

GSR

2011

Discussion

Paper

The Regulatory Landscape for Mobile Banking



Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 7 October 2011.

The views expressed in this paper are those of the author and do not necessarily reflect the opinions of ITU or its Membership.



© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

TABLE OF CONTENTS

	<i>Page</i>
1.1 Introduction	1
1.2 M-banking Models	3
1.2.1 Bank-Based Model.....	3
1.2.2 Non-bank based Model.....	7
1.2.3 Comparison of Models	9
1.3 Key Regulatory Issues.....	11
1.3.1 Identification of roles and responsibilities for regulators.....	11
1.3.2 Regulatory frameworks for m-banking	14
1.4 Facilitating Roll-out and Use of Mobile Banking.....	20
1.4.1 Education on m-banking and mobile payments.....	20
1.4.2 Consumer Protection.....	22
1.5 Regulator Checklist.....	25

1 THE REGULATORY LANDSCAPE FOR MOBILE BANKING

*Authors: Janet Hernandez, Jeff Bernstein, and Amy Zirkle,
Telecommunications Management Group (TMG), Inc.*

1.1 Introduction

Nearly 2.7 billion adults in the developing world are considered “financially excluded,” that is they do not have access to basic financial services such as bank accounts.¹ 2.2 billion of the unserved adults live in Africa, Asia, Latin America, and the Middle East.² Research indicates that within developing countries, on average, one bank branch and one automated teller machine (ATM) exists for every 10,000 people.³ This lack of, or limited access to, banking and financial services constrains growth and prosperity for consumers and the economy. For these “unbanked” individuals, lack of access to banking services leaves them trapped in an oftentimes poor, cash only society.⁴ For a country’s economy, limiting banking activity to traditional approaches can stifle entrepreneurship, stunt development and even stall economic growth through the effective exclusion of large numbers of potential banking customers.

However, for those “unbanked” individuals, access to a variety of financial services is now accessible through their mobile devices (“m-banking”). This accessibility changes the landscape for these unbanked individuals since more than 4 billion people in the developing world are mobile phone subscribers.⁵ Individuals can engage in a variety of financial services, including mobile transactions and payments, by using their mobile phone and without having to visit a financial institution. Given the large penetration of

mobile services in many countries, including in developing countries, m-banking offers a potentially important way to bring banking and financial services to the “unbanked.”

M-banking services can thus be both transformative in targeting the unbanked, and additive by targeting those who already have a bank account and providing an alternative means of accessing the services available with that account.⁶ Among the advantages of m-banking are that the costs of such services are typically lower than branch-based services; transactions can be made instantly; and customers do not need to be reliant on cash or visiting a physical location that may be many miles away.⁷ This, in turn, means that banking services will not only be accessible, but can be conducted in real time offering customers greater efficiencies and providing a swift and reliable means to engage in these services.

Some m-banking services began by offering customers the opportunity to transfer airtime credits to other users as a proxy for sending electronic money, and then introduced more robust money transfer services (including bill payments, deposits to bank accounts and other common transactions) as users became more comfortable with the concept.⁸ The vendor of prepaid airtime has been transformed into a provider or enabler of banking services, accepting and disbursing cash transferred via mobile networks.

Consumer prerequisites for m-banking

- Mobile device capable of sending and receiving m-banking messages or instructions⁹
- Subscription to a mobile service
- An account at a banking institution (for bank-based services) or an MNO-based m-banking service¹⁰
- M-banking application (may be embedded on SIM card supplied by mobile operator or downloaded from bank, service provider or application store)

In the realm of m-banking, a large portion of services conducted may be viewed as mobile payment type transactions where the mobile handset plays a key role in the initiation and authorization for payment. The mobile phone can thus be transformed into a virtual wallet to make payments between parties with compatible accounts, transfer funds, and convert virtual money into cash. As m-banking services have become more widely accepted in a given market, there has often been increasing acceptance of the use of such services to transfer payment from consumers to businesses, from businesses to employees, and from governments to citizens. Beyond payments, m-banking services also serve as a secure store of value, allowing customers to store their funds electronically, making them less prone to theft or loss. M-banking services can also be leveraged to authenticate financial transactions, as discussed in Box 1. There are a variety of m-banking models, which have often been described as falling into two primary categories or on a continuum between two extremes: a bank-based model and a branchless or non-bank-based model. These models each have distinct means of operating, especially with respect to the relationship with the end customer in terms of establishing accounts, deposit taking, and lending services.¹¹ Although the universe of m-banking services now encompasses a wide range of service models that cannot always be neatly described as following one or the other model, or sometimes even being easily placed on a continuum between the two models, this paper uses these two primary models as discussion points and examines some of the ways that m-banking has been introduced around the world. It also addresses the key regulatory issues that have emerged with respect to m-banking and analyzes the ways in

which governments, particularly telecommunications and financial service regulators, can help to promote m-banking in their countries.

Because m-banking technologies and services are still in an early stage of development, it is difficult to generalize about their impact – or lack thereof – on banking activity or revenue generation. Nevertheless, according to the GSM Association (GSMA), as of July 2011, there were 122 live deployments of m-banking systems and an additional 85 planned deployments.¹² In most cases, however, m-banking services still report relatively low levels of adoption. According to a 2011 World Economic Forum report, only four countries – Ghana, Kenya, Philippines and Tanzania – demonstrate mobile financial service adoption rates above 10 percent.¹³ Nevertheless, the Central Bank of Kenya (CBK) had increases of nearly 150 percent in the number of formal bank accounts in Kenya between the end of 2005 and the end of 2008.¹⁴ The CBK attributed a significant portion of this increase to formerly unbanked consumers gaining familiarity with banking concepts through mobile operator Safaricom's m-banking service and opting to also open a formal bank account. In terms of revenues, for the year ending March 2010, revenues from M-PESA commissions accounted for 9 percent of revenues, or approximately KSH 7.56 billion (approximately USD 94.26 million). This paper primarily focuses on m-banking services in developing countries, but it is important to note that, as discussed in Box 2, there are m-banking services deployed in developed countries as well.

Box 1: Authentication of financial transactions

It is worth noting that mobile handsets and networks can be used for authentication of financial transactions, such as through the use of smartcard technology embedded in handsets or SIM cards. There is significant work underway in the mobile and banking industries with respect to the incorporation of smartcard technology into mobile devices, and new or revised regulatory frameworks will be an important component in enabling such services. In particular, the use of mobile handsets for authentication of payments will likely require an enabling environment that clearly defines the role of each party as well as the characteristics of a mobile or electronic ID for users. These important developments merit further detailed attention and are outside the scope of this paper.

Box 2: M-banking in developed countries

While this paper focuses primarily on m-banking services as they apply to developing countries, it is important to note that there are also m-banking and m-payment systems deployed in developed countries. In general, these services tend to be bank-based, offering customers mobile access to the accounts they hold in traditional banks. Such systems are seeing rapid adoption, particularly with the rising adoption of smartphones.

For example, a study released in May 2011 showed that 20 million mobile users across five European markets (United Kingdom, France, Spain, Germany and Italy), representing 8.5 percent of mobile subscribers in these markets, accessed their bank account via a mobile handset in March 2011. This represented a 15.4 percent rise in mobile banking users since August 2010, reportedly driven by smartphone users who accounted for 70 percent of the mobile banking market in March 2011. According to the study, among smartphone owners the number of banking users has risen by 40 percent since August 2010.¹⁵

1.2 M-banking Models

The growth, sustainability, and expansion of m-banking services have been characterized by the use of several different models to support the delivery of a variety of banking products and solutions. The approach or model that a company implements to roll-out m-banking services is often dependent on the country's current financial laws and regulations in force and the degree of flexibility the financial regulator wishes to allow in order to make m-banking available. In some cases, almost any model or approach may be used and the decision on how to advance m-banking will be more flexible—based on what policymakers and service providers think will work best. In other cases, countries may have detailed or strict regulations that will limit the ability of (prospective) financial service providers to offer m-banking services. Consequently, m-banking services may be required to adopt a particular model, or the countries' legislators and/or regulators will have to make changes in order for a wider set of m-banking services to be offered. Often, the constraints that may exist in a given market preventing development of any m-banking type application largely are attributed to restrictions posed by existing financial regulations. However, it may also be the case that the primary operator within a market may not have an interest in providing the applications necessary to support mobile banking.¹⁶

Although the sections below describe two primary models, many variations of each model exist. The variations in approach are often based on the unique set of circumstances in a particular country that will dictate how m-banking systems and services may be rolled out. As a result, it is perhaps better to consider these models as two ends on a scale, with multiple possibilities for m-banking in between. Figure 1 sets forth the range of business models for m-banking that may be considered. Working from top to bottom the

first model reveals a bank-based model where a mobile network operator provides the most minimal, albeit critical piece in service delivery. Working down the diagram, the various models of m-banking are presented with the final being a solely mobile run model.

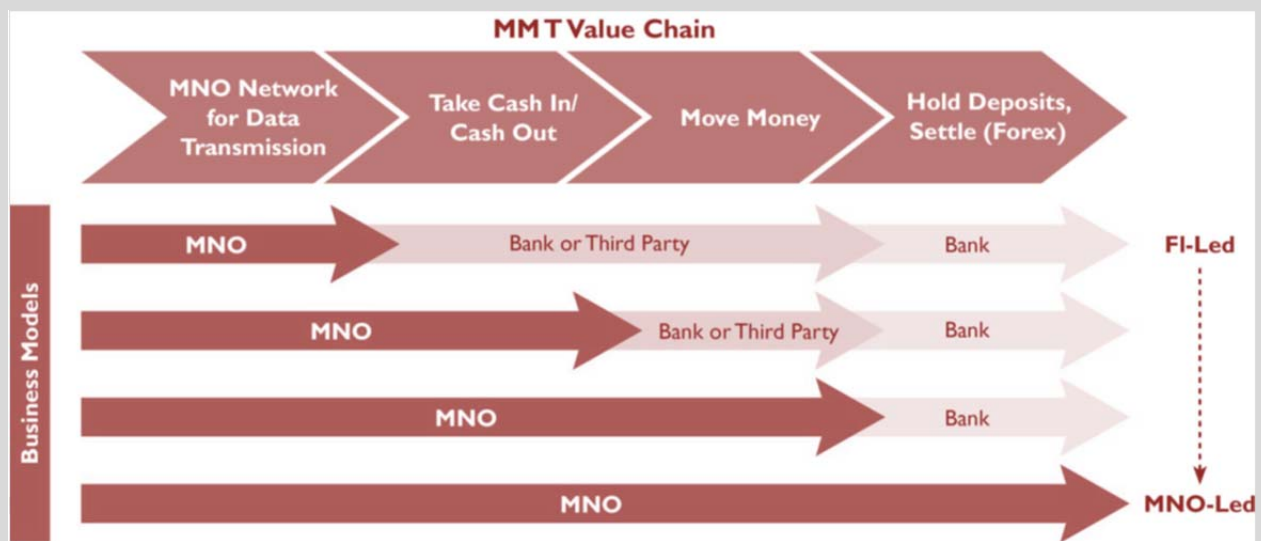
1.2.1 Bank-Based Model

The most conventional form of m-banking is the bank-based model. In this model, banks make some of their services available through the use of a mobile device, entering into an arrangement with the mobile operator to offer their services either through text messaging or more elaborate smartphone applications. This allows customers to conduct a range of financial transactions without having to go to a physical bank facility.

In the bank-based model, a customer establishes a direct contractual relationship with a licensed and supervised financial institution. The use of this model offers banks the potential to substantially increase the use of their services, both by extending new mobile services to their existing customers and by extending services to mobile telephony customers who do not currently have a bank account. In either case, the customer can access their bank accounts and other financial services through their mobile device.

The m-banking customer's relationship with his or her bank may also be carried out through the utilization of agents as a means to provide services. In simplest terms, an agent is an extension of the bank; they are able to provide commercial or transactional services e.g. customer service, keep records, handle cash and manage liquidity.¹⁷ Agents can play a role in a broad range of services including account opening, cash-in and cash-out services including disbursement of bank-approved loans and person to person transfer services.¹⁸

Figure 1: Business Models



Source: USAID FS Share, FS Series #9: Enabling Mobile Money Interventions

Many countries permit a wide range of individuals and legal entities to be agents for banks. There appears to be no singular formula for identifying suitable entities to serve as agents. In India, for example, post offices, and mobile network operators, can all act as agents. Kenya allows any for-profit organizations, such as a grocery store, or other local retail establishment in a community to act as an agent. However, non-government organizations or educational institutions cannot serve as agents.¹⁹ The determination of a suitable agent network is typically determined by the lead provider as to whether they will use existing retail chains or develop a new network.²⁰ Some approaches taken in Latin America with respect to branchless banking are for example the Brazilian and Peruvian model, i.e. using stores and smaller chains as banking agents, or the Mexican model i.e. partnering with large retail chains to set up full branches.²¹

Another bank-based approach is in Peru where mobile operator Movistar launched Pago Móvil, a service that allows Movistar subscribers to make payments charged to their Visa credit card through their mobile handset. The service is available in conjunction with Visa cards issued by several Peruvian banks.²²

Bank-based m-banking models are generally considered “additive,” meaning that mobile banking services are generally targeted to existing bank customers. These customers are typically comfortable with technology and want a convenient method in addition to credit cards, ATMs, and the Internet to

manage money without having to handle cash. Bill payment, account transfers, and balance inquiries are common services offered to retail customers.²³ Nevertheless, once an m-banking program is put in place, a financial institution may find that it can attract new customers based on the advantages that such services offer in terms of security, stability, and customer base. For example, people who previously have not had a bank account may feel more secure dealing with an established and regulated financial institution rather than a non-bank alternative, and may be more comfortable using services via their phone rather than by going to a physical bank.

In addition, some m-banking services are targeted to the unbanked but have structured as bank-based models due to existing legal and regulatory constraints that related to the provision of financial services. This was the case in Pakistan. In 2008, the State Bank of Pakistan (SBP), which acts as the regulatory authority over Pakistan’s banks, issued its branchless banking regulations.²⁴ These regulations only allowed m-banking to be provided through a bank-based model on the basis that this provided greater reliability because the existing banking institutions could be made fully liable for the provisioning of service.²⁵ However, it would allow joint ventures between a bank and an operator/non-bank, whereby the operator can be used as a channel to provide the bank’s services.²⁶ Pursuant to the SBP’s new rules favoring a bank-based model, but allowing for joint ventures, Telenor Pakistan acquired a 51 percent controlling stake in Tameer Microfinance Bank (TMB), which gave it the ability to

provide m-banking services under the new rules. Telenor Pakistan and TMB launched *easypaisa* in 2009. As noted earlier, *easypaisa* seeks to target the unbanked population rather than the existing customers of a bank. A recent study found that the majority of *easypaisa* customers (69 percent) live on less than \$3.75 per day, 40 percent live on less than \$2.50 per day, and just a few customers (5 percent) live below \$1.25 per day.²⁷ Half of the respondents did not have a bank account.²⁸ Telenor estimates that as a

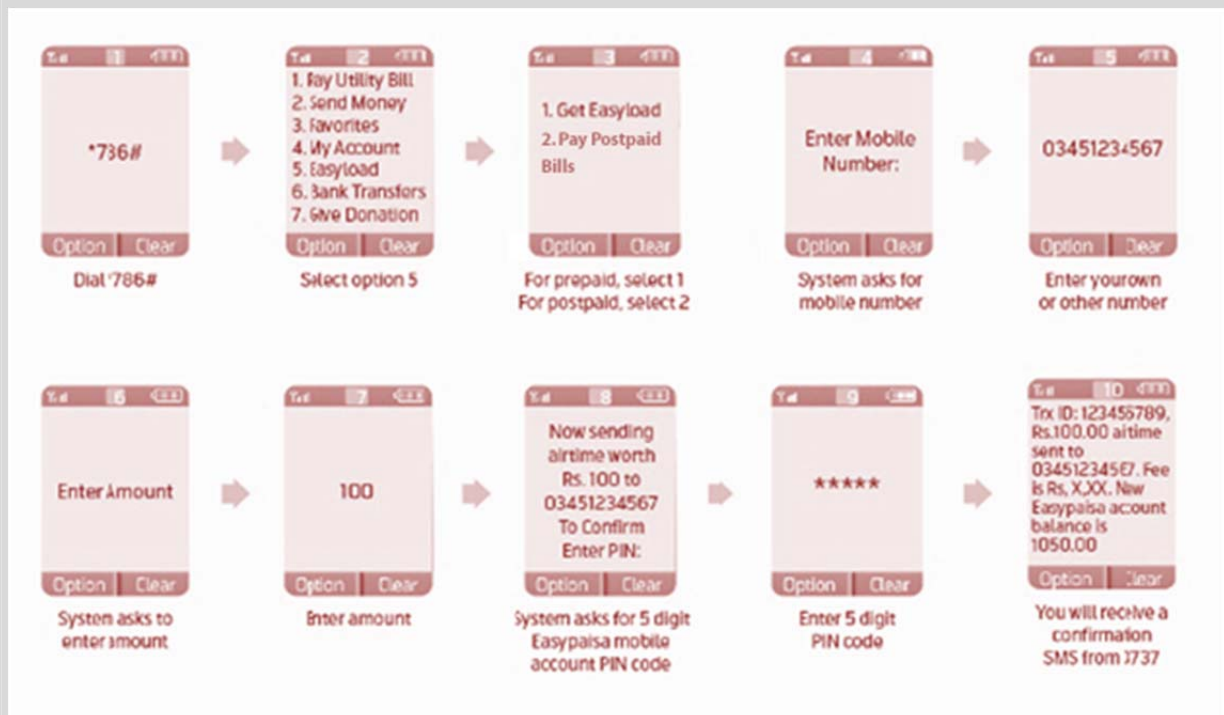
result of the provision of m-banking services, increased financial inclusion will lead to Pakistani GDP growth of 3 percent by 2020.²⁹ See Box 3 for more detail on *easypaisa* usage.

The introduction of m-banking service has often required modifications in the legal and regulatory framework. For example, in Bangladesh, non-banks offering m-banking services must obtain a license from the Bangladesh Bank (See Box 4).

Box 3: *easypaisa* – How do customers set up an account and utilize the service?

Under *easypaisa*, a customer can register for a mobile account from any of the Telenor Franchises, Telenor Sales and Service Centers, Tameer Bank branches or Tameer Bank Sales and Service Centers. The customer representative captures the customer information in the system; takes a photograph of the customer and a copy of their thumbprints; and prints out the account opening fee receipt. The customer receives a verification call from the bank within three hours, and after successful verification, an account for the customer is opened. Subscribers can either dial *786# from their handset or log into the *easypaisa* mobile account website to access their account.³⁰ Figure 2 demonstrates how *easypaisa* customers can utilize their mobile account.

Figure 2: Example *easypaisa* transaction



Source: *easypaisa*

Box 4: M-banking services in Bangladesh

In Bangladesh, as of 2009, 97% of the adult population did not have access to formal banking services.³¹ In order to facilitate allow m-banking, Bangladesh introduced certain modifications into its banking regulations. In late 2009, Bangladesh Bank (the Central Bank) published draft payment and settlement system regulations to modernize the payment and settlement systems in Bangladesh.³² Bangladesh Bank is the designated authority to grant licenses for payment systems, payment system operators and payment service providers. Under Bangladeshi regulations, payment system operators are entities licensed by Bangladesh Bank to operate a settlement system between participants, with the principal participant a bank or financial institution that maintains accounts with Bangladesh Bank for meeting cash reserve requirements. Similarly, a payment service provider must also have accounts with Bangladesh Bank for meeting cash reserve requirements.³³ The regulations also set forth provisions for the Bank to undertake corrective and remedial measures to protect against any violation of the licensing terms and conditions including the power to suspend or revoke the license, impose financial penalties and order compensation. Under these regulations, parties interested in providing m-banking services must acquire a license from Bangladesh Bank which typically takes several months.³⁴

Three banks currently offer m-banking services in Bangladesh: Dutch-Bangla Bank Limited (DBBL), BRAC Bank Ltd., and Islami Bank Bangladesh Ltd (IBBL).

DBBL was the first bank to introduce m-banking services through mobile operators Banglalink and Citycell.³⁵ Primarily using these mobile operator's retail outlets and agents, low-income individuals in remote areas can receive m-banking services such as mobile payments and remittance services. Subscribers must own a mobile phone to receive the service. Subscribers withdraw and deposit cash from the mobile by going through the agent network.

Islami Bank Bangladesh Limited (IBBL) entered into an agreement with Software Shop Limited (SSL) Wireless to provide m-banking services to existing IBBL customers. As a result, customers of IBBL can check their balance and make inquiries using their mobile phone. Customers can also receive SMS alerts and mini statements by just sending SMS to 6969 number from any mobile operator. The goal is to upgrade the service to allow customers of IBBL to receive money from anywhere in Bangladesh and abroad.³⁶

On July 22, 2011 BRAC Bank launched what it describes as Bangladesh's 'first complete mobile financial service,' offering mobile subscribers a range of banking and other financial services via their mobile phones regardless of whether they have a bank account or not. The service is being offered through bKash Ltd., a subsidiary of BRAC and in partnership with mobile operator Robi (Axiata Bangladesh). Robi customers are provided with a fully encrypted bKash mobile wallet account, developed on a VISA technology platform and fully encrypted to enable secure transactions. Customer accounts can be credited with electronic money either as salary, loan, or as domestic remittance. The cash can then be moved out as electronic money to any of the cash-out agents assigned by bKash. Currently, the service is only available to Robi subscribers but the hope is to expand this to other mobile operators in Bangladesh.³⁷

As m-banking services develop and more companies want to get involved, we are also seeing varied arrangements of the bank-based model (see Table 1).

Some banks opt not to have an exclusive arrangement with one mobile operator but allow their m-banking services to be used by any the customer of any mobile operator. For example, one of Pakistan's largest commercial banks: UBL, began offering services in 2009. It has no arrangement with a designated

mobile operator.³⁸ Rather, it follows a "one to many" model. It has built its own agent network under the brand "Omni" and can serve customers of any mobile operator, or none, with an account that can be accessed via phone or card. Similarly, mobile operators are not limiting themselves to working with just one bank to offer m-banking services. Software Shop Limited (SSL) Wireless in Bangladesh offer its m-banking services through a distributed bank system that includes over 13 banks in the country.³⁹

Table 1: Different Variations of M-Banking Models

One to One Model	Exclusive arrangement between a bank and a mobile operator.
One to Many Model	The bank provides m-banking services through multiple operators or a mobile operator provides m-banking through multiple operators.
Many to Many Model	The banks and mobile operators all provide m-banking services and exclusivity is not permitted.

Source: Telecommunications Management Group, Inc.

Following this non-exclusive paradigm, in 2008, the Bank of Ghana issued branchless banking guidelines that supported a bank-based model of m-banking using nonbank retail agents but prohibited exclusive partnerships to deliver service and only permitted what is termed a “many to many” model.⁴⁰ This approach, according to the guidelines, would offer the maximum connectivity and outreach to all given that all banks and all mobile operators should be able to “entertain each other’s customers.”⁴¹ The guidelines further note that agents can include merchants, gas stations, or the post office, but notes specifically that the customer account relationship must reside with the financial institution.⁴² There are currently three m-banking services that are provided by mobile operators in partnership with banks. These include MTN Mobile Money, Airtel Money and Tigo Cash. Of these, MTN Mobile money has the largest number of subscribers, currently approximately 1.9 million across Ghana.⁴³

1.2.2 Non-bank based Model

Under a non-bank based model, a formal bank typically only serves as a holder of deposits. The primary entity or operating unit managing the customer relationship is a non-banking entity. Most often this is a mobile operator. This model seeks to overcome the barriers that prevent the establishment of formal banks in developing economies—including remoteness, significantly high banking costs, and a lack of customer education and knowledge about financial services—by decoupling financial services from the traditional banking providers.⁴⁴

A non-bank based model has certain distinct characteristics. First, customers have no direct contractual relationship with the regulated financial institution. Instead, customers exchange cash at a retail agent in return for an electronic record of value.⁴⁵ The

customer conducts transactions (e.g., making transfers, depositing money) at a retail establishment that serves as an agent for the non-bank based service. The customer’s “money” is then recorded in a virtual account on the server of a non-bank entity.⁴⁶

Non-bank based models are typically “transformational” because the m-banking services are primarily targeted to the unbanked. This may include poor or remote populations living in informal or cash economies that have limited or no access to formal banking institutions.⁴⁷ Transformational banking focuses largely on areas where there is moderate to high mobile phone penetration coupled with a low penetration of traditional banking institutions.

Under this approach, a mobile phone can be transformed into a virtual wallet and utilized to make payments, transfer funds, and convert virtual money into cash without the need for a bank. As described in Box 5, mobile provider Globe Telecom in the Philippines, for example, offers its “GCASH” service, which provides a cashless and cardless way to transform a mobile phone into an electronic wallet meaning that the phone can be utilized to send and receive money from and to other GCASH users. A similar approach is used in Brazil, where mobile operator Oi offers its Oi Paggo service, through which payments can be made to retailers as long as both customer and retail have Oi Paggo accounts and handsets capable of text messaging.⁴⁸

The direct links to customers under a non-bank based model are the authorized agents. A variety of functions can be performed at Globe Telecom retail agents including converting virtual money into cash, making payments and transferring funds. Agents can include other local retail establishments such as grocery stores and gas stations.⁴⁹

Box 5: GCASH in the Philippines

To use the GCASH service, a Globe Telecom customer registers its account with Globe Telecom. A customer loads its mobile wallet with GCASH via a *cash-in transaction* – the process of converting cash to GCASH at a Globe Center or at any accredited GCASH partner (for example many convenience stores (e.g., 7 Eleven) are GCASH partners). The BSP requires retail agents conducting cash in and cash out functions to register with the Central Bank and send personnel for training on anti-money laundering practices.⁵⁰ Agents are also required to maintain records of all transactions for up to five years. While the Core Information and Technology Supervisory Group (CITG) within the BSP handles all mobile banking issues and supervises telecommunications companies, telecommunications companies are solely responsible and liable for their agents.⁵¹

M-banking customers under a non-bank based model can order payment of funds to anyone else who may be participating in the system and can receive payments from them. In this scenario, customers may also use m-banking as a means to transfer money between accounts and pay bills. There are two mechanisms typically used to conduct transactions – a point of sale network and phone-based system. If the system relies on a point of sale network and distributes cards, customers are required to visit a participating retail agent each and every time they want to conduct a transaction.⁵² Under a phone-based system, customers are required to visit a retail agent in order to add value by depositing cash or convert stored value back into cash.

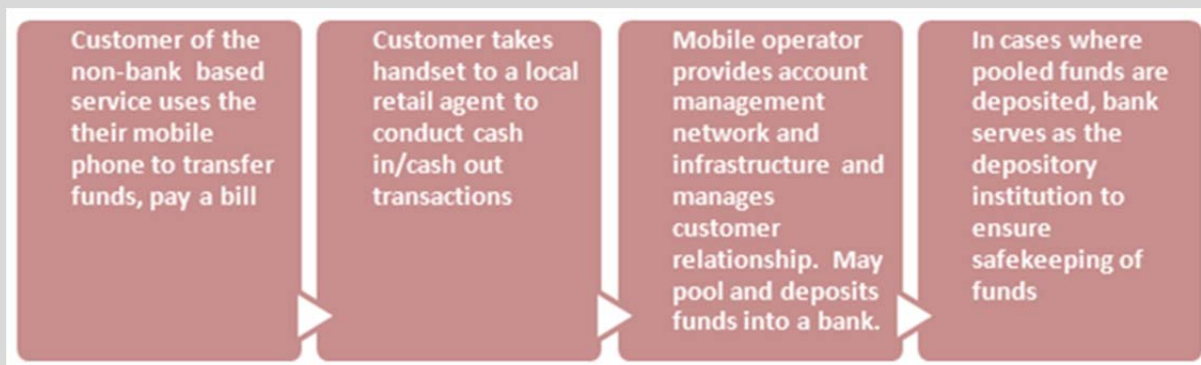
An illustration of the non-bank model is presented in Figure 3.

Perhaps the most successful non-bank m-banking service is M-PESA, a mobile money transfer service launched on a pilot basis in October 2005 by Safaricom

and Vodafone and commercially launched in March 2007 (See Box 6 for additional information on the service). The M-PESA stored value accounts are carefully structured so as not to constitute a “banking activity” under the Kenyan Banking Act.⁵³ However, to address liability concerns, M-PESA, in consultation with the Central Bank of Kenya, Safaricom invests an amount equal to M-PESA’s net deposits in commercial banks in order to ensure the safety of customer deposits.

M-PESA is at the far end of the spectrum in terms of not requiring any license to provide its services. Arguably, since M-PESA was an early entrant into the m-banking business, it was able to take advantage of more openness and flexibility from the regulatory framework. However, in many other jurisdictions, m-banking services that are provided by non-banks are subject to licensing requirements. For example, in the Philippines, the Central Bank (BSP) allows non-bank companies to provide m-banking services.⁵⁴ However, companies must first obtain prior approval from the BSP before offering such services.

Figure 3: Example of non-bank based model



Source: Telecommunications Management Group, Inc.

Box 6: M-PESA in Kenya

M-PESA targets un-banked pre-paid mobile subscribers. The service comprises a simple registration process to establish a customer’s new M-PESA account into which they can deposit, transfer and withdraw cash at a large number of Safaricom’s reseller/distribution agents. The account identifier is the mobile phone number and the customer goes to the very same place that they would go to buy airtime. M-PESA operates through a wide network of locations, including Safaricom customer care centers or M-PESA agents. Only Safaricom customers can register for M-PESA. However, recipients do not need to have an M-PESA account or be a Safaricom subscriber, although the M-PESA service is less expensive if money is sent to a registered M-PESA customer.

A current Safaricom customer may need a SIM replacement to get a new SIM with the M-PESA applications on it. SIM replacement is done at any Safaricom office. If a customer is not a Safaricom subscriber they need to purchase a Safaricom line with the M-PESA application to enable registration as a new customer.

1.2.3 Comparison of Models

1.2.3.1 Advantages and Disadvantages of the Models

Bank-based

The bank-based model of m-banking most closely mimics the traditional banking relationship and serves as an extension of that formal arrangement. Customers enter into a direct contractual relationship with a licensed and supervised financial institution. The new technology-enabled banking distribution model permits an unbundling of activities traditionally conducted at a bank branch office. As further discussed in Section 1.3.2.1, existing regulation was not developed with the convergence of telecommunications and finance in mind. This typically leaves many gaps and ambiguities through which innovative applications may not be fully considered, including those offered by bank-based m-banking service providers.⁵⁵

A disadvantage of the bank-based model is that it may not be able to innovate as easily or respond as rapidly to market needs. In addition, a bank-based model that is closely tied to existing services offered by a formal bank may have a more limited reach than a non-bank service, depending on the level of interaction the client is required to have with a bank branch.

By contrast, an advantage of the bank-based model is that requirements to mitigate risks and address data security and customer privacy are already established as banks are already required to comply with such requirements and regulations. Although banks still need to modify or add additional requirements to address the delivery of its products through a mobile device, customers may find greater comfort that the traditional brick and mortar bank is standing behind the service.

Non-Bank-based

The non-bank-based model of m-banking is typically viewed as more “transformative” because it often targets providing banking and financial services to underserved or rural regions without access to banks or the formal financial system. In this model, mobile operators are generally key to providing the service and managing the customer relationship.

Since there are different models of a non-bank based approach, the advantages and disadvantages of this model may vary. In general terms, one of the greatest advantages to the non-bank model is that it can more easily increase access to financial services for those in low-income and rural areas because the customer does not need to engage in a direct contractual relationship with the bank. An additional potential advantage may be that the company offering the service may not be subject to the more restrictive regulations imposed on a traditional bank because it does not fall under the traditional definition of a “financial institution” or its services may not fall under the definition of a “banking activity, as was the case with M-PESA mentioned above.” The non-bank based model also often more flexible in providing support through its expansive agent network. While a bank-based model often utilizes a similar network, it is generally more limited in scope to existing ATM facilities, branch offices, or mobile operator outlets. In the case of a non-bank approach, with a mobile operator taking a leading role, there is typically greater flexibility in how it approaches the establishment of an agent network, often expanding to include other local retail establishments.⁵⁶ Finally, because in a non-bank based model, the customer has a relationship primarily with the mobile operator, it can be perceived as a more familiar relationship and less daunting or overwhelming for some consumers.

From the perspective of the non-bank actor, usually a mobile network operator, four main advantages have been identified by USAID:

- Reduced customer turnover (churn),
- Better brand positioning based on service creation and innovation,
- Distribution cost reduction, and
- Additional revenues from mobile transactions.⁵⁷

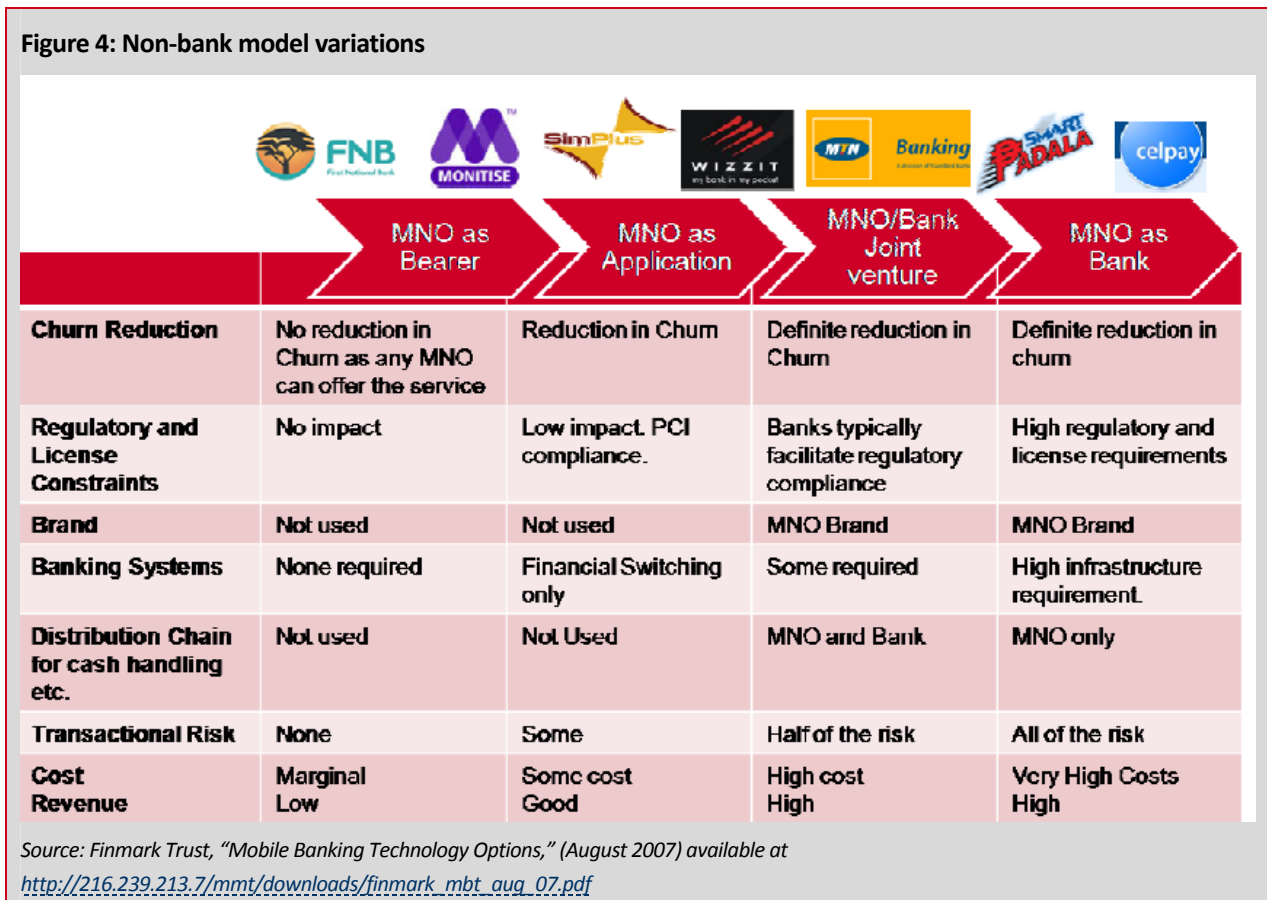
A disadvantage to a non-bank based model is ensuring that sufficient capital is in place to mitigate any financial risk due to a lack of funds within the system. This in turn could affect the liquidity of the system and the availability to provide cash to customers. A further risk associated with the non-bank based model is providing adequate consumer information and protection; particularly since many of these non-bank based customers may be new to banking and may not fully understand how these services operate through a mobile phone. In this instance, user education plays a key role⁵⁸, with the non-bank entity, usually the mobile operator, supporting this function.

The greatest potential for problems in a non-bank model is the risk of utilizing agents to serve as points of contact for transactions. While agents are utilized in a bank-based model, the distinction here is that those agents are subject to banking regulations and requirements. Under the non-bank based model, agents are not necessarily subject to the same types of policies and regulations. The potential for operational risk is thus heightened in this model. For example, customers or retail agents could commit fraud, as discussed in Section 4.2.2 or property could be stolen from a retail agent’s premises.

An additional disadvantage to the non-bank model is that it often necessitates the need for further review and refashioning of banking and/or telecommunications regulations in order to provide the service, as well as to provide adequate protection for consumers, ensure economic stability, and guarantee reasonable network interoperability.

As noted, the non-bank model can have several variations. Figure 4 presents an overview of four variations and compares some of their characteristics.

In considering both the advantages and disadvantages to the two primary m-banking models, it is important to note, that while the terms address what are “bank-based” or “non-bank based” approaches, the reality in both cases is that a banking institution is likely involved in the operation of both models. While in the case of the bank-based model, the bank stands front and center as the entity with which customers establish a business relationship, a bank may also be key to the operation of the non-bank model as well. The distinction may be that in the non-bank based approach, it is a mobile operator or other entity with which customers establish a business relationship and the bank may operate in supporting the “back office” component of the service or simply in holding the aggregated deposits collected by the mobile operator. The development of a suitable m-banking model for a given market appears to largely be driven by the legal and regulatory regimes. Thus, perhaps it is not simply bank versus non-bank models, but the determination of a suitable m-banking model evolves as a byproduct of the policy environment present in the country.



1.2.3.2 Economic Benefits

With respect to m-banking and economic development, an analysis should focus on the means by which m-banking can transform, or at a minimum, enhance economic growth. The hope is that m-banking can contribute greatly to economic development through its ability to create income generation, enabling more people to access needed financial services in a cost efficient and relevant way.⁵⁹ Overall, the rise of m-banking is expected to result in a substantial macroeconomic benefit resulting from a 5-20 percent reduction of financial exclusion by 2020 across several developing economies.⁶⁰

On a microeconomic level, m-banking has the power to create opportunities for the rural poor, through access to financial services, by increasing not just financial security, but by bringing a significant developmental impact to individuals across a range of areas. Indeed the developmental impact of mobile financial services can be significant when it intersects with other sectors such as health. In this instance m-banking services can have a significant impact within the health sector whether dealing directly with health workers as supporting salary payments, performance-based funding, vouchers or conditional cash, supply chain settlements, or directly to patients enabling payments and conditional cash transfers, micro-health insurance, and payments for transportation to hospitals/clinics.⁶¹ M-banking may also support education and further educational opportunities by enabling families to better manage their money and provide them the security to keep their children in school rather than needing to send them to work to help the family's financial situation.⁶² M-banking and m-payment systems can also be leveraged to ensure secure and less-costly delivery of government-to-person (G2P) payments, which can include social transfers as well as wage and pension payments. According to CGAP, there were at least 170 million poor people worldwide that received G2P payments.⁶³ By making such payments more secure and easier to receive and store, m-banking services could expand the developmental impact of G2P payment programs.

The model most suitable for a given country will depend on the regulatory environment and if the policies that exist favor development of one model over another. This is especially true in the case of a non-bank-based model. In order for this model to be utilized, a regulatory structure must be in place that will allow

non-banks to engage in some subset of banking activities such as facilitating payment services.

1.3 Key Regulatory Issues

M-banking presents regulatory challenges in terms of each of the models discussed in the previous section. Telecommunications, financial, and competition regulators have sometimes overlapping issues to address, while m-banking providers must navigate the regulatory requirements from all three regulators to ensure that their services comply with all relevant laws and regulations.

1.3.1 Identification of roles and responsibilities for regulators

1.3.1.1 Telecommunications regulators

As m-banking continues to attract new customers and service providers, telecommunications regulators find themselves in the position of determining what changes – if any – are necessary to their existing regulatory framework. Traditionally, the key roles for the telecommunications regulator in an economy's financial system were indirect: to ensure the reliability and security of the communications infrastructure that connected financial institutions to their customers as well as to each other – the same role played by the telecommunications regulator in most sectors outside of the ICT sector itself. Although the rise of m-banking and m-payment services does not change this role, certain additional issues come into play with the development of m-banking services.

Due to m-banking services, mobile service providers are playing a much more integral role in the transmission and/or storage of funds. This is blurring the traditionally clear boundary between regulation of telecommunications services and regulation of financial services. Depending on the business model employed by the service providers, telecommunications regulators may face questions regarding their responsibility for overseeing or facilitating these emerging services. For example, in the case of non-bank based m-banking or m-payment systems, which may not fall under the regulatory purview of financial sector regulators, does the telecommunications regulator bear any responsibility for ensuring the safety and accessibility of e-money?

Telecommunications regulators should understand the type(s) of m-banking systems already introduced in

their markets, as well as to evaluate what other type(s) of models may or may not be permitted under current telecommunications and financial regulation. This analysis should involve the coordination and participation of the financial regulator. While the financial regulator will be familiar with its own financial regulations, it is less likely to be familiar with the laws and regulations imposed on mobile operators, as well as the technical aspects of the service. In addition, in coordination with the financial regulator, the telecommunications regulator could then undertake a review of existing sector regulation to assess whether regulations need to be revised to account for m-banking and m-payment activities, and any cases in which new regulation may be required.

For example, perhaps due to the success of m-banking and greater familiarity with the service, the Pakistan Telecommunications Authority (PTA) is working with the SBP to develop revised guidelines to expand how the bank-based model operates in Pakistan.⁶⁴ The head of the PTA has expressed the need to develop a unified and open regulatory framework for further promotion and expansion of mobile banking services in the country. His vision is the establishment of a “TPS” (Third Party Solution Provider) model including mobile operators (providing m-commerce application interface), banks (providing financial services), consumers (end-user utilizing m-commerce services) and a TPS (a third party vendor performing integration of all entities).⁶⁵ Such an approach would seek to move Pakistan beyond the bank-based model and enable it to evolve to a non-bank based structure.

As will be discussed in Section 1.3.2.1, telecommunications regulators appear to have several existing responsibilities that may warrant reconsideration or revision in order to accommodate the wide range of m-banking. These areas of responsibility may include, but are not necessarily limited to, customer protection, interoperability, accounting requirements, universal service obligations, tariff regulation, and SIM registration.

1.3.1.2 Financial regulators

Financial regulators also face many questions and concerns regarding their role in the regulation and oversight of m-banking services. Often, financial regulators are empowered to specify the scope of banking services carried out by a financial institution and to issue appropriate banking licenses. A key consideration is that, in general, only banks are

authorized to take deposits, and thus the protection of deposits is a key component of banking regulation.⁶⁶ On the other hand, credit can often be offered by non-bank institutions. The question of whether m-banking services and their providers are subject to banking regulation is therefore dependent upon the determination of what constitutes a banking activity as well as how a bank is defined. Thus the financial sector regulator, depending on their enabling legislation, can play a significant role in – essentially – determining whether m-banking and m-payment activities require separate licenses from a mobile operator license; if a separate license is required, what type of licenses needs to be obtained; and more generally whether the m-banking provider will be otherwise subject to the same financial regulation as traditional banks. In considering their approach to regulation of m-banking services, financial regulators will need to aim for a regulatory regime that imposes suitable oversight and safeguards on all services identified as banking services, whether traditional or mobile, while permitting sufficient flexibility for providers to develop innovative financial products.

For example, policymakers and regulators around the world are currently debating if and how existing regulation ensuring the safety and liquidity of customer deposits to m-banking services regulation should be imposed on m-banking systems. With the bank-based m-banking model some level of protective regulation is in force, as deposits are held by banks already subject to regulation. But some non-bank based m-banking systems may currently fall outside of all financial regulation, and thus be free of such regulation. Between these two extremes may lay a number of permutations, such as the M-PESA model in which Safaricom, in consultation with the Central Bank of Kenya, invests an amount equal to its net deposits in commercial banks in order to ensure its safety.⁶⁷

Financial regulators are also the key actors in anti-money laundering (AML) activities and combating the financing of terrorism (CFT) efforts. The introduction of m-banking and m-payment services, while having the beneficial effect of expanding banking services to the unbanked, also provide new avenues for criminal or terrorist actors to move money in service of less-desirable goals. Financial regulators bear responsibility for implementing appropriate AML/CFT mechanisms, often through the use of Know Your Customer (KYC) requirements⁶⁸ imposed on financial institutions. In the case of m-banking and m-payments, financial sector regulators need to determine the appropriate balance

between stringent KYC requirements – which may limit access to banking services – and more relaxed requirements that will make it easy for more people to sign up, but that may be less effective for combating money laundering and terrorism. For example, in South Africa the government established a tiered KYC system, under which the existing AML/CFT law was amended to allow the poor and unbanked greater access to banking services by allowing less-demanding registration requirements for certain types of accounts.⁶⁹ So-called Exemption 17 accounts may be opened by South Africans who cannot provide proof of their address, but have daily and monthly restrictions on the amount of money that can be transferred out of the account, as well as maximum balance restrictions. A further change noted that m-banking falls under Exemption 17, but that if the consumer wishes to open a banking account without submitting to an in-person identity verification process, even lower limits on transfers and maximum balances apply.⁷⁰ Similarly, in Ecuador⁷¹, Colombia, Mexico and Peru⁷², the financial regulator has also authorized the creation of “basic accounts” with less-stringent KYC requirements – as well as balance or transaction limitations – that can be leveraged by m-banking providers as a means to improve financial inclusion by making banking services available to those who may not be able to satisfy the KYC requirements of a traditional bank account.

1.3.1.3 Competition authorities

Competition authorities, depending on their enabling legislation, are responsible for the enforcement of competition law, including addressing anti-competitive behavior, reviewing and approving or denying merger requests and certain business partnerships, as well as promoting competition. In addition, some competition authorities are responsible for consumer protection regulations. M-banking brings about a market situation in which divergent actors – banks and mobile operators, for example, or even alliances between banks and mobile operators – are offering substantially similar services. However, sector-specific regulators – such as the telecommunications regulator and the financial sector regulator – may also have oversight or enforcement power regarding competition matters within their specific sector.

As competition issues arise in the fields of m-banking and m-payment, it is possible that competition regulators could become involved, whether as required by the legal framework or in an advisory capacity. One analysis identified two key issues with respect to m-

banking for competition authorities: the acceptable boundaries of cooperation in payment infrastructure, and the risks of anti-competitive “lock in” of a particular service.⁷³ The exact requirement to or interest in coordination between an economy’s competition authority and either or both of the financial sector or telecommunications sector regulators will depend on the legal and regulatory framework in place.

1.3.1.4 Opportunities for coordination/cooperation among regulators

Perhaps the most important potential change to the regulatory regime with respect to m-banking is the necessity for closer cooperation and coordination among the relevant regulators. It is likely that the greatest coordination will take place between the telecommunications and financial services authorities. But other agencies are likely to be integrally involved, such as competition regulator, as well as agencies responsible for consumer protection issues. For example, in bank-based m-banking models, as mobile network operators and banks enter into partnerships to deliver and promote m-banking services, it would be preferable for the regulators to coordinate their oversight or to clearly define responsibilities so that all parties – the regulators, the companies and even consumers – clearly understand relevant regulations and oversight mechanisms for such business arrangements. Similarly, while competition issues in the telecommunications and financial sectors may currently be addressed by the relevant sector-specific regulator and the competition authority, the close relationships between network operators and financial institutions may require at least some level of consultation regarding the nature and timing of decisions in one sector and how such decisions could affect the other.⁷⁴

Cooperation between regulators will be a necessary tool for the development of a coordinated approach to the oversight of m-banking and m-payment systems. As discussed above, each regulator will have unique competencies and capabilities that can be brought to bear in a coordinated approach to regulation and oversight of m-banking services. For example, the financial regulator may benefit from relying on the technical and technological expertise of the telecommunications regulator as both seek to understand the emerging options for m-banking, m-payments and other financial transactions enabled by mobile technology.⁷⁵ Similarly, the telecommunications regulator will benefit from the specialized knowledge of the financial sector regulator with respect to, for

example, KYC requirements that could be harmonized with similar SIM registration requirements.

The specific impetus for cooperation between regulators, as well as the form such competition should take, will necessarily vary by jurisdiction, taking into account government policies and priorities, existing legal and regulatory frameworks, and market conditions. However, options for promoting cooperation and coordination could include an inter-governmental commission where the financial sector and telecommunications sector regulators periodically convene to discuss and address current and emerging issues related to m-banking. In addition, the two regulators could cross-train relevant staff members and leadership on issues related to m-banking.

1.3.2 Regulatory frameworks for m-banking

1.3.2.1 Challenges of the convergence of ICTs and financial services

In addition to the need to promote coordination and cooperation among the relevant regulators, another key challenge resulting from the ongoing convergence of ICTs and financial services are outdated legal and regulatory policies.

In many economies, the legal and regulatory environments in the banking, competition and – to a somewhat lesser extent – telecommunications sectors were developed or most recently revised well before the convergence of ICTs and financial services. For example, in Peru, banking laws and regulations previously only allowed banking to be conducted by entities with physical locations, but in 2008 were revised to enable branchless banking by allowing licensed financial institutions to make use of agents.⁷⁶ Policymakers, legislators and regulators need to review and revise frameworks to account for mobile financial services. According to one analysis, in the absence of new policies or regulations, there may be preliminary evidence to indicate a difference in m-banking opportunities between economies with civil law traditions and common law traditions.⁷⁷ Oversimplifying for the purpose of comparison, in common law systems, behavior is permitted if it is not prohibited in the law, while in civil law systems behavior is prohibited until it is expressly defined and permitted. Because the concept of banking through a mobile device may not have been considered when drafting a law or regulation in a common law country, this may allow the introduction of m-banking, as was the case of M-PESA.

In civil law systems, the regulatory ambiguities are less likely to leave space for innovation,⁷⁸ creating a different – but still important – need for revised frameworks, in this case to provide regulatory certainty and the resulting openness in the market for the entry and growth of m-banking services. We have seen such modifications to legal frameworks introduced in numerous countries such as India, Mexico, and Philippines to allow for the provision of such services. Nevertheless, even in countries where m-banking services may be allowed to operate, the regulators may still find it necessary to modify existing laws and regulations to address other aspects of the service relating to the use of agents, provision of remittance services, etc.

1.3.2.1 Other regulatory issues

The changes identified below are considered with respect to m-banking in general, rather than focusing on one particular m-banking model. Current regulatory frameworks are more likely to enable m-banking services closer to the bank-based model end of the spectrum identified in Section 1.1. However, regulatory frameworks can be amended to permit the establishment of non-bank based m-banking systems, which may help foster the spread of m-banking. Many of the challenges faced by regulators include reconsidering their existing responsibilities with an eye to oversight of m-banking and potentially making appropriate adjustments. For example:

1.3.2.1.1 Customer protection

In an environment in which m-banking becomes a crucial means of storing value or transmitting payments, who is responsible when there is an error related to a transaction? To whom should customers address their complaints? What redress mechanisms are in place? What safeguards exist to protect consumers' personal and financial data? These issues are relevant to all m-banking models, although the responsibility for addressing consumer protection would more likely fall within existing financial sector regulation for a bank-based model. By comparison, for a non-bank based model, addressing customer protection may require telecommunications regulators to look to financial sector regulators, as well as possibly consumer protection agencies for guidance, as well as to reevaluate the tools at their disposal, such as quality of service (QoS) guidelines and relevant reporting and monitoring procedures, to take into account new use cases, particularly those related to transactional errors

within a non-bank based m-banking system – a case that is not already subject to at least some level of financial sector regulation. They may also consider potential new reporting or monitoring requirements, such as tracking the number of customer queries or contacts related to m-banking concerns or errors.⁷⁹

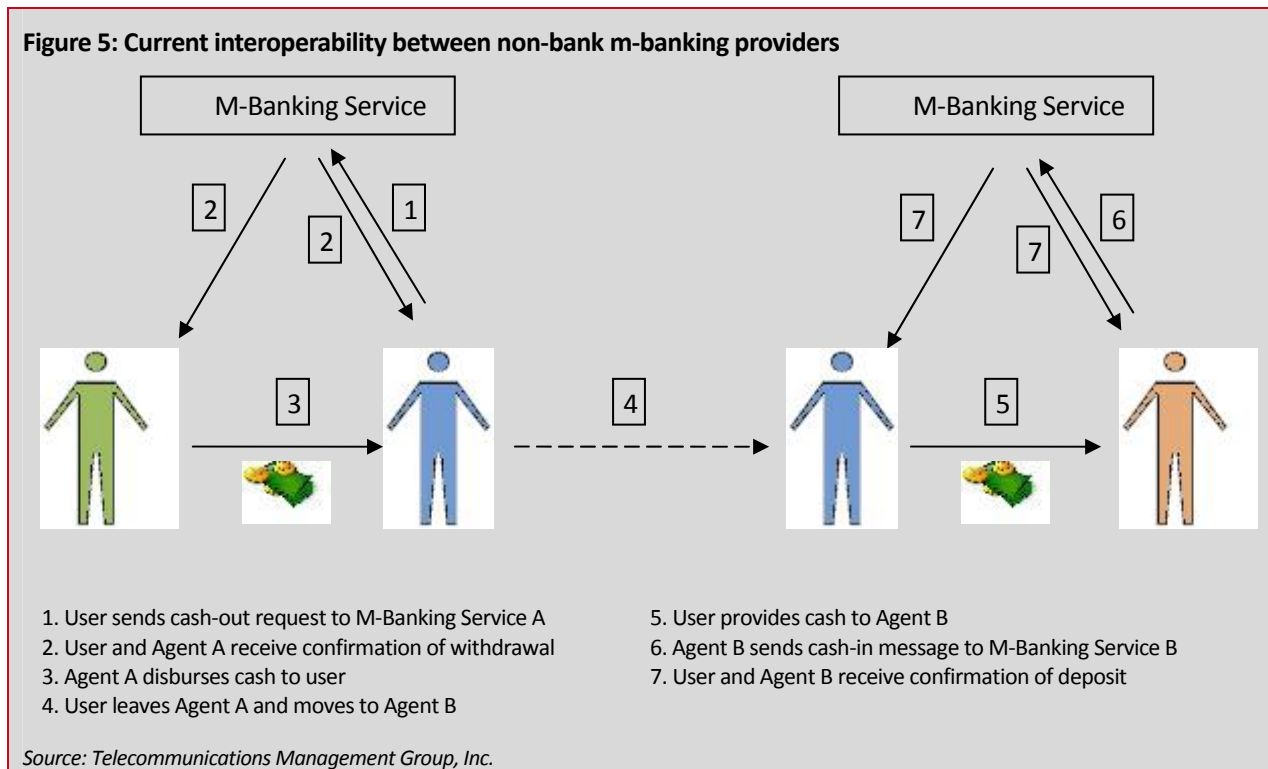
1.3.2.1.2 Interoperability

As m-banking services continue to expand, the issue of interoperability – or the ability to transfer e-money from one m-banking service to another – is likely to become increasingly important. This discussion focuses on transfers between or involving nonbank-based systems, where value is not stored in a bank, as mechanisms and protocols for inter-bank transfers – and thus between bank-based m-banking services – are well-established. As noted above, there are no widely reported interoperability agreements between providers of m-banking services that allow the direct, electronic transfer of stored value from an account in one m-banking service to an account in another m-banking service when at least one of the services does not involve a traditional bank. Unfortunately, this leads to a case such as is found in Kenya, where consumers transfer money between non-bank m-banking services by visiting an agent to cash out the desired amount of money from the first service, then carrying cash to an agent of the second service to cash in, and paying any

applicable commissions or agent fees. This situation is illustrated in Figure 5.

The issue of interoperability of m-banking systems is much more likely to require new reviews or actions as non-bank based service providers enter the market and may not have tight integration with a licensed bank. By comparison, licensed banks generally work with a clearing house – which may or may not include the economy’s central bank – that facilitates interbank transfers, or rely upon internationally accepted standards and systems for cross-border transfers. As noted by the World Bank in 2011, voluntary interconnection between m-banking account providers is feasible, but may not occur due to divergent business interests.⁸⁰

Regulators have not yet taken steps to encourage or require interoperability of m-banking systems, though they could conceivably do so, such as setting standards for interconnection of m-banking platforms or attempting to mandate interconnection, although both approaches have notable drawbacks and may not achieve the regulator’s desired result. Interconnection standards would need to be sufficiently technology neutral to minimize the risk of being outdated soon after – or perhaps before – finalization and implementation.



A technology-neutral approach could be limited to basic requirements for authentication, communication protocols and verification. Mandated interconnection would potentially have to address interconnection charges and the possibility of unbundling m-banking services (for example, the platform from the provision of accounts or payments). Financial and telecommunications sector regulators need to weigh the potential complexity of encouraging or mandating interoperability of m-banking systems against the risk of stifling innovation and investment. By way of comparison, another major banking revolution –ATMs – are driven by standards developed within the banking industry. For example, the EMV standard defines integrated-chip cards and compatible ATMs and point-of-sale terminals that can read the cards. The EMV standard was initially developed by the Europay, Mastercard and Visa global payments networks.⁸¹

In the meantime, the mobile telecommunications industry and financial services providers have taken steps to facilitate interoperability without a regulatory mandate, as described in Box 7.

1.3.2.1.3 Roaming

To date, there has been little analysis or examination of the use of m-banking or m-payment systems while roaming on a mobile network other than that which provides the customer's local m-banking service, whether within national borders or internationally. However, certain assumptions can be made regarding the use of m-banking services while roaming:

- The roaming agreement between operators will govern what types of services are available to roaming users. Thus, the ability to manage an m-banking account via SMS, smartphone applications or other means will be dependent upon the existence of a roaming agreement, the specifics of the roaming agreement and the customer's roaming profile. In cases where the mobile network operator is part of a multinational firm with subsidiaries in other markets, there is an increased likelihood of access to m-banking services.

Box 7: Facilitating m-banking interoperability

Industry-led interoperability

The GSMA has established a global mobile money transfer (MMT) initiative that includes among its principles an effort to address interoperability issues, messaging and financial transfers at an international, multilateral "hub" level rather than at the local level.⁸² The GSMA model is described in terms of international remittances, but would likely work in the same manner for any sort of inter-network transfer. In short, the GSMA's networked approach seeks to replace bilateral agreements between mobile network operators and other members of the m-banking or m-payments value chain with a multilateral approach. In the organization's view, multilateral models reduce an operator's time and resource commitments, as each operator connected to a multilateral hub is then able to send a remittance to any mobile phone user in the world on any other participating network without any additional negotiation or agreement. This, in turn, drives consumer uptake and generates economies of scale.⁸³

International remittances

Another area in which m-banking interoperability is already being addressed by stakeholders is international remittances. According to the Migration Policy Institute, in 2009, officially recorded flows totaled over US\$414 billion worldwide, including US\$316 billion sent to developing countries.⁸⁴ In 22 countries, remittances were equal to more than 10 percent of GDP in 2009; in 11 countries they were equal to more than 20 percent of GDP.⁸⁵ The key advantage of leveraging m-banking services for remittances is that they represent an opportunity to send remittances to recipients who may have limited or no access to the money transfer services or banks that comprise formal remittance channels. While visiting a bank branches or money transfer service offices may be inconvenient or impractical for many recipients, especially those in rural areas, access to a mobile handset or an m-banking agent is much more widespread. However, until m-banking services achieve greater interoperability, there are still relatively few options for sending international remittances to a user's m-banking account.

Despite this, some m-banking operators, such as Globe and SMART in the Philippines and M-PESA in Kenya, have entered into arrangements with Western Union to provide a channel for remittances. The service allows senders in selected countries to leverage Western Union's existing agents and locations to send money directly to the m-banking accounts of mobile subscribers in the Philippines and Kenya.⁸⁶ Western Union has also entered into agreements with multinational mobile operators, including MTN and Orascom Telecom, to introduce similar services in additional markets. In addition, Western Union and the GSMA are working together on a framework to more widely enable mobile money transfer services.⁸⁷

- Cash-in/cash-out services are unlikely to be available in areas where the subscriber's mobile network operator (and associated bank, in the case of bank-based models) does not have a presence, unless the network operator or associated bank has established a partnership with a local business or another m-banking service. However, to date, there have been no widely recognized partnerships between disparate m-banking services.

There have been, however, some instances of multinational operators offering m-banking services to customers roaming on networks operated by related subsidiaries. For instance, Zain's Zap⁸⁸ service was initiated in 2009 in Kenya and Tanzania,⁸⁹ followed by launches in Bahrain, Ghana, Niger, Malawi, Sierra Leone and Uganda.⁹⁰ Zain developed Zap to operate on its One Network platform, which enabled Zain subscribers in Africa and the Middle East to roam freely in all Zain markets while enjoying local calling and messaging rates and the ability to purchase airtime in any Zain market.⁹¹ At launch, Zain noted that among Zap's features was the ability to send airtime to other Zain customers in East Africa,⁹² effectively creating a cross-border m-banking system. Airtel is currently in the process of restructuring its m-banking offerings in Africa, and in June 2011 signed a memorandum of understanding with Ecobank to promote mobile banking services across the 14 African countries in which they both operate.⁹³

Telenor's *easypaisa* service advises customers that they can access their accounts when roaming on partner networks, but does not provide specific details of the services available when roaming.⁹⁴

1.3.2.1.4 SIM registration/know your customer

Although not a universal practice, there has been increasing interest among policymakers in the idea of registration of prepaid SIM cards as a means to reduce the use of prepaid mobile handsets in criminal or terrorist activities. SIM registration schemes have been introduced or considered in countries including Australia, Bolivia, Brazil, Germany, Indonesia, Japan, Liberia, Malaysia, Mexico, Norway, the Philippines, Peru, Singapore, South Africa, Switzerland, Thailand and the United States. The rise of m-banking services could prompt telecommunications regulators to alter SIM-registration programs in multiple ways. For example, SIM registration uses could be expanded to include anti-money laundering efforts, particularly in non-bank

based m-banking systems where the financial regulator may have little to no oversight.

Telecommunications regulators may also seek to coordinate or integrate SIM registration schemes with the KYC regulations that are more common in the financial sector, so as to facilitate coordination between telecommunications and financial regulators to combat fraud and financial crimes as well as to ease the registration burdens on customers of both telecommunications and financial services. The issue of m-banking service providers having detailed knowledge of their customers and/or requiring registration applies to all m-banking models as a means to comply with crime prevention requirements.

1.3.2.1.5 Universal Access/service

M-banking by definition requires adequate mobile service coverage, and thus the areas with weak mobile network coverage will face significant difficulty in leveraging m-banking services. Expanded access to mobile services, such as could be facilitated through universal access/service plans, would therefore expand the reach of banking services to more of the unbanked population. While high-income countries have near-universal mobile coverage, as recently as 2009, upper middle income countries had 91 percent population coverage, lower middle income countries had 86 percent population coverage, and low income countries had only 67 percent population coverage.⁹⁵ M-banking services led by banks and nonbanks would benefit from expanded mobile coverage and penetration driven by universal access/service policies.

1.3.2.1.6 Accounting

As network operators begin to store customers' value and to derive revenues from m-banking services, regulators will need to review accounting regulations and determine if any changes are necessary. Specifically, accounting separation requirements will likely come into play, both as a means to prevent cross-subsidization and to ensure the security of consumer value stored outside of financial institutions. This issue is more likely to be relevant to non-bank based m-banking services.

1.3.2.1.7 Tariff regulation

Tariff regulation, often employed to prevent the abuse of dominance,⁹⁶ may become a tool for creating fair competition among m-banking services. In a market

with competing m-banking service offerings, even the rate charged for a standard SMS message or a USSD short-code – currently a primary means by which m-banking transactions are executed – could differentiate service offerings. The introduction of a m-banking service alongside existing mobile services could provide new opportunities for cross-subsidization or other distortions in tariff structures as operators compete for customers. The use of tariffs as a differentiating factor among m-banking services is more likely to be a competitive issue among non-bank based m-banking services, but may also be relevant to bank-based services.

1.3.2.1.8 Law enforcement access/compliance

Finally, while there are likely to be existing regulations regarding law enforcement's authority to monitor and access traditional bank-based systems, the application of those laws to non-bank based systems may need to be evaluated. Particularly in cases where a non-bank entity is holding and transferring monies, it seems likely that law enforcement authorities will want the same visibility into those transactions as they have into traditional bank transactions.

1.3.2.2 Regulatory changes to enable and encourage m-banking

In addition to reconsidering how to execute existing responsibilities and duties, policymakers, legislators and the regulators themselves could implement more significant changes designed to create an enabling environment for m-banking services. The exact definition of an enabling environment is subjective, of course, but could be defined as being characterized by openness to new m-money and m-banking models and a degree of certainty in regulatory frameworks or guidance regarding new approaches.⁹⁷ The World Economic Forum's *Mobile Financial Services Development Report*, for example, identifies several regulatory changes that could bring more certainty and help promote m-banking, including regulations governing the use of agents to facilitate financial services, the ability of mobile operators to deploy mobile financial systems as a principal operator, the characterization of value stored in a mobile account as a "deposit" (and therefore eligible to earn interest and to be protected by deposit insurance, for example), and appropriate AML/CFT regulation for the mobile context.⁹⁸

E-money (electronic money): stored value held in the accounts of users, agents, and the provider of the mobile money service.

The specific areas of focus indicated below identify some regulatory changes that could promote m-banking.

1.3.2.2.1 Flexible telecommunications licensing for m-banking services

A country's current telecommunications regulatory regime may place restrictions on the ability of mobile operators to offer non-telecommunications services, such as m-banking or m-payment services. In some countries, the telecommunications regulator may require additional licenses. For example, value-added service licenses may be required (e.g., China, Kenya and Saudi Arabia) and the specific service to be provided must be included in the license (e.g., Philippines).⁹⁹ Requiring a separate license or the inclusion of service descriptions in a license are not insurmountable barriers to the launch of m-banking services. However, depending on the licensing process, including the efficiency of the regulator in processing license applications or amendments, such requirements may create barriers limiting or slowing the entry of mobile network operators into the m-banking market. In addition, coordination of licensing requirements with other regulators is key here as it may be that the m-banking provider may also be subject to licensing requirements from the financial regulator. In order to foster m-banking, it may be useful to see what efforts can be made to streamline any licensing process that is imposed on m-banking providers.

1.3.2.2.2 Implementation of mobile number portability (MNP)

The ability of subscribers to port their mobile number from one operator to another can present a barrier to adoption of m-banking services if, for example, a customer would like to change service providers in order to subscribe to a different operator's m-banking offering, but is unwilling to give up their existing mobile number. MNP has been introduced in a growing number of jurisdictions, so the need for regulatory change globally continues to decline. However, in markets without MNP or plans to implement it, telecommunications regulators should consider the extent to which a lack of MNP prevents m-banking adoption.

In addition to these telecommunications-specific issues, there are regulatory changes outside the telecommunications sector that will affect if and how telecommunications service providers can offer m-banking and/or m-payment systems.

1.3.2.2.3 *Implement fund safeguarding*

While licensed banks are generally subject to reserve requirements to satisfy potential depositor claims, without legislative changes, funds held by non-bank institutions are not necessarily subject to any similar requirements. Without such protections, the security of customer funds held by a non-bank entity could be seen as significantly riskier than funds held by a prudentially regulated bank. Regulations in economies including Afghanistan, Cambodia, India, Indonesia, Malaysia, the Philippines and the economies of the West African Economic and Monetary Union¹⁰⁰ have been implemented requiring nonbank issuers of e-money to maintain liquid assets at a prudentially regulated bank or sometimes in “safe” assets such as government securities, in an amount equal to the total value of customer funds collected.¹⁰¹ In some cases, these liquidity requirements are bolstered by additional regulations that limit the use of deposited funds or require that deposited funds are split among multiple banks.¹⁰² On a related note, most developing countries do not extend deposit insurance protection to the funds deposited in banks to support e-money deposits, and in cases where deposit insurance does exist, because service providers pool the accounts they service, resulting in bank-held accounts that exceed the deposit insurance coverage limits. Regulators could instead offer pass-through deposit insurance to individual customers, as is the case in certain U.S. pooled accounts, such as employee benefit accounts,, where insurance coverage passes through the plan

administrator to each participant’s interest.¹⁰³ Pass-through deposit insurance avoids a situation where pooled bank-held accounts exceed deposit insurance coverage limits by covering each depositor’s holdings up to the applicable coverage limit, even if that means that the overall pooled account would exceed the coverage limit. Regulatory changes to ensure the safety of customer deposits would reduce the potential risk of m-banking services offered by non-bank entities.

1.3.2.2.4 *Allow for interest and savings*

An advantage enjoyed by banks over non-bank providers of m-banking services is the ability to lend the customer deposits they hold, and in return to pay interest on those deposits. So far, e-banking and related regulations have prohibited the payment of interest to customers and, through measures such as the fund safeguarding regulations described above, prevented nonbank actors from investing customer deposits. The unavailability of interest-bearing accounts removes an incentive for take-up of m-banking services, as well as an incentive for using m-banking services as a vehicle for savings. Two CGAP experts have argued for allowing nonbank e-money to earn interest, given that the regulations prohibiting lending have negated the risk that customer funds would be unavailable for withdrawal.¹⁰⁴ By allowing m-banking providers to offer interest, regulators would create additional incentives for the unbanked to join the banking system. Companies, such as Safaricom, are already teaming up with banks to offer their customers interest and saving insurance (See Box 8). But although these models are promising it is still necessary for regulators to see what alternatives can be developed for non-banks to provide interest, as well as insured savings, with their m-banking services.

Box 8: M-KESHO in Kenya

In Kenya, Safaricom and Equity Bank have developed a joint product -- M-KESHO -- which provides M-PESA users with an interest bearing and insured Equity Bank account accessible through mobile phones. However, the service results in numerous fees for its low-income customers that may limit its success and popularity. In order to withdraw funds from M-KESHO, a customer must first pay a fee to transfer funds from the M-KESHO account held at Equity Bank to the M-PESA account and then pay a second fee to withdraw cash from M-PESA. These two transaction fees largely undercut any interest gains. Although models like M-KESHO are promising it is still necessary for regulators to see what alternatives can be developed to non-bank based m-banking services to provide interest, as well as insured savings.

Source: Financial Access Initiative, “M-KESHO in Kenya: A new step for M-PESA and mobile banking,” (May 27, 2010), available at <http://financialaccess.org/node/2968>.

1.3.2.2.5 *Avoid additional taxation and implement tax incentives*

Policies governing the taxation of mobile handsets and services can affect the adoption of mobile service and, by extension, m-banking services. Taxes may include value-added taxes (VAT)/goods and services taxes (GST)/sales taxes that apply broadly across the economy as well as specific taxes on telecommunications goods and services, though taxes on handsets, for example, may be significantly offset by operator subsidies. A 2006-2007 study of taxation in 101 countries found that taxes accounted for an average of 17.4 percent of the total cost of mobile ownership.¹⁰⁵ While the introduction of m-banking services may present an appealing possible new source of tax revenue, government authorities should consider whether taxation of m-banking services – in addition to existing taxes imposed on telecommunications services and equipment – is likely to have a detrimental effect on mobile and m-banking adoption.

1.3.2.2.6 *Avoid imposing detailed technical requirements for m-banking services*

Although there has been some discussion of the telecommunications regulator's role in requiring or encouraging the development of m-banking systems that are accessible to even the most basic mobile handsets and technologies,¹⁰⁶ this may run the risk of stifling innovation or competition. As has been seen around the world over the past two decades, the telecommunications industry innovates at a rapid pace, such that regulatory frameworks are often characterized as regulating the last service, not the next service. Particularly in the current early stages of m-banking development, both telecommunications and financial sector regulators should be wary of imposing detailed technical requirements on m-banking services that could deter innovation or market entry.

1.4 Facilitating Roll-out and Use of Mobile Banking

As policymakers, regulators and industry consider the utility of m-banking services and the business cases for their introduction, a number of considerations come into play regarding encouraging the deployment and use of such services, beyond the regulatory issues noted above. It is crucial, for example, that both agents and consumers be educated regarding the utility and benefits of m-banking services, and agents are additionally responsible for understanding their roles and responsibilities.

In addition, m-banking and electronic payment systems rely upon an ecosystem of technologies and services that enable easy, fast and secure financial transactions. As the popularity of m-banking grows and technologies continue to evolve, regulators and service providers will have to keep pace with technological change while preserving and improving the utility, efficiency, and security of m-banking services.

1.4.1 Education on m-banking and mobile payments

1.4.1.1 Education and training of agents

M-banking is critically reliant on the use of agents to provide services to customers. The parties to whom direct customer interaction is outsourced may or may not be agents of the bank or non-bank on whose behalf they interact with customers in the true legal sense. This can vary depending on the regulatory system and contractual arrangements that are made.¹⁰⁷ For example, in South Africa, WIZZIT, employs agents who are independent franchisees that purchase starter packs from WIZZIT. (See Box 9).

In other cases, retail agents are local airtime offices for a mobile carrier, or can be a grocer, postal facility or other business that also acts as an agent.

Agents are indispensable for m-banking growth. An agent office can be outfitted with the necessary technology and operate at a fraction of the cost of opening and operating conventional bank branches. This also makes it possible to reach new groups of poorer customers in a more profitable manner. In addition, agents offer customers both convenience and a familiar environment for those who may not be as familiar with banking practices to feel comfortable transacting business.

Agents will need to be educated and trained on the products offered and the services they are providing. Perhaps more importantly, the use of agents has created heightened risks related to providing service. These risks can include theft of an agent's cashbox or if an agent is robbed on their way to or from a bank branch. Efforts to prevent this type of theft from happening may require agents to keep smaller amounts of cash on hand or make more frequent trips to the bank to make smaller deposits.¹⁰⁸ Agents present a variety of operational risks to the provider, as well as reputational risks given that the agent is the public face of the provider.

Box 9: WIZZIT of South Africa

WIZZIT, a South African start-up company established in 2002, has partnered with the South African Bank of Athens to offer its m-banking services.¹⁰⁹ WIZZIT's target customers are the unbanked. The company does not offer its services through branches or separate offices. WIZZIT customers are recruited by Wizzkids – formerly unemployed people trained by WIZZIT to issue clients a debit card and familiarize customers with the card's use and application.¹¹⁰

One of the service's main advantages is that the m-banking technology works on any handset and SIM card and across all South African mobile networks. WIZZIT customers generally have pay-as-you-go mobile access and 16k SIM cards. For money transfers, it uses the South African inter-bank clearing system, which it accesses as an autonomous division of the South African Bank of Athens. This feature gives WIZZIT account-holders the ability to transact with any mobile user regardless of the identity of their network operator or their bank. WIZZIT has arrangements with the post office and the South African Bank of Athens, which collectively provide customers with approximately 3,500 sites for deposits. Since WIZZIT customers are issued a debit card, cash can be withdrawn at all South African ATMs. Employers can pay their staff by making payments directly into an employee's WIZZIT account electronically.¹¹¹

WIZZIT does note that it operates in compliance with the Code of Banking Practice established by the Banking Council of South Africa.¹¹² The code is a set of guidelines intended to help consumers understand how members of the association relate to their clients, promoting fairness, transparency, and adequate understanding of financial products and services, among other goals.

Agents may face challenges due to liquidity or lack thereof. Retail agents, especially those that are relatively small, unsophisticated and remote may not have enough cash on hand to meet customers' requests for withdrawals and may lack experience in the more complex liquidity management required for offering financial services. To manage liquidity effectively, agents will have to balance several variables, including turnover of cash, ease of access to the retail agent's bank account and processing time of transactions.

Many countries in which m-banking services are offered have rules related to anti-money laundering (AML) and combating the financing of terrorism (CFT). As such, m-banking providers must ensure that their agents comply with such rules. It may be necessary to have these rules adjusted to permit remote account opening with customer due diligence (CDD)/KYC rules with the limited formal documentation often associated with low income or remote customers who do not typically possess all the documents associated with establishing a traditional bank account.¹¹³ The risks surrounding AML/CFT with subsequent transactions can be limited through the use of an electronically enforced maximum allowable transaction and balance thresholds.

1.4.1.2 Consumer education and outreach

M-banking, while offering tremendous benefits to customers, especially those in poor and remote regions, also presents significant risks and challenges to

customers. Consumer education and outreach should focus on two areas. The first is ensuring that consumers understand what the service offers, how it operates, and the best ways to utilize the service. It will be critical to educate consumers on the suitable use of services offered; this, in turn, will enhance consumer protection. Consumers will also need to understand how to protect their personal information to minimize theft and enhance security.

Depending on the region where the service is offered, consumers may need to be educated on enrollment, registration and customer access procedures. It may be a new experience for some consumers to see the mobile phone as an instrument of financial management.¹¹⁴ To that end, it will be important to establish adequate consumer protection measures to ensure security of transactions and prevent fraud.

Customer education may need to focus on how best customers can experience and utilize m-banking services. Retail agents may need to provide additional materials to customers outlining what services are offered and how they are used. Further information should be made available if there are customer complaints or a means for resolution of any concerns or problems customers encounter through agents.

1.4.1.3 Credit history

While some observers have identified m-banking services as a means to begin developing credit histories

among formerly unbanked users, there has been little published research in this area to date. One study, conducted in Kenya by USAID, drew several conclusions regarding the potential for building credit history via m-banking services in that country.¹¹⁵ Some of these conclusions are likely applicable broadly across markets in which m-banking services are active, and others that are likely more relevant to developing countries, as indicated in Table 2. It may be that the market and regulations will need time to adjust to and enable the use of m-banking transactions to develop credit history for users, as has been the case with prepaid credit cards in developed markets such as the United States.

1.4.2 Consumer Protection

1.4.2.1 Transaction Security

Ensuring transaction security in m-banking and m-payment systems has multiple aspects, overlapping considerably with existing measures to ensure security in electronic financial transactions. While these responsibilities are not unique to m-banking, they are arguably even more relevant in a mobile context, where handsets can be easily misplaced or stolen.

With respect to telecommunications networks, the threats to m-banking are the same that apply to any

other services delivered over the mobile network. Such security issues include:

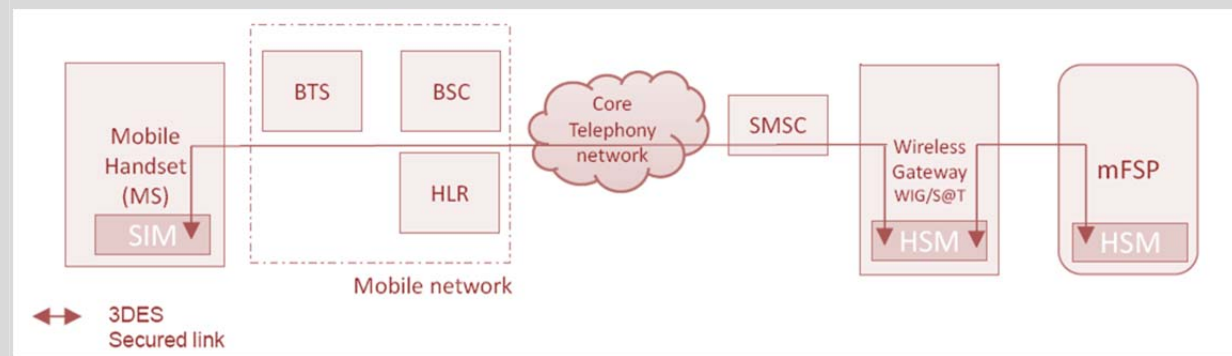
- attempts to disable or damage the network infrastructure, including denial of service attacks;
- attempts to limit legitimate users' access to the network, such as through wireless interference;
- unauthorized access to the network; and
- interception, monitoring or alteration of transmissions.

Telecommunications operators and vendors have invested heavily in technologies and processes to minimize security issues on mobile networks, and such technologies can be applied to m-banking services as well. In the case of an m-banking service enabled by the SIM Application Toolkit¹¹⁶, in which the m-banking application resides on a SIM card obtained from the network operator, the security model can be illustrated as shown in Figure 6. In this case, the SIM card contains security keys that are linked to keys in the high-security module (HSM) attached to the wireless gateway, which are in turn linked to keys at the HSM on the mobile financial services provider's (mFSP) network. The entry of a PIN and commands by the user are encrypted between the handset and the HSM, then deciphered and reencrypted by the HSM for transmission to the mFSP.

Broadly applicable	More relevant to developing markets
Mobile transaction data may be more useful as a market segmentation tool to separate lower- and higher-risk segments.	Licensed and functioning credit reference bureaus must be established – and relevant regulations implemented – before attention can shift to alternative (i.e., non-bank) data sources for credit history, such as mobile network operators.
There may need to be a longer record history before one can gain a reliable sense of behavior and trends from the data.	Regulations must allow the disclosure of mobile subscription statement and account data to third parties, such as credit bureaus. Regulators may need to amend regulations to require or allow the sharing of data such as mobile transaction data or utility payments.
The data potentially have predictive value—that is, they may increase the accuracy of credit scoring and risk evaluation models to predict ability to repay or likelihood of default—when combined with mainstream credit bureau data.	A clear and compelling business case is needed in order for MNOs and m-payment providers to share information with and subscribe to a credit reference bureau.

Source: Telecommunications Management Group, Inc., adapted from USAID Mobile Banking – The Key to Building Credit History for the Poor?

Figure 6: Sample m-banking security model



Source: Bankable Frontiers

The Bank for International Settlements (BIS) in 2003 suggested a series of risk management principles for application to electronic banking, many of which are applicable in the more specific context of m-banking.¹¹⁷ A 2008 report reconsidered the BIS principles and their applicability or implications for m-banking.¹¹⁸ The list below presents the principles that are arguably most relevant to the protection of m-banking transactions. Service providers should:

- take appropriate measures to authenticate the identity and authorization of customers with whom they conduct business over the Internet;
- use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions;
- ensure that appropriate measures are in place to promote adequate segmentation of duties within e-banking systems, databases and applications;
- ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications;
- ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information;
- ensure that clear audit trails exist for all e-banking transactions;
- take appropriate measures to preserve the confidentiality of key e-banking information, commensurate with the sensitivity of the information being transmitted or stored;
- take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions in which supplying e-banking services;

- have effective capacity, business continuity and contingency planning processes to ensure the availability of e-banking systems and services; and
- develop appropriate incident response plans to manage, contain and minimize problems from unexpected events including internal and external attacks that may hamper provision of services and products.

As both m-banking services and telecommunications networks continue to evolve, there will be new opportunities for both threats to m-banking security and techniques to mitigate such threats. For example, while most m-banking and m-payment transactions in developing countries are conducted using relatively basic handsets, more powerful (3G or 4G) handsets enable more complex security functionality. However, the introduction of additional complexity in both the handset and the banking application can also create additional opportunities for malicious attacks (hacking) or for security failures. As described in Box 10, the ITU has issued recommendations related to m-banking security.

1.4.2.2 Fraud Prevention

Fraud prevention is ultimately the responsibility of the m-banking service provider, regardless of the m-banking model employed. Responsibility for oversight and enforcement of anti-fraud measures depend on the legal and regulatory framework and the m-banking model employed, and may fall under the jurisdiction of agencies including law enforcement, the financial sector regulator or the telecommunications regulator, or some combination of those agencies. An example of a telecommunications regulator with significant responsibility for preventing fraud as it relates to m-

banking is found in Kenya, where the Communications Commission of Kenya (CCK) is charged with facilitating the development of e-commerce, including responsibility for developing a sound framework to minimize forged electronic records and fraud in e-commerce and other electronic transactions.¹¹⁹

Fraud can take many forms, but can be generally categorized into four cases (see Table 3), as identified by CGAP: (i) money laundering; (ii) defrauding of customers by agents or other consumers; (iii) agents defrauding the service or system; or (iv) individuals/consumers defrauding agents.¹²⁰

Box 10: ITU Recommendations on M-banking security

In September 2010, ITU-T issued two recommendations related to secure mobile financial transactions, identifying four security levels that address all necessary security dimensions. ITU-T Recommendation Y.2740 describes the principles of security system development for mobile commerce and mobile banking systems, including security requirements for mobile commerce and mobile banking systems, based on four security levels, known as Assurance Levels. Recommendation Y.2740 also outlines probable risks in the mobile commerce and mobile banking systems, and specifies means of risk reduction. Recommendation Y.2741 specifies the general architecture of a security solution for mobile commerce and mobile banking, describing the key participants, their roles, and the operational scenarios of the mobile commerce and mobile banking systems. The recommendation also provides examples of implementation models of mobile commerce and mobile banking systems, beginning with enrollment in a mobile payment system and concluding with usage of the payment system, including transactions between discrete systems.

Money laundering	Service providers will need to comply with applicable AML regulations. CGAP suggests proportionate regulation that is effective, but not so stringent as to be a barrier to poor customers who transact small amounts.	The most effective AML approach is for providers to comply with regulations and, if applicable, encourage regulators to develop effective, proportionate regulation.
Customers are defrauded	Agents can defraud customers, especially in environments in which customers are less-educated and rely on verbal instructions rather than on written material. For example, agents can pretend to make a cash-in transaction or change the fees they charge for providing a service. It is also possible that bank tellers or agents recommend a simple PIN for the customer to use, generally in good faith to help customers who are not familiar with the concept. Despite good intentions, such a situation can enable agents to use the information to defraud the customer. Customers can also be defrauded by other customers who gain access to their PIN or personal information.	Providers can educate customers regarding how the system works, including the importance of safeguarding information such as PINs and the need to wait for official confirmation (often via SMS) that a transaction is complete. Education efforts can include radio, television, posters, graphics, and other alternatives to written material. Providers should also have a call center where customers can call with questions or to complain about potential fraud. Further, providers should have a clear policy regarding reimbursement of individuals who have been defrauded.
Agents and customers defraud the system	Agents and customers can work together to defraud the service, such as by splitting one transaction into two or more smaller ones in order to work around a pricing structure that charges higher fees for larger transactions. In addition, customers can defraud the system by making direct deposit into a different phone number than their own, in effect “transferring” funds to another person’s m-wallet without paying a transfer fee. Also, agents can partner with customers to take advantage of a spread between commissions and fees by making repeated deposits and withdrawals and splitting the difference between commissions and fees.	Providers can develop internal systems to monitor transactions and quickly identify suspicious transactions or transaction patterns, such as repeated similar or identical transactions by a customer a short period, or multiple failures of a transaction by an agent. Providers can also examine their pricing and commission models for vulnerability to fraud.

<p>Customers (or those posing as customers) defraud agents</p>	<p>Although agents are well trained compared to customers, they are not immune to fraud and abuse by customers. In one example, thieves pretended to represent Safaricom auditors in order to gain access to an agent’s accounts and used the information obtained to generate fraudulent SMS messages to the agent to facilitate a cash-out transaction.</p>	<p>Providers can continue to invest in rigorous agent training, arguably the best defense against fraud and abuse. Providers should also consider ensuring that handset user interfaces clearly differentiate m-banking-related messages from other functions and messages so that messages from the provider are distinctive and not easily imitated. Providers may also consider compensating agents who are defrauded in order to avoid inadvertently encouraging agents to keep cash limits low, which could ultimately harm customer service standards.</p>
---	---	--

Source: CGAP, *Agent Management Toolkit: Building a Viable Network of Branchless Banking Agents – Technical Guide*

1.5 Regulator Checklist

Each market will have its own unique policy, legal and regulatory environment with respect to m-banking and m-payment systems. The goal of the checklist below is to: (i) identify the issues and challenges faced

by policymakers and regulators with the introduction of m-banking (or the desire to facilitate its introduction); (ii) identify possible action items to address the issue/challenge; (iii) provide representative examples of countries that have successfully addressed these particular issues.¹²¹

Issue/Challenge	Action	Representative Example
Evaluation of current permissibility for m-banking		
<p>1. Is the introduction or deployment of m-banking services permissible under the current financial sector legal and regulatory regime? Have currently permissible m-banking model(s) been identified?</p>	<ul style="list-style-type: none"> • If m-banking is permissible, identify potential areas for review or streamlining of regulations to smooth introduction or expansion of m-banking services and provide an appropriate level of flexibility. • If m-banking is not permissible, assess how m-banking will impact stability of financial system, and revise or draft applicable legislation and/or regulations. 	<p>Pakistan</p>
<p>2. Has the unbanked population been identified?</p>	<ul style="list-style-type: none"> • Develop an approach for quantifying and identifying the unbanked population. • Compare populations reached by mobile services and banking services. 	
<p>3. Does the government actively encourage the introduction of m-banking services?</p>	<ul style="list-style-type: none"> • Identify policy or regulatory changes that could encourage the introduction or expansion of m-banking services. 	<p>Philippines</p>
<p>4. Is a high-level m-banking policy necessary or appropriate?</p>	<ul style="list-style-type: none"> • Government develops m-banking policy. • Input from sector regulators • Define roles of regulators with respect to m-banking, including oversight of competition 	<p>Philippines</p>
<p>5. Is there a process for cooperation or coordination between the telecommunications and financial regulators, as well as other relevant regulators, regarding m-banking?</p>	<ul style="list-style-type: none"> • Implement mechanism or requirement for cooperation, such as: <ul style="list-style-type: none"> – Joint commission – Training 	<p>Colombia</p>

Evaluation of regulation and practices relevant to m-banking		
6. Is telecommunications network coverage and capacity adequate to support m-banking?	<ul style="list-style-type: none"> • Develop policies to support increased build out by: <ul style="list-style-type: none"> – Facilitating competition – Providing tax incentives – Implementing regulatory reforms – Implementing universal service reform 	Kenya
7. Is lack of mobile service coverage preventing m-banking adoption?	<ul style="list-style-type: none"> – Revise and strengthen universal service/access plans to expand mobile coverage. – Consider licensing requirements for minimum coverage. 	Ghana
8. Are network security practices sufficient to protect m-banking information?	<ul style="list-style-type: none"> • Develop/adopt new standards for financial and transaction security. • Revise applicable laws/regulations to reflect appropriate security concerns. 	Pakistan
9. Are device security/encryption requirements sufficient to protect m-banking information?	<ul style="list-style-type: none"> • Require use of internationally-accepted secure transaction/transmission formats. 	South Africa
10. Do current network infrastructures enable interconnection and interoperability of m-banking services?	<ul style="list-style-type: none"> • Determine if/how to encourage or mandate interconnection or interoperability. 	Ghana
11. Have undesirable gaps or prohibitions in telecommunications sector regulations been identified and addressed? Do network operators face barriers to entry into the financial services market?	<ul style="list-style-type: none"> • Review telecommunications sector regulatory framework to assess necessary changes to address m-banking. • Identify barriers to provision of financial services by mobile network operators. 	Kenya
12. Do m-banking services and traditional banking services face the same level of regulation? Should they?	<ul style="list-style-type: none"> • Determine if there is a need to differentiate the regulation of m-banking and traditional banking. 	
Emerging legal and regulatory issues relevant to m-banking		
13. Does the legal/regulatory framework define and enable e-money and e-commerce?	<ul style="list-style-type: none"> • Conduct a review of e-money/e-commerce (and potentially other related issues) regulation and revise or create new instruments as appropriate. 	European Union
14. Are banking agents subject to oversight and regulation? If so, who is the responsible regulator? Are there processes for conflict mediation, dispute management, etc. between banks or network operators and their agents?	<ul style="list-style-type: none"> • Develop or revise regulations to address agent practices and relationships with banks and/or mobile networks. 	Brasil
15. Are AML/CFT measures applicable and proportionate in the case of m-banking services? Do KYC requirements present disproportionate barriers for the unbanked to obtain m-banking service?	<ul style="list-style-type: none"> • Determine if changes to existing AML/CFT regulations are necessary in the context of m-banking. Consider suitability of current requirements to m-banking. <ul style="list-style-type: none"> – Consider tiered KYC requirements – Consider synchronization between financial and telecommunications sector requirements. 	United Kingdom

16. Does the current legal/regulatory framework address m-banking transaction security needs?	<ul style="list-style-type: none"> Determine if current banking transaction security measures apply to m-banking, and if necessary revise accordingly in order to increase confidence in m-banking services. 	Ghana
17. Are fund safeguarding requirements in place for nonbank-based m-banking services?	<ul style="list-style-type: none"> Determine if/how nonbank-based m-banking services are required to safeguard consumer funds/value. 	Malaysia
18. Can users transfer value directly from one m-banking service to another?	<ul style="list-style-type: none"> Determine if inability to transfer value is due to regulation or industry. Consider if inability to transfer value constitutes anti-competitive behavior. 	Ghana
19. Are accounting separation measures in place to prevent nonbank-based services from engaging in cross-subsidization involving m-banking activities?	<ul style="list-style-type: none"> Review and revise accounting separation requirements to ensure segregation of m-banking activities. 	
20. Can tariffs be regulated to prevent anti-competitive activity?	<ul style="list-style-type: none"> Review and revise tariff regulations, for example, by considering that SMS and/or data access tariffs affect the cost of m-banking services. 	
21. Is responsibility for ongoing monitoring and enforcement of relevant laws and regulations clearly assigned?	<ul style="list-style-type: none"> Government and regulators should coordinate to clearly define each agency's responsibilities. <ul style="list-style-type: none"> Legislation Joint working group Memorandum of Understanding 	India
22. Are existing consumer protection/data privacy regulations adequate?	<ul style="list-style-type: none"> Review and revise relevant regulations to enable and enhance customer protection in order to increase confidence in m-banking services. 	México
23. Is additional consumer education regarding m-banking/m-payment necessary or beneficial?	<ul style="list-style-type: none"> Encourage – or require – customer education efforts. <ul style="list-style-type: none"> Regulators can reach out to customers directly, or Service providers can be encouraged or required to engage in educational efforts. 	Pakistan
24. Does the current mobile number portability regime enable users to move between m-banking providers?	<ul style="list-style-type: none"> Consider if/how introduction or revision of MNP requirements could enhance competition in m-banking. 	Ghana

Source: Telecommunications Management Group (TMG)

-
- 1 Consultative Group to Assist the Poor (CGAP), "Tilman Ehrbeck interview: Full financial inclusion in our lifetime," (August 19, 2011), available at www.cgap.org/gm/document-1.9.53154/Tilman_Ehrbeck_Transcript.pdf.
- 2 Financial Access Initiative Framing Note, "Half of the world is Unbaked." (October 2009) available at http://financialaccess.org/sites/default/files/110109%20HalfUnbaked_0.pdf
- 3 McKinsey & Company, "Capturing the promise of mobile banking in emerging markets," (February 2010), available at www.mckinseyquarterly.com/Telecommunications/Strategy_Analysis/Capturing_the_promise_of_mobile_banking_in_emerging_markets_2539?gp=1.
- 4 Rasheda Sultana, *Mobile Banking: Overview of Regulatory Framework in Emerging Markets*, Grameenphone Ltd., (2009).
- 5 Key ICT indicators for developed and developing countries and the world (totals and penetration rates), available at www.itu.int/ITU-D/ict/statistics/index.html.
- 6 Johan Hellstrom, "The Innovative use of Mobile Applications in East Africa," *Sida Review* 2010:12 (May 2010).
- 7 Rasheda Sultana, *Mobile Banking: Overview of Regulatory Framework in Emerging Markets*, Grameenphone Ltd., (2009).
- 8 USAID, "FS Series #9: Enabling Mobile Money Interventions," (April 2010) at 13, available at http://pdf.usaid.gov/pdf_docs/PNADW294.pdf.
- 9 Depending on the specific m-banking service, capabilities could include SMS, USSD or a mobile broadband connection.
- 10 Consumer may be able to open an account through an agent, depending on m-banking service and appropriate legal/regulatory framework.
- 11 State Bank of Pakistan, *Policy Paper on Regulatory Framework for Mobile Banking in Pakistan*, Banking Policy & Regulations Department, available at www.sbp.org.pk/bprd/2007/Policy_Paper_RF_Mobile_Banking_07-Jun-07.pdf.
- 12 GSMA, "Mobile Money Live," available at www.wirelessintelligence.com/mobile-money/.
- 13 James Bilodeau, William Hoffman and Sjoerd Nikkelen, "Findings from the Mobile Financial Services Development Report," *The Mobile Financial Services Development Report 2011* (2011), available at http://www3.weforum.org/docs/WEF_MFSD_Report_2011.pdf.
- 14 USAID, *Mobile banking: The key to building credit history for the poor?* (April 2009) at ix, quoting Matu Mugo, Manager, Bank Supervision, Central Bank of Kenya, on March 26, 2009.
- 15 comScore, "Europe Sees 40 Percent Growth in Mobile Banking Through Smartphones," (May 27, 2011), available at www.comscore.com/Press_Events/Press_Releases/2011/5/Europe_Sees_40_Percent_Growth_in_Mobile_Banking_Through_Smartphones.
- 16 Kabir Kumar, Claudia McKay, and Sarah Rotman, "Microfinance and Mobile Banking: The Story So Far," (July 2010), CGAP Focus Note. No. 62, available at http://www.cgap.org/gm/document-1.9.45546/FN62_rev2.pdf.
- 17 Michael Tarazi and Paul Breloff, "Regulating Banking Agents," (March 2011), CGAP Focus Note No. 68, available at www.cgap.org/gm/document-1.9.50419/FN68.pdf.
- 18 *Ibid.*
- 19 *Ibid.*
- 20 CGAP, Building a Viable Network of Branchless Banking Agents, June 2011, available at <http://technology.cgap.org/2011/06/09/need-to-train-your-colleagues-about-agents-cgap-releases-agent-management-training-package/>.
- 21 <http://technology.cgap.org/2007/06/12/will-peru-be-the-next-mexico-or-the-next-brazil/>
- 22 VisaNet Peru, "Visanet y Movistar lanzan sistema de pago móvil," available at www.visanet.com.pe/visanet_new/detalle_noticia.asp?id=5.
- 23 Federal Reserve Bank of San Francisco, "Asia Focus," (November 2010).

- ²⁴ State Bank of Pakistan, *Branchless Banking Regulations for Financial Institutions Desirous to undertake Branchless Banking*, (March 31, 2008), available at http://www.sbp.org.pk/bprd/2008/Annex_C2.pdf.
- ²⁵ *Ibid.*
- ²⁶ The regulations did note that the government would consider the prospect of introducing non-bank based models at a later stage.
- ²⁷ CGAP, "Does Branchless Banking Reach Poor People?" (June 7, 2011), available at <http://technology.cgap.org/2011/06/07/does-branchless-banking-reach-poor-people-the-evidence-from-pakistan/>.
- ²⁸ *Ibid.*
- ²⁹ Telenor Group, *Shaping our Financial Future: Socio-economic impact of mobile financial services*, (2011).
- ³⁰ Easypaisa, "Easyload," available at www.easypaisa.com.pk/index.php/en/easy-load.
- ³¹ As of 2009 approximately only 3% of the adult population had formal access to banking services; see Rasheda Sultana, *Mobile Banking: Overview of Regulatory Framework in Emerging Markets*, Grameenphone Ltd., (2009)
- ³² Rasheda Sultana, *Mobile Banking: Overview of Regulatory Framework in Emerging Markets*, Grameenphone Ltd., (2009).
- ³³ *Ibid.*
- ³⁴ *Ibid.*
- ³⁵ Orascom Telecomm Bangladesh Limited ("Banglalink") is fully owned by Orascom Telecom Holding S.A.E., Egypt, the parent company of the group is Vimpelcom; Citycell (Pacific Bangladesh Telecom Limited) is public limited company and its shareholders are: Pacific Motors Limited, Pacific Traders Limited, Pacific Industries Limited, Far East Telecom Limited, SingTel Asia Pacific Investments Pte Ltd, SingTel Consultancy Pte Ltd, Singapore Telecom Paging Pte Ltd.
- ³⁶ Islami Bank Bangladesh Limited, "Islami Bank Bangladesh Limited Introduces Mobile Banking Services," available at www.islamibankbd.com/news.php?Events=160.
- ³⁷ The Daily Star, "BRAC Bank launches mobile banking service," (July 22, 2011), available at www.thedailystar.net/newDesign/news-details.php?nid=195176; bKash, "Frequently Asked Questions," available at www.bkash.com/faq.php.
- ³⁸ Chris Bold (CGAP), "Pakistan: Branchless Banking's Business Model Laboratory," (May 2011), available at <http://technology.cgap.org/2011/05/24/pakistan-branchless-banking%E2%80%99s-business-model-laboratory-2/>.
- ³⁹ SSL Wireless, "Mobile Financial Services," available at www.sslwireless.com/index.php/services-portfolio/mobile-financial-services.html.
- ⁴⁰ Claudia McKay (CGAP), "Ghana: Aiming for Interoperability in Branchless Banking," (June 16, 2011), available at <http://technology.cgap.org/2011/06/16/ghana-aiming-for-interoperability-in-branchless-banking/>.
- ⁴¹ Bank of Ghana, *Guidelines For Branchless Banking, Notice No. BG/GOV/SEC/2008/21* (August 2008), available at www.bog.gov.gh/index1.php?linkid=216&day=12&month=8&year=2008&fm=1.
- ⁴² *Ibid.*
- ⁴³ MTN, "MTN Mobile Money and UT Bank pay first Insurance Premium in three days," (July 2011), available at www.mtn.com.gh/NewsArtDetails.aspx?AID=169&ID=0&CID=40&MID=11&FirstParentID=1.
- ⁴⁴ *Ibid.*
- ⁴⁵ USAID, "FS Series #11: Innovations in Financial Services Delivery – Branchless Banking," (June 2010), available at http://egateg.usaidallnet.gov/sites/default/files/FS%20Series_Branchless%20Banking_Final_0.pdf.
- ⁴⁶ *Ibid.*
- ⁴⁷ Federal Reserve Bank of San Francisco, "Mobile Banking in Asia," (November 2010), available at www.frbsf.org/publications/banking/asiafocus/2010/november_asia_focus.pdf.

- 48 Telco 2.0, "Oi Paggo: A disruptive Brasileiro credit play," (June 2008), available at www.telco2.net/blog/2008/06/oi_paggo_a_disruptive_brasilei.html.
- 49 Mark Flaming, Claudia McKay, and Mark Pickens, "Agent Management Toolkit: Building a Viable Network of Branchless Banking Agents," (2011) at 71, available at http://mmublog.org/wp-content/files_mf/agentmanagement_tg.pdf.
- 50 Federal Reserve Bank of San Francisco, "Mobile Banking in Asia," (November 2010), available at www.frbsf.org/publications/banking/asiafocus/2010/november_asia_focus.pdf.
- 51 *Ibid.*
- 52 *Ibid.*
- 53 Timothy R. Lyman, Mark Pickens, and David Porteous, "Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance," CGAP Focus Note No. 43 (January 2008), available at www.cgap.org/gm/document-1.9.2583/FN43.pdf.
- 54 Bank-based services are also permitted in the Philippines, as exemplified by SMART Communications' SMART Money service.
- 55 Timothy R. Lyman, Mark Pickens, and David Porteous, "Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance," CGAP Focus Note No. 43 (January 2008), available at www.cgap.org/gm/document-1.9.2583/FN43.pdf.
- 56 Mark Flaming, Claudia McKay, and Mark Pickens (CGAP), "Agent Management Toolkit: Building a Viable Network of Branchless Banking Agents," (2011) at 71, available at http://mmublog.org/wp-content/files_mf/agentmanagement_tg.pdf.
- 57 USAID, "FS Series #9: Enabling Mobile Money Interventions," (April 2010) at 2, available at http://egateg.usaidallnet.gov/sites/default/files/M_Banking_Primer.pdf.
- 58 OECD, *Recommendation on Principles and Good Practices for Financial Education and Awareness* (July 2005), available at www.financial-education.org/dataoecd/7/17/35108560.pdf
- 59 Telenor Group, *Shaping our Financial Future: Socio-economic impact of mobile financial services*, (2011).
- 60 *Ibid.* Developing economies cited include Pakistan, India, Bangladesh, Serbia, and Malaysia.
- 61 World Economic Forum, *Amplifying the Impact: Examining the Intersection of Mobile Health and Mobile Finance: A discussion guide for collaborative insight presented by the World Economic Forum, in partnership with the mHealth Alliance* (2011), available at http://www3.weforum.org/docs/WEF_HE_IntersectionMobileHealthMobileFinance_Report_2011.pdf.
- 62 Telenor Group, *Shaping our Financial Future: Socio-economic impact of mobile financial services*, (2011).
- 63 Mark Pickens, David Porteous and Sarah Rotman, "Banking the Poor via G2P Payments," CGAP Focus Note No. 58 (December 2009), available at www.cgap.org/gm/document-1.9.41174/FN58.pdf.
- 64 Pro Pakistani, "Initial Details of Third Party Mobile Banking Unveiled," (April 10, 2011), available at <http://propakistani.pk/2011/04/10/initial-details-of-third-party-mobile-banking-unveiled/>
- 65 Mohammed Yaseen, "Mobile Banking – Market Dynamics for Pakistan," available at www.dryaseen.pk/m_banking_article.pdf.
- 66 Rolf H. Weber, "Regulatory Framework for Mobile Financial Services," available at www.mgovworld.org/libra/mbanking/papers/regulatory-framework-for-mobile-financial-services.pdf.
- 67 M-PESA, "Amendment Deed to the Declaration of Trust in favour of all M-PESA Account Holders of Safaricom Ltd.," (June 19, 2008), available at www.safaricom.co.ke/fileadmin/M-PESA/Documents/Deed_of_Amendment_to_Declaration_of_Trust_-_MPesa_Account_Holders.pdf.
- 68 Due diligence required of banks in which they must verify the identity of a potential customer and obtain other information that is relevant to the conduct of a banking or financial relationship.
- 69 Minister of Finance, "Exemption 17 to Financial Intelligence Centre Act of 2001," (2004).

- 70 South African Reserve Bank, "Guidance Note 6/2008 issued in terms of Section 6(5) of the Banks Act, 1990: Cell-phone banking," available at www.cgap.org/gm/document-1.1.6005/SARB%20Guidance%20Note%206%20of%20on%202008%20Cell-Phone%20Banking.pdf.
- 71 Superintendencia de Bancos y Seguros del Ecuador, *Resolución No. JB-2011-1919* (April 19, 2011), available at www.superban.gov.ec/medios/PORTALDOCS/downloads/normativa/2011/resol_JB-2011-1919.pdf
- 72 Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, *SBS Resolution 2108-2011*, available at <http://intranet1.sbs.gob.pe/IDXALL/FINANCIERO/DOC/RESOLUCION/PDF/2108-2011.R.PDF>
- 73 David Porteous, "The Enabling Environment for Mobile Banking in Africa," (May 2006) at 35, available at www.cab.org.in/ICTPortal/Lists/Knowledge%20Bank/Attachments/14/Enabling%20Environment%20for%20M-banking%20-%20Porteous_16_12_200749.pdf.
- 74 Michael Klein and Colin Mayer, "Mobile Banking and Financial Inclusion," World Bank Policy Research Working Paper (May 2011), available at www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2011/05/18/000158349_20110518143113/Rendered/PDF/WPS5664.pdf.
- 75 Rolf H. Weber, "Regulatory Framework for Mobile Financial Services," available at www.mgovworld.org/libra/mbanking/papers/regulatory-framework-for-mobile-financial-services.pdf.
- 76 Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, *Resolución SBS No. 775-2008* (March 26, 2008), available at <http://intranet1.sbs.gob.pe/IDXALL/FINANCIERO/DOC/RESOLUCION/PDF/0775-2008.R.PDF>.
- 77 Bankable Frontier Associates, "How Enabling is the Latin American Environment for Mobile Money?," Briefing Note No. 1 (August 2009), available at www.bankablefrontier.com/assets/pdfs/la-mobile-money.pdf.
- 78 *Ibid.*
- 79 LIRNEasia and UP-NCPAG, "Mobile banking, mobile money and telecommunication regulations," (2008) available at http://lirneasia.net/wp-content/uploads/2008/05/Mobile-2.0_Final_Hor_EA.pdf.
- 80 Michael Klein and Colin Mayer, "Mobile Banking and Financial Inclusion," World Bank Policy Research Working Paper (May 2011) at 21, available at www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2011/05/18/000158349_20110518143113/Rendered/PDF/WPS5664.pdf.
- 81 EMVCo, "About EMVCo," available at www.emvco.com/about_emvco.aspx.
- 82 GSM Association, "MMT: Catalysing the Mobile Money Market," (2007) at 13, available at www.mobilemoneylive.org/go/download/?file=93dd87a0.pdf.
- 83 *Op cit*, at 18.
- 84 Migration Policy Institute, "The Global Remittances Guide," available at www.migrationinformation.org/datahub/remittances.cfm.
- 85 These amounts capture remittances sent via formal channels, but the total amount of international remittances, including those executed via informal channels, is likely significantly higher.
- 86 Western Union, "Send Money to a Mobile Phone," available at <https://wumt.westernunion.com/WUCOMWEB/staticMid.do?method=load&pagename=serviceMobile&countryCode=US&languageCode=en>.
- 87 Western Union, "Mobile money transfer fact sheet," available at http://corporate.westernunion.com/news_media_MobileMoney.html.
- 88 Subsequently rebranded as Airtel Money in Africa following Bharti Airtel's purchase of Zain's African operations.
- 89 Zain, "Zain dials up mobile banking in Africa with Zap," (February 16, 2009), available at www.zain.com/muse/obj/lang.default/portal.view/content/Media%20centre/Press%20releases/ZapLaunchAfrica.

- ⁹⁰ Paul Leishman, "A Closer look at 'ZAP' in East Africa," GSMA case study (May 2010), available at http://mmublog.org/wp-content/files_mf/zaineastafrica.pdf.
- ⁹¹ Zain, "Africa abolishes roaming as Zain's One Network expands," available at www.zain.com/muse/obj/lang.default/portal.view/content/Investor%20relations/Press%20releases/One%20Network%2012%20countries.
- ⁹² Zain, "Zain dials up mobile banking in Africa with Zap," (February 16, 2009), available at www.zain.com/muse/obj/lang.default/portal.view/content/Media%20centre/Press%20releases/ZapLaunchAfrica.
- ⁹³ Bharti Airtel and Ecobank, "Ecobank and Bharti Airtel join forces to promote mobile banking across Africa," (June 6, 2011), available at www.ecobank.com/upload/20110609041755906868zvH34uvF8M.pdf.
- ⁹⁴ Easypaisa, "easypaisa Mobile Account: FAQs," available at <http://www.easypaisa.com.pk/mobile-faqs.php>.
- ⁹⁵ Mark Williams, "Broadband in Africa: Where are we and where are we going?" (January 27, 2010) at 4, available at <http://siteresources.worldbank.org/EXT/DEVELOPMENT/Resources/Williams.pdf>.
- ⁹⁶ *infoDev*/ITU ICT Regulation Toolkit, "7.1.5 Tariff Regulation," available at www.ictregulationtoolkit.org/en/Section.2060.html.
- ⁹⁷ Bankable Frontier Associates, "The enabling environment for mobile banking in Africa," report for DFID (2006), available at www.infodev.org/en/Document.76.aspx.
- ⁹⁸ James Bilodeau, William Hoffman and Sjoerd Nikkelen, "The Seven Pillars of Mobile Financial Services Development," *The Mobile Financial Services Development Report 2011* (2011), available at http://www3.weforum.org/docs/WEF_MFSD_Report_2011.pdf.
- ⁹⁹ GSMA, "Regulatory Framework for Mobile Money Transfers," (2007) at 18, available at www.mobilemoneyexchange.org/Files/8e31752b.
- ¹⁰⁰ Benin, Burkina Faso, Cote d'Ivoire, Guinea Bissau, Mali, Niger, Senegal and Togo.
- ¹⁰¹ Michael Tarazi and Paul Breloff, "Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds," CGAP Focus Note No. 63 (July 2010), available at www.cgap.org/gm/document-1.9.45715/FN_63_Rev.pdf.
- ¹⁰² *Ibid.*
- ¹⁰³ Federal Deposit Insurance Corporation, "Stored Value Cards and Other Nontraditional Access Mechanisms, New General Counsel's Opinion No. 8." Financial Institution Letter FIL-129-2008 (2008).
- ¹⁰⁴ Tilman Ehrbeck and Michael Tarazi, "Putting the Banking in Branchless Banking: The Case for Interest-Bearing and Insured E-Money Savings Accounts," *The Mobile Financial Services Development Report 2011* (2011), available at http://www3.weforum.org/docs/WEF_MFSD_Report_2011.pdf.
- ¹⁰⁵ Deloitte and GSM Association, "Global Mobile Tax Review 2006-2007," at 4, available at www.gsmworld.com/documents/tax_review_06_07.pdf.
- ¹⁰⁶ LIRNEasia and UP-NCPAG, "Mobile banking, mobile money and telecommunication regulations," available at http://lirneasia.net/wp-content/uploads/2008/05/Mobile-2.0_Final_Hor_EA.pdf.
- ¹⁰⁷ Timothy R. Lyman, Mark Pickens, and David Porteous, Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance, CGAP Focus Note No. 43 (January 2008) at: www.cgap.org/gm/document-1.9.2583/FN43.pdf
- ¹⁰⁸ CGAP, "Building a Viable Network of Branchless Banking Agents," Agent Training package, available at www.cgap.org/gm/document-1.9.51330/CGAP_Building_Viable_Network_of_Agents%20Training_Package_Final.pptx.
- ¹⁰⁹ Wizzit, www.wizzit.co.za.
- ¹¹⁰ "Wizz Kids and cellphone banking," (September 2005), available at www.wizzit.co.za/media/wizzkids.pdf.
- ¹¹¹ *Ibid.*

- ¹¹² Banking Council of South Africa, “Code of Banking Practice,” available at www.banking.org.za/consumer_info/code_of_banking/Code%20of%20Banking%20Practice.pdf.
- ¹¹³ Timothy R. Lyman, Mark Pickens, and David Porteous, Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance, CGAP Focus Note No. 43 (January 2008) at: www.cgap.org/gm/document-1.9.2583/FN43.pdf
- ¹¹⁴ Best Practices for Mobile Device Banking Security, ATM Industry Association, www.atmia.com/ClassLibrary/Page/Information/DataInstances/1556/Files/773/Mobile_Phone_Banking_Best_Practices_Executive_Summary.pdf.
- ¹¹⁵ USAID, “Mobile Banking – The Key to Building Credit History for the Poor?” (April 2009), available at www.microlinks.org/file_download.php/Mobile+Banking_Key+to+Building+Credit+History.pdf?URL_ID=38595&filename=12428526631Mobile_Banking_Key_to_Building_Credit_History.pdf&filetype=application%2Fpdf&filesize=284537&name=Mobile+Banking_Key+to+Building+Credit+History.pdf&location=user-S/.
- ¹¹⁶ The SIM Application Toolkit is a standard for enabling value-added services using SIM Toolkit-enabled handsets and compatible SIM cards. SIM Application Toolkit enables the SIM card to drive the handset interface, build up an interactive exchange between a network application and the end user and access or control access to the network. Originally defined by the GSM 11.14 standard, the SIM Application Toolkit standard is now contained in 3GPP 31.111.
- ¹¹⁷ Bank for International Settlements, “Risk Management Principles for Electronic Banking,” (July 2003), available at www.bis.org/publ/bcbs98.pdf.
- ¹¹⁸ Bankable Frontier Associates, “Managing the Risk of Mobile Banking Technologies,” (March 2008) at 71, available at www.oecd.org/dataoecd/32/55/41837245.pdf.
- ¹¹⁹ Kenya Communications (Amendment) Act, No.1 of 2009, Part VIA, available at www.communication.go.ke/Documents/media.pdf.
- ¹²⁰ Mark Flaming, Claudia McKay, and Mark Pickens (CGAP), “Agent Management Toolkit: Building a Viable Network of Branchless Banking Agents,” (2011) at 71, available at http://mmublog.org/wp-content/files_mf/agentmanagement_tg.pdf.
- ¹²¹ Country examples are not intended to represent an exhaustive list of governments or regulators that have addressed a specific issue.