may involve creating a new instrument, such as e-money, to serve

as the source from which and to which value is transferred. However, m-payment may be made using an existing instrument or store of value such as a bank account (see the overlap between the spheres in Figure 1) although the term is sometimes used to describe only those payments that are not from a bank account. There are a variety of types of mobile payments, including:

- **Person-to-person (P2P):** also known as a mobile money transfer or mobile remittances.
- **Person-to-business (P2B):** the payment of bills, goods, and services, and purchase of airtime. The reverse, Business-to-person (B2P) occurs when businesses pay people (for example, in wages or for goods delivered) and is broadly referred to as m-commerce.
- **Government-to-person (G2P):** an official body makes a payment, such as a salary or social transfer to an individual.

Mobile phones are now used to send and/or receive payments in each of these three ways in various parts of the world.

Figure 1: A definitional framework for mobile financial services



⁹ For example, the Committee on Payment and Settlement Systems at BIS has no definition of m-payment or m-banking in its glossary of payment and settlement terms. See <http://www.bis.org/publ/cps00b.pdf?noframes=1>.

¹⁰ See Jenkins, 2008, for a report on the first Mobile Money Summit, where the term 'mobile money' was popularized. http://www.hks.harvard.edu/m-rcbg/CSRI/publications/report_30_MOBILEMONEY.pdf.

¹¹ The European Central Bank is one of relatively few banks with a specific definition in its glossary: "A payment where a mobile device (e.g. a phone or personal digital assistant (PDA)) is used at least for the initiation of the payment order and potentially also for the transfer of funds." See: <http://www.ecb.int/home/glossary/html/glossm.en.html#611>.

How it works: products and models

Using the framework in figure 1, this section discusses the regulatory implications of emerging service and business models for mobile financial services. As different models proliferate, it is no longer useful to distinguish only between bank-based and non-bank based approaches; with any mobile financial service there is always at least one bank and at least one mobile network operator (MNO) involved.¹²

In order to assess the different types of emerging models, a functional perspective is helpful. This requires understanding the roles of different parties across the core functions of mobile financial services:

- **Operating retail transaction points:** for enrolling new clients and/or handling cash-in and cash-out and/or client queries or disputes
- **Electronic messaging:** the transmission of the payment instruction from sender to recipient and transaction notifications to sender

- **Account issuance:** the entity legally liable to the account holder for the balance stored
- **Account management:** the accounting function for the accounts (or wallets) involved
- **Investment of funds:** the intermediation of stored balances

In Figure 2 below, four main models are identified based on the roles of different parties across the functional value chain. Note that column 2 (electronic messaging) always involves at least one mobile operator and column 5 (investment of funds) involves a bank or banks (which hold wholesale or float accounts that they can intermediate as their terms of licensing allow).

Figure 2: Functions and roles

Model	Function				
	Retail transaction points	Electronic messaging	Account issuance	Account management	Investment of funds
M-banking (many banks)	Bank**	MOBILE OPERATOR	Bank	Bank*	BANK
Mobile channel enabler (Claro)	Mobile operator		Bank	Bank*	
Outsourced branded service (MTN Mobile Money)	Mobile operator		Bank(s)	Mobile operator	
Full mobile money service (M-Pesa Kenya)	Mobile operator		Mobile operator	Mobile operator	

Note: in all columns except column 2, the use of the term 'mobile operator' could also refer to a third party provider

* could be outsourced

** in addition to a bank's own branches, ATMs, or even agents, other transactional infrastructure such as third-party ATMs could be used

For each function, the regulator will want to know which party is responsible and which is liable in the event of mistake or failure, especially since the models above often involve a number of different outsourcing and agency agreements with different parties. This specialization of roles carries advantages and cost reduction that are important for affordability, but it also increases complexity and the risk that failure of one party

could lead to the failure of others. Apart from the legal questions of who is liable for the transactions, the regulator must also consider the way the public understands the distribution of responsibilities, in particular, whom they should address in the case of complaints. Hence, the branding of a service affects the extent to which customers may expect recourse from the owner of the brand.

¹² The original distinction between 'bank based' and 'non-bank based' models introduced by Lyman et al (2008) refers primarily to the source of electronic value—whether a bank account or not— as well as the custodian of the deposited funds, but does no longer fully capture the increasingly diverse range of roles and business models through which mobile financial services are provided.

How it works: products and models continued

The language used to describe the relationships between different parties may in fact blur understanding of their roles. For example, whether an account is called an 'm-wallet' or a deposit account does not change the nature of the issuer's role, which is to store value electronically, but the regulatory differences between the two types of accounts may be significant. The risk of confusion is greatest with models in which 'agents' are involved since they may play a range of different functions, some of which may have nothing to do with agency. For example:

- To enroll new clients, mobile financial services may use agents to collect application forms (an outsourced function that does not involve binding the principal) or, where the law allows it, delegate the power to agents to fulfill customer due diligence (CDD) requirements and open accounts on behalf of the operator. The latter is indeed an agency function for which the principal must be held responsible.
- In the provision of cash-in and cash-out services, the agent is often simply transferring electronic money to another party in exchange for cash, using the payment system to make the transfer in real time (which substantially reduces the risks of loss for both parties). However, the transfer is not made on behalf of the provider and is no different in substance from two individual users transferring money to one another in exchange for cash.

Clarity on regulatory issues around the use of agents is important but beyond the scope of mobile financial services alone, and will be addressed in a forthcoming AFI Policy Note. Regulators do, however, need to understand the actual role played by agents in the provision of mobile financial services in order to clearly foresee who is to be held accountable for the transactions conducted and any regulatory or contractual breaches.

A variety of partnerships between individual banks and telcos have been instigated over the years. In 2004, MTN and Standard Bank of South Africa formed a joint venture to pursue mobile financial services, although Standard Bank recently bought back MTN's share. The M-Kesho service offered by Equity Bank and Safaricom in Kenya represents a product-specific partnership between bank and telco through which customers can open co-branded savings accounts at the bank. Through this account they can transfer funds from their M-Pesa e-money account on

a preferential cost basis (see Box B). This service substantially increases the potential outreach of the banking system to unbanked people and the scope of m-banking. Meanwhile, in the Philippines, after several years of experimentation by the Rural Bankers Association to promote partnership arrangements between its member banks and the two major telcos, small rural banks are now able to offer services linking client bank accounts to mobile wallets offered by the telcos, from which various forms of electronic payments can be made.

One way to avoid the difficulties that can arise in joint ventures between separate entities, such as conflict over who 'owns' the client, especially among large banks and telcos, is to align interests through common ownership. For example:

- To cement its customer base and roll out its M-Paisa service, large Pakistani MNO Telenor bought 51% of the microfinance bank Tameer (2008)
- Filipino MNO Globe Telecom invested alongside large commercial bank BPI and their controlling shareholder in a new low-end bank, BankO, in 2009. Among other services, BankO converts the mobile wallets of G-Cash customers into savings accounts and allows their clients to use the G-Cash agent network.

Chris Bold (2010) speculates that these new types of ownership arrangements may signal a trend in the way MNOs enter the market for mobile financial services and that models like M-Pesa might become the exception rather than the rule.

While there is always at least one mobile operator involved, financial regulators in jurisdictions such as India, Mexico, and Nigeria require interoperability among the services they provide. That is, a mobile financial service must work for any operator's clients, regardless of the operator that is directly involved in the supply of the service. The guidelines issued by the Bank of Ghana, for example, indicate an explicit preference for so-called 'many-to-many' models in which the clients of multiple banks and multiple telcos can interconnect. Often, a third party provider is required to achieve this degree of interconnection and manage multiple interfaces and different technologies across networks. The issue of whether and how to promote interconnection will be considered in the next section.

Box B: Bank-telco partnership to offer additional services: M-Kesho in Kenya

M-Kesho is the brand name for a package of financial products issued by Equity Bank to clients who use the M-Pesa mobile payment system in Kenya. The package is co-branded and was launched by Equity Bank and MNO Safaricom under a one-year exclusive arrangement in May 2010. The core product is a bank savings account on which interest is earned, although credit and insurance options are also available.

Customers can open accounts either at Equity branches or at M-Pesa agents where Equity Bank has placed a bank representative.

The M-Kesho account offers only electronic transactions: money can flow into and out of the account either from the customer's M-Pesa account or (optionally) from a regular Equity Bank account. To deposit cash, customers must first load their M-Pesa account at an agent and then initiate a transfer to the M-Kesho account (this is free to the customer but the Bank pays M-Pesa a fee for each incoming transfer). To withdraw cash, the process is reversed, although customers pay for the transfer from their account (as well as the standard M-Pesa withdrawal fee).

M-Kesho is part of a next generation of mobile-enabled financial services that adds savings, credit, and insurance to the mobile transactional products already offered by M-Pesa, and creates a new type of partnership between a bank and a telco.

For more information: <http://www.safaricom.co.ke/index.php?id=263> or <http://technology.cgap.org/2010/05/18/m-pesa-meets-microsavings-with-equity-bank-deal-in-kenya/>



Third party providers that are not MNOs or banks have played an important role in innovating in mobile financial services. Celpay in Zambia, which became independent from MNO Celtel in 2005, launched one of the world's first mobile payment services in 2001. Similarly, Wizzit, launched in 2005 in South Africa, is designed, marketed, and operated by an entity independent from banks and MNO's, although the underlying accounts are formally held by a partner bank.

The business model for third parties is often more challenging than for established players with other revenue streams. In fact, the biggest risk for new entrants of this type may be having sufficient capital to sustain them through the development phase until their business becomes cash positive. Because the fees per transaction

are small and there are high fixed startup costs, the business of providing payments and issuing e-money is usually only sustainable with a large volume of transactions. To date, few specialized third party mobile financial service providers have reached this scale. The most robust business models to date are either banks that extend a new lower cost channel for clients to conduct transactions or telcos that seek to retain their pre-paid clients (or reduce so-called churn) and increase the average revenue per user (ARPU) by adding mobile payments as a service offering. However, as Mas and Kumar (2008) point out, it is not easy to optimize the mobile channel as a business proposition, even for banks, and few have done it yet.

Box C: 'Many-to-many' branchless banking in Ghana

The Bank of Ghana (BOG) published branchless banking guidelines in 2008. In these guidelines, the BOG stated that branchless banking of any kind, including mobile banking, could only be undertaken by licensed deposit-taking institutions and their agents.

The guidelines further specify that mobile banking must use the 'many-to-many' model. This means that clients of one bank should be able to use certain services of other banks and should not be limited to just one MNO network. The BOG guidelines rule out exclusive partnerships between banks and telcos and declared the end goal as being 'any-to-any' where full interconnection existed for clients of all banks and all telcos.

MTN Mobile Money is one example of a mobile financial service approved by BOG under these guidelines. This service was developed in 2009 by MTN, Ghana's largest MNO. Customers sign up for accounts at one of seven partner banks that have contracted with MTN to offer the service. A bank agent network managed by MTN provides cash-in and cash-out locations. The initial marketing focus was on remote person-to-person transfers. Two other non-bank mobile financial service providers were also approved to offer similar services in the same year.



Policy questions

1. How can regulators enable models of mobile financial services that expand inclusion and make the financial sector more efficient?

Enabling new models of financial services like mobile payments requires that regulators balance openness to experimentation and innovation with sufficient certainty about the legal framework that protects users and clearly assigns liabilities. Without openness, a new mobile service can become bogged down by restrictions that are applied to more traditional channels and business models. Without certainty and clear regulatory frameworks, reputable providers are likely to be unwilling to commit the resources to launch and sustain deployments (Porteous 2006). At the same time, clients might find offers from new entrants unreliable and therefore unattractive. Enablement must also provide adequate safeguards for consumers' interests, without which large-scale adoption is unlikely anyway (Lyman et al, 2008).

Ideally, an enabling environment has high levels of openness and certainty. In practice, however, countries that have pioneered mobile financial services, such as Kenya and the Philippines, have often had more openness than certainty (Porteous 2009), at least during the early stages of implementation. Both countries chose to allow reputable early implementers to proceed under close

monitoring and with frequent engagement rather than developing a general regulatory framework upfront. In recent years, both countries have adopted measures that have improved the degree of certainty.

Enablement does not necessarily require a one-off approach, but rather a sequential progression. As the scale and reach of the market grows, so does the need for certainty and customer protection. In the early stages of a market, it is possible to allow more scope for experimentation. The Principles for Innovative Financial Inclusion issued in June 2010 by the G20 Financial Inclusion Experts group recognizes this by advocating a 'test and learn' approach by regulators rather than regulating in advance of market conditions.¹³ This process of enablement requires that policy makers maintain an active dialogue with providers to understand obstacles and to monitor levels of market development. The 'test and learn' approach is particularly relevant to the development of mobile financial services given its innovative and evolving nature. Instead of attempting to foresee all possible business models and issue corresponding regulatory measures, regulators should set requirements in a flexible and open manner that can encompass different models in a single range of rules and elaborate as needed further on, rather than inhibiting the development of new products from the outset.

Box D: Central Bank of Kenya audits M-Pesa

In December 2008, the Minister of Finance in Kenya requested a special audit on the operations of M-Pesa. After engaging with Safaricom in 2006 to study the nature and risks of the new service, the Central Bank had issued a letter of no objection and Safaricom launched the service in March 2007. The rapid takeoff of the service, which reached 4.5 million registered users by November 2008, raised concerns at the Bank about risks mounting with scale, about consumer protection, and about competition among domestic money transfer operators.

The CBK conducted an investigation that showed, among other things, that while the volumes of payments via M-Pesa were indeed large and growing, the values remained small, and the average balances on each account were very low, suggesting that most usage was for money transfer. CBK also reviewed a second security audit undertaken by an expert firm to satisfy its concerns about the robustness of the system. CBK provided its findings to the Ministry of Finance, which published its satisfaction with the outcome and with the status of M-Pesa at that stage, while accepting the need to provide greater regulatory certainty to the rapidly growing mobile financial services sector in Kenya that other firms—telcos and third parties—were now interested in entering.

To read the full case study on the M-Pesa audit, see AFI's website:

<http://www.afi-global.org/en/knowledge-center/afi-publications-and-documents/category/42-casestudiesa>



¹³ <http://fas.imf.org/misc/G20%20Toronto%20Principles%20for%20Innovative%20Financial%20Inclusion.pdf>

2. How should the issuance of new mobile payment instruments like e-money be regulated?

The growth of mobile financial services has raised foundational policy questions for regulators of how to distinguish a ‘payment’ (mobile or not) from a ‘deposit’, and what differentiates the business of providing payments from that of deposit taking. These boundary questions are not new, but the spread of the mobile phone is necessitating greater clarity because it has enabled the creation and distribution of electronic payment instruments on a widespread scale, which was neither easy nor even possible in many places until recently.

While most countries have a Banks Act or equivalent piece of legislation that both defines the concept of a deposit and generally restricts the business of deposit-taking to regulated deposit-taking entities, the same legal certainty does not pertain to payments. This is in part because ‘payment’ is a much broader concept, covering a multitude of daily transactions, making it hard to regulate and/or supervise. Many countries still lack specific legislation that provides a legal basis for regulatory oversight of the business of operating payment systems and providing payment services.¹⁴ Notwithstanding uncertainties in legal practice in many countries, the conceptual boundary between payment and deposit is clear: the former involves a transfer of funds from payer to payee, while the latter involves at least the storage of funds repayable to the depositor in future.

The technology to store electronic value on a device such as a smart card has been available for several decades at least. However, until now it has been used little outside of closed loop environments like mass transit systems. The spread of mobile phones has accelerated the use of electronic money (e-money) as a source of funds for payments, but many developing countries still lack an official definition of e-money. Those that have developed one usually build upon a fairly basic definition, such as that of the Basel Committee on Payment and Settlement Systems (CPSS): “value stored electronically on a device such as a chip card or hard drive in a personal computer” and added the requirements that e-money be issued in exchange for currency and be accepted by parties other than the issuer as a means of payment. However, there are several variations on this basic definition. E-money is recognized as a class of electronic payment instruments distinct from other conventionally recognized forms such as credit transfers, debit transfers, and card payments. In most places, regulated deposit-taking institutions are allowed to issue e-money and e-money is differentiated from bank deposits through certain restrictions, such as not allowing interest to be paid on balances and not having deposit protection insurance. A key policy question is whether non-banks can issue e-money and, if so, on what basis. At present, countries tend to fall into one of the four categories in Figure 3 below.

Figure 3: Categorizing e-money regimes

		Have a clear regulatory framework for e-money?	
		Yes	No
Allow non-banks to issue e-money?	Yes	European Union (1999, 2009) Philippines (2009) Indonesia (2009)	Kenya
	No	South Africa (2006, 2009) Mexico (2010) ¹⁵	Ethiopia Bolivia

There is a clear trend towards creating legal certainty through guidance or new legislation that regulates e-money issuance. Countries like Kenya, where oversight of non-bank e-money has been under general regulatory powers, have announced their intention to publish guidelines that may become regulations once an enabling payment law is in place. However, among countries with a clear legal framework, there has been a clear bifurcation between:

- those countries that allow non-bank e-money issuance, like the Philippines, which passed a general circular 649 in 2009 after a period of four years in which a mobile scheme (G-Cash) was allowed to operate under close oversight;¹⁶ and
- those that restrict e-money issuance to banks only, such as South Africa, which published an initial guideline to this effect in 2006 and reaffirmed its position in 2009.¹⁷

¹⁴ 35 of 128 countries in the World Bank Global Survey on Payment and Settlement Systems (2008) reported having oversight powers found in a payment system law, although a further 57, including many developing countries, reported having general authority to oversee payment systems. Countries in which mobile payments are already important, but which do not yet have a payment system law in place, include Kenya, Philippines, and Tanzania, although these countries reported having general or explicit authority over payment systems from other legislation.

¹⁵ Even when Mexico has not allowed non-bank institutions to issue e-money, the Mexican financial authorities have introduced a new model for banking licenses, known as niche banks, for the issuance of e-money (similar to Electronic Money Issuers). Niche banks specialize in the issuance of e-money and are subject to lower capital requirements.

¹⁶ Available online: <http://www.bsp.gov.ph/regulations/regulations.asp?id=2346>.

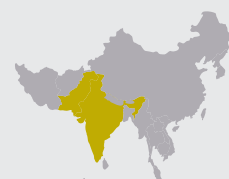
¹⁷ See Position Paper on e-money NPS01/2009: [http://www.reservebank.co.za/Internet/Publication.nsf/LADV/756673A1CFBE64D9422576690027DD17/\\$File/01_2009.pdf](http://www.reservebank.co.za/Internet/Publication.nsf/LADV/756673A1CFBE64D9422576690027DD17/$File/01_2009.pdf)

Policy questions continued

Box E: Rethinking the issue of non-bank e-money in Pakistan and India

The State Bank of Pakistan (SBP) was an early mover in publishing Branchless Banking regulations in 2008.¹⁸ These regulations stated explicitly that only bank-based models were allowed for the time being, but that a “non-bank led model will be opened up after the players and stakeholders attain the necessary level of maturity and after putting in place the necessary controls” (SBP 2008:3).

The mobile payment operative guidelines issued by the Reserve Bank of India (RBI) in 2008, like those of SBP, explicitly stated that only banks could offer mobile payment services, but went further to restrict the role of the mobile operator to “providing...connectivity and hosting certain solutions”.¹⁹ However, in 2009, the RBI issued policy guidelines that permitted non-bank entities, including mobile operators, to issue mobile-based pre-paid instruments, effectively a form of e-money. K.C Chakrabarty, Deputy Governor of the RBI, also indicated in a December 2009 speech that RBI’s insistence on a bank-based model was not the last word if inclusion goals were not achieved: “...if the banks continue as laggards, the system will have to look for an alternate non-bank model. The important end of inclusive growth cannot suffer on account of our insistence on a particular model.”²⁰



3. How should the use of the mobile phone as a channel be regulated?

Mobile channels are a subset of electronic channels available for financial services. The regulatory questions raised around the channel are therefore a subset of electronic banking transactions more generally. Many regulators have followed the general principles for e-banking set out by the Bank for International Settlements to craft e-banking regulations that providers are required to use to identify, manage, and address risks.²¹ The Bangko Sentral ng Pilipinas, for example, has issued a series of e-banking circulars over the years that set out procedures for Filipino banks to follow when launching and operating their electronic banking channels.²² Another example is Chapter X of the “Circular Unica de Bancos”, issued by the National Banking and Securities Commission of Mexico (CNBV), which takes a risk-based approach in assessing the degree of risk in the amount of each transaction.²³

Many of the risks associated with using mobile channels are the same as Internet banking with a PC or using a card at an ATM, but there are other risks that are unique. For this reason, countries such as Pakistan, India, and

Nigeria have introduced special regulations and guidelines. The State Bank of Pakistan (SBP) (2008:14), for example, identified the following special issues regarding the supply of financial services through the mobile channel:

- **Communication protocol risk:** the risk that arises when certain GSM bearer channels do not perform two-way authentication or allow for end-to-end encryption
- **Data storage risk:** the risk of unauthorized physical or logical access to transactional data stored at telco facilities or mobile devices
- **Availability and quality of service:** the risk of interruption or denial of service on mobile channels affecting the ability to transact (which is heightened when the mobile channel is the only transactional channel for a service)

For a fuller description of these risks and potential mitigation strategies, see Bezuidenhout & Porteous (2008). In response to these risks, SBP has adopted a tiered approach through which the level of data security varies with the data channel used (2008:17-18). Mexico’s CNBV provides for security requirements to vary according to channel and transaction size (see Box F).

Box F: CNBV’s approach to mobile financial services

The Mexican National Banking and Securities Commission, CNBV, has adopted a tiered approach to authentication and data transmission for mobile financial services based on the size of the transaction. This approach allows small transactions (below US\$24) to be conducted without the need for a PIN (making it fast and easy for micropayments). As transaction size increases, additional security features are required, such as full encryption, pre-registration of all beneficiaries, and compulsory notifications to the user. This tiered approach, shown in Figure 4, is an example of regulating the use of the mobile channel in a way that is proportionate to the risks involved.



¹⁸ Available online: <http://www.sbp.org.pk/bprd/2008/C2.htm>

¹⁹ Available online: http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=18432

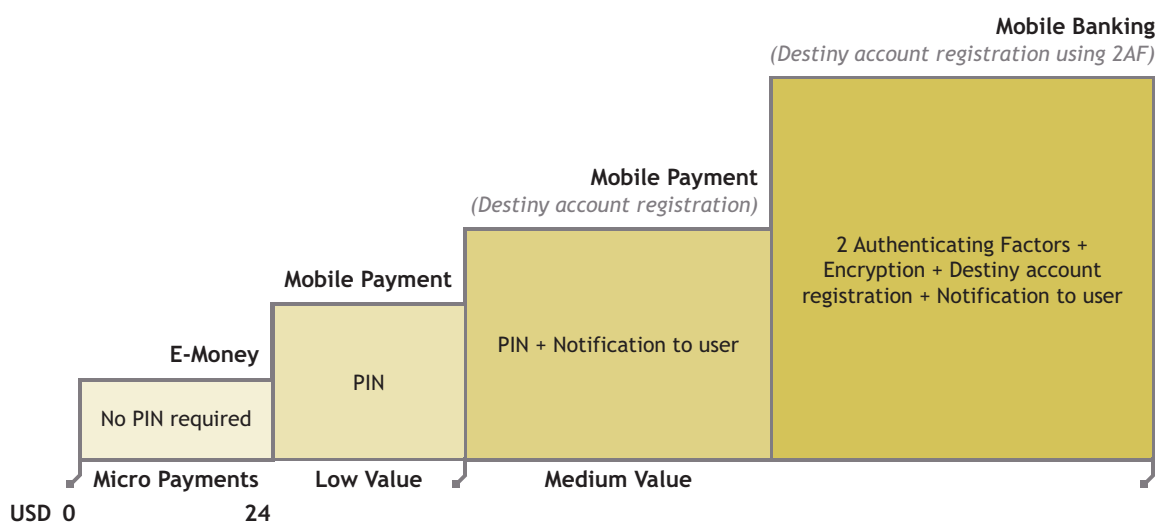
²⁰ Chakrabarty, K.C., 2009, “Mobile Commerce, Mobile Banking: The Emerging Paradigm,” India Telecom 2009 Conference, New Delhi, India, 4 December 2009, <http://rbiidocs.rbi.org.in/rdocs/Speeches/PDFs/DGKCCS0412009.pdf>.

²¹ Bank for International Settlements (BIS), 2003, “Risk Management Principles for Electronic Banking,” <http://www.bis.org/publ/bcbs98.htm>.

²² See Circular 240, <http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=570>, and Circular 269, <http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=541>, which were followed by Circular 511 on technology risk management, <http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=641>, and Circular 542 on consumer protection, <http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=1025>.

²³ Available online: <http://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20carácter%20general%20aplicables%20a%20las%20instituciones%20de%20crédito.docx>

Figure 4: Distinguishing types of mobile services in Mexico



Source: CNBV 2010

4. Do mobile financial services create new consumer protection and financial literacy challenges?

As discussed earlier, mobile financial services typically involve the provision of electronic payment instruments using agents. The consumer protection issues arising from these domains have been covered elsewhere.²⁴

The question here is whether the use of the mobile device, whether in the hands of the end consumer or an agent, changes or adds to the risks of abuse in any way.

Many consumer protection concerns commonly arising in mobile financial services, such as compromise of a PIN number or sending funds to a wrong account number, are common to card or Internet-based services as well. However, the use of mobile phones may heighten particular concerns such as:²⁵

- limited disclosure due to the restricted display capability of most phones (except smart phones);
- services that involve the transmission of PIN numbers in plaintext SMS, which can be easily compromised (these are less common now because of these concerns); and

- portability makes a mobile phone easy to misplace and customer accounts more vulnerable to access if security is inadequate.

Other common concerns, such as illiterate and first-time users being more vulnerable to abuse, are common to all new electronic payment instruments and platforms. The biggest concerns usually have more to do with expected scale of mobile deployments than with the inherent nature of mobile financial systems. These systems have the potential to connect large numbers of first-time users to the financial system in ways that may overwhelm the ability of providers and legal systems to address complaints and grievances fairly. Without adequate consumer protection schemes, mobile financial services risk becoming unattractive to clients and are unable to fulfill the goal of financial inclusion.

²⁴ See Dias & McKee (2010)

²⁵ See Bezuidenhout & Porteous (2008)

Box G: Consumer vulnerability with new electronic banking and payment channels

Because most mobile financial services deployments are new, there is so far limited evidence of complaints and abuse arising from the use of mobile channels. One of the most widespread deployments, M-Pesa in Kenya (see also Box D), has been studied widely. Collins (2010) analyzed findings from a large survey of M-Pesa users from the perspective of consumer experiences with monetary loss and perceptions of security. In fact, a very low proportion of respondents (<0.4%) reported experiencing monetary loss while sending or receiving money (the most common use of the system). A high proportion was aware of the fee structure, indicating transparency around pricing, which is a first line of defense against customer abuse. A very high percentage of the sample of users (over 90%) reported that they perceived their money to be safe, even though, unlike bank accounts, M-Pesa accounts are not covered by deposit insurance. This perception may also result from the fact that low average balances, which are the norm for M-Pesa accounts (see Box C), meant that exposure to loss was in fact low. Even the agent channel did not appear to cause undue problems: over 80% of respondents felt safe when transacting cash in agent premises although the lack of liquidity at agents sometimes prevented a cash-in or cash-out transaction (one of the most common experiences). However, this led to no loss, since the client could either wait until later or find another agent nearby (in urban areas at least). These findings are only indicative since they are based on a survey sample and at a relatively early stage of deployment, but this early evidence does not seem to suggest a need for elevated concern. However, regulators should monitor trends in complaint data across all channels on an ongoing basis to detect emerging issues.

5. What are the AML/CFT concerns in relation to mobile financial services?

Mobile financial services are relatively new in most places, and evidence of abuse of mobile financial services systems for money laundering or terrorist financing reported by operators and regulators is very limited to date. Based on evidence of how crime patterns shift slowly with the adoption of new channels, this may change over time and regulators and operators should maintain adequate controls and surveillance from the outset.

A 2008 World Bank report highlighted features of some mobile financial services that may make them vulnerable to money laundering and terrorist financing (Chatain et al, 2008). These features included greater anonymity (for users where identity verification is not required), elusiveness (the ability to cover up usage patterns), velocity (the high speed at which transactions are carried out) and poor oversight (not all models and services are currently covered by AML-CFT legislation). Many of these vulnerabilities are shared with other electronic payment instruments. In a 2010 publication, Solin and Zerzan (2010) from GSMA argued that, on a relative basis, the vulnerability of existing payment instruments to money laundering and financing of terrorism, such as cash, are greater in all respects except for the speed of transactions. Susceptibility to these risks may be greatest among agents of mobile schemes, who have higher limits than end users and more functionality, but this risk applies to financial services agents in general. Risks can be managed by introducing appropriate controls, such as limits on a transaction's value, turnover, and account balance, as well as real-time monitoring of accounts, reporting of suspicious transaction patterns, and close screening, training, and surveillance of agents.

International standards for AML-CFT set by the Financial Action Task Force (FATF) and regional bodies allow for country regulators to implement risk-based approaches. A commonly used approach is to tier CDD procedures for account opening so that the scope and intensity of verification procedures rises with the functionality and transactional limits on the account. AML-CFT regulation extends well beyond CDD to include other aspects such as record keeping and training. In addition, the system must be capable of monitoring the velocity of transactions, identifying suspicious transaction profiles, and reporting on them.

Nevertheless, there remains a relatively high degree of uncertainty among country regulators about how to apply a risk-based approach in practice, and a forthcoming World Bank report (Chatain et al, 2010) updates the earlier findings.

Whatever the specifics of the final framework, the chosen approach must ensure that account opening is simple and straightforward in order for mobile financial services to proliferate. This is because a high volume of transactions is needed for this type of business model to be profitable and to prosper. In particular, in the case of mobile payments focused on low value transactions and low value storage, the risks posed by money laundering and terrorism financing lie well below a worrisome threshold if adequate transactional limits, and monitoring requirements, are imposed. Under this scenario, the benefits of allowing for flexible CDD procedures outweigh the risk of rendering mobile financial services unviable, especially at the early development stage.

6. How should mobile financial services be supervised?

Increasingly, countries are adopting frameworks to regulate mobile financial services. With regulatory frameworks in place, the focus of attention is now moving towards the question of how best to oversee and enforce the application of the framework in the context of proliferating new mobile financial services providers.

If mobile financial services can only be offered by already-regulated entities such as banks, then the supervision of the mobile channel involves extending existing procedures (such as e-banking supervision practices) to cover the features of mobile financial services discussed above. Since technology is evolving fast in this area, understanding the operational risks arising from new channels, communication standards, and security protocols is no easy task for regulators. Some supervisors have created specialized teams with specific skills in IT and e-banking to focus on this task. The Core Information Technology Specialist Group (CITSG) at Bangko Sentral ng Pilipinas and the Supervisory Department for Operational and Information Technologies Risks at Mexico's CNBV are examples of this.

If a new class of regulated entity is created by a new framework, then additional questions arise. Regulators must identify whether these entities incur prudential risks (as e-money issuers may) and, if they do, which departments within traditional bank regulators are best positioned to supervise them. Since e-money issuance is often enabled through payment systems regulation, the task may be assigned to the payment system overseer. However, they may not be the best equipped for a role that requires knowledge of prudential supervision. On the other hand, if the prudential risks are limited and the operational risks are greater and more complex, as with 'pure' payment system providers, then maintaining the supervisory relationship through the payment system department or unit may well be appropriate. Supervision may require close coordination with other sectoral regulators such as ICT regulators, who may also license the service providers.

Whatever the appropriate scope and location for supervision of new instruments and channels, it is clear that financial regulators will need expanded resources to train and build the capacity to oversee fast-moving technology. Electronic reporting and oversight may reduce the need for physical inspection but increase the need for specialist skills in the regulator.

7. What are the implications of mandating interoperability and interconnection of mobile financial services?

In most countries, telco regulators have the authority to mandate that networks are not only interoperable (have the technological capability to exchange information) but also able to interconnect (users of one network can reach users of another). It is rare that payment system regulators have the same well-defined authority to require that retail payment systems interconnect. Especially if policy makers want to promote inclusion, financial infrastructure such as ATMs and agents should be shared so the fixed costs of deployment are spread across a larger user base. This objective is explicitly stated by regulators such as the Bank of Ghana, which requires that all existing providers and new services connect to the national financial switch. However, even this regulatory requirement does not guarantee a fully interconnected outcome and may, in fact, be counterproductive. Similarly, the expectation that interconnection will automatically emerge over time may not be realistic in all circumstances. Even in middle-income countries with developed electronic banking systems such as Brazil, regulators have deplored low levels of interconnection in card-based payment systems.²⁶

Mobile financial services add new dimensions to standard financial sector interconnection issues: on the one hand, most mobile bearer channels are fully interconnected in most places, making the wireless network already one of the most interconnected. On the other hand, different handset types, security protocols, and business models add complexity to the issue. One concern about some mobile financial services is that they are by nature 'walled gardens' created by mobile operators with limited incentives to connect to the broader financial system. However, premature regulatory intervention may also destroy commercial incentives to roll out a new system.²⁷

Most financial regulators handle this issue with care, expressing strong support for the desired outcome of full interconnection, while refraining from hasty intervention that may have unintended consequences, such as stifling the development of mobile financial services and limiting expansion to unserved segments of the population. Regulators may opt to foster interconnectivity through the creation of incentives rather than by mandate. Whatever the approach, questions about how to promote competitive healthy markets for mobile financial services is a fast-rising priority.

²⁶ See Directive 1/2006 issued by the Banco Central do Brasil: http://www.bcb.gov.br/Pom/Spb/Ing/Directive2006_1.pdf.

²⁷ See article by Houpis and Bellis, 2008.

References and further reading

- Alexandre, Claire, Ignacio Mas and Daniel Radcliffe. 2010. "Regulating New Banking Models that Can Bring Financial Services to All." Social Science Research Network: <http://ssrn.com/abstract=1664644>.
- Alliance for Financial Inclusion. 2010. "Enabling Mobile Money Transfer: The Central Bank of Kenya's Treatment of M-Pesa." <http://www.afi-global.org/en/phoca-publications-case-studies>.
- Bezuidenhout, Johann and David Porteous. 2008. "Managing the Risk of Mobile Banking Technologies." FinMark Trust. <http://www.finmark.org.za>.
- Bold, Chris. March 15, 2010. "Mobile operators and banks: if you can't beat them...buy them!" CGAP Technology Blog. <http://technology.cgap.org/2010/03/15/mobile-operators-and-banks-if-you-cant-beat-them-buy-them/>.
- Chatain, Pierre-Laurent, Raúl Hernández-Coss, Kamil Borowik, et al. 2008. *Integrity in Mobile Phone Financial Services: Measures for Mitigating the Risks from Money Laundering and Terrorist Financing*. Washington, DC: World Bank.
- Chatain, Pierre-Laurent, Andrew Zerzan, Wameek Noor, et al. forthcoming. *Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions*. Washington, DC: World Bank.
- Collins, Daryl. 2010. "Consumer experience of branchless banking." Presentation delivered at Windsor 3 Seminar on Regulating Branchless Banking, Windsor, UK.
- Comisión Nacional Bancaria y de Valores de Mexico (CNBV). 2010. "Financial Inclusion: Access through Innovation." Presentation to G20 Experts Group, Windsor, UK.
- Dias, Denise, and Katharine McKee. 2010. "Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options." Focus Note 64. Washington, D.C.: CGAP. <http://www.cgap.org/gm/document-1.9.47443/FN64.pdf>.
- Houpis, George and James Bellis. 2007. "Competition Issues in the Development of M-Transaction Schemes." In *The Transformational Potential of M-Transactions*, Vodafone SIM Panel Policy Paper 6: 36-42. http://www.nokia.com/NOKIA_COM_1/Corporate_Responsibility/Sidebars_new_concept/Transformational_Potential_of_M-Transactions/VOD833_Policy_Paper_Series.pdf.
- Jenkins, Beth. 2008. *Developing Mobile Money Ecosystems*. Washington, DC: IFC and the Harvard Kennedy School. http://www.hks.harvard.edu/m-rcbg/CSRI/publications/report_30_MOBILEMONEY.pdf.
- Leishman, Paul. 2009. "Mobile Money: A US\$5 Billion Market Opportunity: Initial findings of the CGAP-GSMA Mobile Money Market Sizing Study." *MMU Quarterly Update* 1. http://www.gsmworld.com/mmu/mmu_quarterly_update.pdf.
- Lyman, Timothy R., Mark Pickens and David Porteous. 2008. "Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance." Focus Note 43. Washington, DC: CGAP/DFID. <http://www.cgap.org/p/site/c/template.rc/1.9.2583/>.
- Mas, Ignacio and Kabir Kumar. 2008. "Banking on Mobiles: Why, How, for Whom?" Focus Note 48. Washington DC: CGAP. <http://www.cgap.org/p/site/c/template.rc/1.9.4400/>.
- Mas, Ignacio. 2009. "The Economics of Branchless Banking." *Innovations: Technology, Governance, Globalization* 4(2): 57-75. <http://www.bankablefrontier.com/assets/pdfs/INNOVATIONS-Economics%20of%20Branchless%20Banking.pdf>.
- Porteous, David. 2008. "Mobile Phone Banking: Is m-banking advancing access to basic banking services in South Africa?" Marshalltown, South Africa: Finmark Trust and Bankable Frontier Associates. http://www.finmark.org.za/new/pages/Focus-Areas/Payment-Systems.aspx?randomID=37df4fb1-05b8-46ad-aabe-4134b31e6dfe&linkPath=8&IID=8_10.
- Porteous, David. 2006. "The Enabling Environment for Mobile Banking in Africa." *Report commissioned by Department for International Development (DFID)*. Boston, MA: Bankable Frontier Associates. <http://www.bankablefrontier.com/assets/pdfs/ee.mobil.banking.report.v3.1.pdf>.
- Porteous, David. 2009. "Mobilizing Money through Enabling Regulation." *Innovations: Technology, Governance, Globalization* 4(1): 75-90. <http://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2009.4.1.75>.
- Zerzan, Andrew and Marina Solin. 2010. "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks." *GSMA Discussion Paper*. London: GSMA. <http://www.mobilemoneyexchange.org/Files/b0a2fa88>.

Examples of mobile payment regulations and guidelines

Central Bank of Nigeria. 2009. "Regulatory Framework for Mobile Payment Services in Nigeria"
<http://www.cenbank.org/OUT/CIRCULARS/BOD/2009/REGULATORY%20FRAMEWORK%20%20FOR%20MOBILE%20PAYMENTS%20SERVICES%20IN%20NIGERIA.PDF>.

Reserve Bank of India. 2008. "Mobile Payments in India: Operative Guidelines for Banks."
http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=18432. Supplemented 24 December 2009:
<http://rbidocs.rbi.org.in/rdocs/notification/PDFs/MGR241209.pdf>.

State Bank of Pakistan. 2008. "Branchless Banking Regulations." http://www.sbp.org.pk/bprd/2008/Annex_C2.pdf.

Bank of Ghana. 2008. "Guidelines for Branchless Banking." <http://www.bog.gov.gh/privatecontent/File/MPAFSD/REGULATORY%20FRAMEWORK%20FOR%20BRANCHLESS%20BANKING.pdf>

Acknowledgements

This policy note was commissioned by the Alliance for Financial Inclusion and developed by Bankable Frontier Associates with inputs from Carlos López-Moctezuma (Comisión Nacional Bancaria y de Valores, Mexico) and Raymond O. Estioko (Bangko Sentral ng Pilipinas). The note has benefitted from the review of Claire Alexandre (Bill & Melinda Gates Foundation).

Notes

About AFI

The Alliance for Financial Inclusion (AFI) is a global network of central banks and other financial inclusion policymaking bodies in developing countries. AFI provides its members with the tools and resources to share, develop and implement their knowledge of financial inclusion policies. We connect policymakers through online and face-to-face channels, supported by grants and links to strategic partners, so that policymakers can share their insights and implement the most appropriate financial inclusion policies for their countries' individual circumstances.

Alliance for Financial Inclusion

AFI, 399 Interchange Building, 24th floor, Sukhumvit Road, Klongtoey - Nua, Wattana, Bangkok 10110, Thailand
t +66 (0)2 401 9370 f +66 (0)2 402 1122 e info@afi-global.org www.afi-global.org

AFI is funded by the Bill & Melinda Gates Foundation and administered by the GTZ (German Technical Cooperation).