CGAP

FOCUS NOTE

No. 48
June 2008

Ignacio Mas and
Kabir Kumar

Banking on Mobiles: Why, How, for Whom?

If you are a small bank thinking about doing mobile banking,[1] then you are where Abbas Ali Sikander, the group executive director of Tameer Microfinance Bank in Pakistan, was a year ago. He wondered then: "How does Tameer get to market rapidly without the burden of physical infrastructure investments, especially in rural areas?"[2]

Branchless banking looked attractive, and mobile phones could help. With subscription numbers at over 50 million, mobile phones were already reaching rural Pakistanis who have no formal banking access. But which rural mobile phone users should he target? And how can he use mobile phones as a channel and as a service? Abbas knew that, without a clear strategic direction, he easily could get swept away by mobile phone operators who were already well-known retail brands. An even larger issue confronting him was developing an agent network, especially in rural areas, for customers to get access to cash in their accounts.

With a few exceptions, the road to implementing mobile banking is littered with discontinued mobile banking projects, failed new technology vendors, and shelved deployment plans. For customers, mobile banking presents a delicate balance between a conceptually powerful opportunity (being able to transact any time, anywhere) and practical challenges (finicky menu sequences on a small screen and tiny buttons). Many banks launched into mobile banking without a well-articulated idea of what customers' problems were and how to address those problems.

Ivatury and Mas (2008) predicted that poor people are more likely than rich people to use mobile phones to undertake financial transactions. People in developing countries have less options (if any) for transferring money and accessing banking services, because there is less deployed formal banking infrastructure—fewer branches, automated teller machines (ATMs) generally co-located to relieve branches, and low Internet penetration. So a branchless banking channel using mobile phones could be far more preferable to poor people than the available options: traveling to and queuing at distant branches or saving in cash or physical assets.

This paper examines how banks can translate the potential of mobile phones into greater financial access for poor people. Although mobile phone operators have been able to use the mobile phone for mobile remittance and bill payment services in several countries, banks have had little success in using mobile phones as part of a growth or outreach strategy.

For customers, mobile banking presents a delicate balance between a conceptually powerful opportunity (being able to transact any time, anywhere) and practical challenges (finicky menu sequences on a small screen and tiny buttons).

This paper focuses on smaller banks or microfinance institutions (MFIs) that face a much higher cost-of-service delivery because of the smaller transaction values they handle and the likely more remote and dispersed location of at least some of their customers. The opportunity seems particularly great for them, but implementation challenges also loom larger because of their small scale. This discussion assumes these banks and MFIs have adequate back office and transaction switching capability and sufficient internal controls, whether managed in-house or outsourced. Without that, mobile banking is not possible because it is fundamentally a front end to a financial institution's information technology system.

We do not offer a single, generally applicable solution because there are many mobile banking solutions. The journey to success starts with identifying the fit of mobile banking within the bank's overall customer strategy. Beyond that, we offer some "lessons for the road" for banks.

1 Throughout this paper we use the term "bank" to refer to any type of authorized deposit-taking institution and, hence, would generally include some forms of nonbanks, NGOs, cooperatives, and MFIs. We also use the term "mobile banking" broadly to refer to any kind of payment or transaction undertaken using a mobile phone against a bank account that is accessible directly from the user's mobile phone.

2 CGAP is supporting Tameer Microfinance Bank in its implementation of branchless banking.

First, financial institutions need to bring operators to the negotiating table if they want a customer-friendly, fast, and secure mobile banking experience—it's a lot harder to construct the service without the active involvement of the operator. Operators control a key element of the security infrastructure, which is embedded within the phone. The service needs to work under precarious conditions (people using low-end handsets in areas with unreliable wireless connectivity), making the correct technology choices critical. In fact, customer experience is determined directly by the technology platform used. So finding the right technology partner and optimizing the operator's resources is critical. This gives mobile phone operators substantial leverage when negotiating with banks.

Second, customers are more likely to take up the service if they can easily get their hands on cash. Banks need to find a way to provide liquidity through a network of cash-in/cash-out agents. Here again mobile phone operators have an advantage: their network of mass-market prepaid card retailers, which can do double duty as cash agents.

Third, if mobile phones are used to drive customer outreach and mass-market growth rather than to enrich the service experience for existing customers, banks need to develop a highly efficient channel to drive awareness of the service and strong branding to overcome natural customer resistance to new technologies and the associated security fears. Many banks—and not only the smaller ones—choose to rely on mobile phone operators to promote and even brand the mobile banking service given the operators' credibility with and understanding of mass-market marketing techniques.

Once a small bank or MFI considers all of this, the biggest uncertainty remains how to take its customers from their early experimentation with the service to a point where they truly can understand the value it can bring them and they can feel comfortable operating it. There is a large customer adoption barrier—and it's upfront.

Pinpointing the strategic value of mobile banking

Abbas discovered that pinpointing the precise role mobile banking can play within a bank's strategy is not straightforward. The issues are not complex, but they are highly interrelated. Therefore, in our discussion, we first identify what it is about a mobile phone—the device itself—that can make it a potentially useful tool for banks as an access device compared to other electronic banking interfaces. Is it because we can carry it with us? Is it because its architecture offers special security or usability benefits? Or is it simply because it is a widely available Internet or point-of-sale (POS) terminal where there are few alternatives?

Second, we map "inherent" benefits of the mobile phone to four typical strategic drivers for banks: increase penetration, sell more services, retain the most valuable customers, and reduce the cost of providing services.

Third, we build on the first two to develop a set of mobile banking cases or prototypical strategies banks may use.

The second part of this paper leads banks and MFIs through the implementation choices available. In the markets we are primarily concerned with, where most people are using basic handsets,[3] wireless connectivity coverage is limited (see Table 1), the mobile market is less competitive because it has fewer players (e.g., Safaricom has 70 percent market share in Kenya), and there are simply less technological options, the wrong technology choice can easily jeopardize the success of the banking service.

3 A large share of low-income customers in many Asian markets use Nokia 1100 series phones. See http://en.wikipedia.org/wiki/Nokia_1101.

Table 1. Wireless penetration rates for developing regions

	Wireless Penetration Rates (%)		
	2003 (Q1)	2008 (Q1)	2012 (Q1)
Africa	4.75	30.60	50.13
Asia Pacific	13.06	39.08	60.81
Eastern Europe	20.50	102.79	134.72
Latin America/Caribbean	19.74	70.40	90.84
Middle East	17.84	61.91	98.26

Source: Wireless Intelligence at www.wirelessintelligence.com.

Imagining the customer experience

Before getting into the why and how of mobile banking, let's look at what the customer may experience with mobile banking. To open a bank account, the customer goes to a bank branch or an agent accredited by the bank where she is properly identified as required by law. She fills out a form, where she supplies her name, address, and mobile phone number, and she presents an acceptable form of identification. Or, if she already has a bank account, she can register for mobile banking through a mobile phone by sending a text message to a particular number.

Once the account is opened, the bank transmits the mobile banking application wirelessly to the customer's phone. Now the customer registers her phone number and selects her personal identification number (PIN). She finds the mobile banking application, which will appear on the main menu of her phone. Let's say it is under Tools as My Banking.

Once she launches the application, she will be asked to pick and type in a PIN. She can now begin transacting. She will be able to receive her salary, remittances, and other transfers into this account, and she will be able to make payments (e.g., pay utility bills). See Figure 1.

Figure 1. Example of what a customer sees on her phone in a cash withdrawal: The case of M-PESA in Kenya



The customer will need to add or take cash out of her account in person from time to time. Let's say she wants to withdraw cash at a corner store that is acting as an agent for her bank. The customer launches the application from the phone's menu, puts in her PIN, and selects Withdraw from the menu. She will be prompted to select the account from which she wants to withdraw, enter the amount, and then enter the phone number of the store clerk.

The next screen will prompt the customer to confirm the transaction by selecting OK or retyping her PIN. Both the customer and the store owner will get a message confirming that the customer's account is debited and the amount is transferred to the store owner's account. At this point, the store owner hands over the cash.

The first time customers use this service, the process may seem confusing and even protracted. But customers become familiar with the process quickly and appreciate the convenience of not having to carry a separate bank card, and especially being able to transact from anywhere to anyone with a mobile phone—not just to get cash at the store.

Back to basics: What is the "it" in mobile banking?

What contribution can mobile phones make to banking? We examine this by formulating hypotheses on how mobile phones can change the relationship between a bank and its customers.

1. Mobile phone = a ubiquitously *deployed* base of technology?

Under this hypothesis, the potential of the mobile phone, the "clever trick" we might seek to exploit, lies not so much in its inherent capabilities or how customers relate to it, but in the fact that it is (practically) everywhere. This is why we claim that mobile banking offers more opportunity to poor people—who have less alternatives—than rich people. Its power is in transforming the economics of service delivery and less in the nature of the service proposition itself. Consider four specific devices mobile phones could replace:

1a. Mobile phone = a virtual bank card. A bank card is essentially a memory device in the client's possession that serves two purposes: it identifies the user, and it identifies the account (and institution) where the user's financial balances are held. The mobile phone could be used to securely store this information, thereby avoiding the costly exercise of having to distribute cards to the entire banked population. In fact, the subscriber identity module (SIM) card inside GSM phones is in itself a smartcard (i.e., a card with a chip, similar to the more modern bank cards), although it is not encased in the usual plastic form factor. The bank customer's PIN and account number can be recorded on this SIM card or on the phone's memory acting as a virtual card.

1b. Mobile phone = a POS terminal. A mobile phone can be used to initiate transaction requests and communicate with the appropriate bank to solicit transaction authorization. This is the function of a POS terminal at a retail store: it has a screen and data entry keyboard to capture the user's transaction details, a card reader to capture stored client information (to confirm his identity and locate his account), and a secure communications link with a bank. A mobile phone can replicate this functionality. If the client is using a virtual card on his phone, the mobile phone-as-POS will be able to read it directly; otherwise, a card reader will need to be attached to the mobile phone.

1c. **Mobile phone = a human ATM.** A POS is used to pay for goods at the store. If we consider cash and access to your savings as "the good" that customers fetch at the store, then that POS (plus the store's till) serves the cash collection and distribution function of an automatic teller machine (ATM). Mobile phones can provide that POS-as-ATM functionality.

1d. **Mobile phone = an Internet banking terminal.** Internet banking is based on two fundamental customer value drivers: control (instant access to any account detail I need) and convenience (ability to make payments and transfers remotely). It has demonstrated its usefulness, to such an extent that it is now in the channel arsenal of practically all major banks. But its use is limited in many countries by the poor reach of the Internet itself. The mobile phone device and wireless connectivity bring the Internet terminal into the hands of customers.

Leveraging the deployed base of mobile phones has to translate into some cost savings, but how much? Excluding costs associated with connection to the payment system and to switch transactions that they need to incur whether they use branches or mobile phones, we expect to see in at least one case the costs decline from approximately US$70,000 for a branch to US$1,140 for agents using cell phones.

2. Mobile phone = a new way for customers to interact with technology?

The technology elements embodied in a phone may not be new, but what is new may be the way customers relate to the technology. Mobile phones are personal devices. The value of the device is so high for some of us that we even decorate and personalize it like we do our cars or homes. One study indicated that mobile phone users were not without their phones for more than 30 minutes. The device gives us a sense of *immediacy*. It's not so much about anytime/anywhere, it's about here and now. It gives us a feeling of possibility, convenience, and control.

Beyond the cost saving of using an existing deployed base of terminals, how can banks exploit this sense of immediacy to develop a deeper and more meaningful relationship with a customer who happens to have a mobile phone? How can these attributes of the relationship between customers and their mobile phone be used to create new banking services or service models?

At the very least, mobile phones provide banks the opportunity to send personalized messages to all their customers—messages that serve to market a new product, introduce a new feature to a service, or alert on specific account activity. Customers could immediately verify account balances and recent account activity when needed. Moreover, because it allows for two-way interaction, the phone also makes it possible for customers to take immediate action from wherever they are, for instance when they are reaching a low-balance threshold or when there is unusual activity on their account so customers themselves can be part of fraud prevention.

This enhances customers' sense of control. Interactivity can go further into tailoring services as the relationship between banks and their customers matures. For instance, customers could request a higher credit ceiling on the fly, when needed, with verification happening over the phone. In any case, it is probably fair to say that we have only begun to imagine the possibilities of exploiting the mobile phone in creating new service experiences.

3. Mobile phone = a useful *new* functionality?

Is there an inherent capability "inside" the mobile phone that really is new, that allows customers to do something that they simply couldn't easily do before?

A mobile phone can be used to enter, display, process, store, and transmit information—but so can computers, ATMs, and POS devices, which are the electronic network end-points banks use today to service customers. In fact, mobile phones are more limited than these devices, for instance in terms of processing power. There is really not much that is *functionally* new in a mobile phone as a terminal device: after all, no one was thinking of banking applications when mobile phone standards were being defined.

However there is a characteristic of the mobile phone's architecture that sets it apart from most other computing devices that could be used for banking purposes. This is the existence of a device within a device, or a SIM card inside the mobile phone.[4] Neither of the two devices is functionally new: the SIM card is a smartcard (a card with a chip) and the mobile phone is a limited computer. But having one inside the other enables interesting security features.

The SIM's memory contains two essential elements: the phone's user menu and the security keys that are used to encrypt all information the phone sends to and receives from the network. The memory in the SIM is tightly controlled by the mobile operator; no other party, not even the customer, can access it or store applications without the explicit authorization of the mobile operator. Therefore, the contents of the SIM are much more tamperproof than the rest of the phone or any standard computer. The downside is that the closed architecture of the SIM limits service innovation by third parties. Combining the tight security of the SIM with the more open architecture of the phone itself allows mobile phones to attain the best of two worlds: a secure kernel within a flexible, service innovation-friendly shell.

The mobile phone is also a connected device with a particularity: it can attach itself anywhere on the network, automatically. There is one intrinsic feature of a mobile phone that has so far not been used much in mobile banking applications: location awareness. The mobile phone can be spotted in most mobile networks within a couple dozen kilometers or tens of meters (i.e., either single-cell or with more sophisticated multi-cell triangulation technologies). One interesting idea tested by Bankinter in Spain is using the location of the credit card at point of transaction relative to the cardholder's mobile phone (which is presumed to be on or near the cardholder). If they are far apart, there can be more reason to question the authenticity of the requested transaction.

Summary: The power of economics vs. customer experience

A mobile phone is, and always will be, more limited in its capabilities than either a connected personal computer or a specialized POS. But it has economics on its side. For instance, the high cost of the required dedicated broadband infrastructure and the devices themselves will hinder the spread of Internet banking in developing countries. In rural areas it is further hindered by a vicious circle: low device penetration does not warrant roll-out of appropriate broadband communications infrastructure, and while the infrastructure is not in place few customers will invest in personal computers.

But, if we exploit the built-in data-handling capabilities of mobile phones, it turns out that the job of deploying "Internet machines" in developing countries and rural areas is substantially done or under way. By "free riding" on the strong economics of the mobile voice service, business cases have been closed and vicious circles have been broken.

But make no mistake: the mobile phone offers a substandard user experience, at least for users unaccustomed to the service. It's great to be able to

4 Throughout this paper the case of mobile phones is considered using the more prevalent GSM standard. Some networks use other standards (CDMA, iDEN) that may not use a SIM card.

use devices that people already own, and it's great that mobile phones give people an opportunity to feel more in control over their financial services. But driving customer adoption will not be straightforward if they are intimidated when they first hear about it and scared off the first time they experience it. This presents a key trade-off: mobile banking reduces the cost of service delivery but may create a larger adoption hurdle.

What about cash?

Mobile phones are ingenious devices, but one thing they cannot do by themselves is convert cash into electronic value or dispense cash. They can be used only to transfer or transform value electronically. A mobile banking platform therefore needs to be supported with a cash conversion platform—whether full-blown bank branches, ATM terminals, or third-party banking agents. Remember, the whole mobile proposition is based on *choice* and *control:* if I don't have a choice of cashing in or out of my electronic wallet, I am not likely to think mobile banking is doing much for me.

A bank that wants to cover a new geography with a mobile banking strategy will need a cash-in/cash-out network in that same geography. The mobile platform will not "liberate it" from having to figure out a physical cash delivery channel: it's clicks *and* mortar. But it can be "clicks and mortar lite," because the mobile banking platform itself can help in deploying that network cost-effectively by letting, for instance, an agents' mobile phone act as a POS for handling agent transactions.[5]

To what extent will mobile payments replace the need for cash? To answer that question we need to understand the relationship between electronic money that may be accessible through mobile phones and cash. There are two key roles of money: as store of value and as means of payment or exchange.[6] In a totally cash-based economy, cash fulfills the two roles at the same time. It may be inconvenient for people to store and move so much cash around, but at least there is no risk of lack of liquidity: if you have enough value stored in cash, then you have enough cash to make a payment.

It is only when the two roles are separated that liquidity may become a problem. For instance, as people move into savings in real goods (bricks, chicken, real estate) in search of convenience and higher returns in the store-of-value function, the total amount of savings far exceeds the amount of cash easily available. Liquidity might be a problem if you are not able to convert your physical savings into cash readily enough. In that case, you might need to resort to bartering your physical assets—so you tend to choose physical stores of value that are tradable and movable (e.g., livestock). When people need to resort to barter, cash has lost both functions—as store of value and as means of exchange.

Similarly, once there is electronic money, the demand for cash depends strictly on the extent to which this new electronic form of store of value can also be a means of exchange. Can we use electronic money to directly pay for all that we need? In the language of payments, is there a wide acceptance network?

To the extent that electronic money is convenient for us to use and widely accepted, we return to a world where the same "asset" is performing both functions. Now, there is no liquidity issue with electronic money and cash loses its role. But if electronic money is not widely accepted, and we know of only a handful of places where it is accepted as a form of payment, storing my value in electronic form exposes me to liquidity risk: I cannot ensure that I can convert electronic value into cash quickly enough if and when I need to spend the value.

5 For a general description of banking agents, see Mas and Siedek (2008). Note that agents may also play a valuable role in getting customers acclimated to the mobile proposition with on-the-spot training that customers may need to pick up a new service.

6 The other function of money is the "unit of account." We don't cover the issue of alternate currencies—money used in virtual online worlds, for instance. For information on forms of alternate currencies and their economic significance, see David Birch's Digital Money Forum blog at http://www.digitalmoneyforum.com/blog.

People have heralded the end of cash before but the claims of a cashless society are more emboldened today by the growth in cell phone use globally.[7] In fact, the relationship between electronic money accessible via mobile phones and cash is likely to vary over time.

In the early stages of introduction of this electronic money, it will be essential to ensure that people have ready cash-in/cash-out options to support the mobile proposition. Customers will want to test the liquidity of electronic money. Typically they will want to convert all electronic money inflows into cash immediately and in full. In places where cards have been used with microfinance clients or low-income customers, people who live in all-cash economies, most cash out their loans, government benefits, and so forth, on the spot immediately after they receive them.

As electronic money gains acceptance as a store of value, people might restrict getting their cash out to meet their daily liquidity needs for very small value transactions only. In fact, in this stage, we expect there to be substantial net cash into the mobile banking system as it absorbs cash that had previously been performing the store-of-value function (under the mattress). Over time, because goods, services, and salaries will be paid increasingly through electronic transfers, cash conversion will become unnecessary. Direct electronic transfer will skip the electronic value-to-cash conversion on the paying side and the corresponding cash-to-electronic value on the receiving side. Now, finally, total cash substitution is happening, both as store of value and as means of exchange. Ultimately, cash-in/cash-out points may not be necessary at all.[8] But you would do well not to plan for that world as yet.

How can "it" be useful to banks?

The above discussion highlighted the key potential benefits of using mobile phones to deliver banking services: lower cost of deployment for the bank, and choice and control by the user. The potential benefits of mobile banking need to be related to banks' own strategic drivers. There are some basic core strategies banks may follow to promote and protect growth. We illustrate how mobile phones may support each strategy, with reference to the potential benefits of mobile phones discussed above. Table 2 provides a summary of the arguments. These are reinforcing, but banks may need to prioritize among these to be able to develop a coherent, focused strategy.

Increase market penetration. Go for underserved population segments, and grow the total revenue pie. Mobile banking can serve primarily to reduce the cost of deploying customer touch points into lower income or more remotely located population segments (the "deployed base" view). Mobile-as-ATMs can enable merchants to become cash-in/cash-out points; mobile-as-POS can serve to substitute cash and electronically capture transactions at the store. Mobile-as-Internet-machines can allow customers to transact remotely (sending remittances, paying bills) without having to physically access a service point.

Sell more services to existing customers. Develop new products that target *unmet needs* of existing customers. These new services could exploit the new functionality available through a mobile phone (e.g., location awareness, under the "new functionality" view) or its value as a personal technology (the "new way to interact" view). In the latter case, the mobile phone would act as a service "presentation" and delivery channel, its main utility no different than an Internet machine.

Retention of most valuable customers. Protect the roughly 20 percent of customers who bring roughly 80 percent of the value, offering them a quality and breadth of service that will make them less vulnerable to churn. Individual services are rarely unique to a bank, because they are easily replicable. Rather, the

7 For instance, see *The Economist* (2007).

8 We also don't discuss in this section cultural factors that might prevent people from using cash even when there is a wide acceptance network. The authors of this report have observed among colleagues in the same office that despite almost complete acceptance of cards as payment devices where we live and have our offices in Washington, D.C., colleagues still continue to carry a fair amount of cash.

Table 2. Mapping the main benefits derived from using mobile phones to banks' strategic drivers

Use of mobile phone	Strategic drivers for banks: Increase market penetration	Sell more services to existing customers	Retention of most valuable customers	Reduce cost of service provision
Deployed Internet terminal	Remote transactions for underserved populations	Alternate channel for customers	Unique customer experience	Use in place of PC and broadband Internet connection
Deployed POS/ virtual card	Reach underserved populations with agents			Use in place of card and POS device
Personal device		Unique customer experience	Immediate action and sense of control experience	
New inherent functionality	Use SIM functionality for "virtual" card	Use location awareness for real-time products		

important thing is to embed the nonunique services within a unique customer experience. Having an informational and transactional capability in customers' pockets (the mobile-as-Internet-machine), banks may be able to propose new services to their customers in a much more targeted way. Banks also can fully exploit the immediacy of the mobile environment to extend the benefits of control and choice, and hence convenience, across their entire product range (the "new way to interact" view).

Reduce cost of service provision. Put primary emphasis on bottom-line over top-line growth. Cutting costs is not only about margin: seeking low(est) cost position in the market also should deter competitors from engaging in value-destroying price wars, thereby protecting the revenue base. This is fundamentally about replacing more expensive channels and devices with the cheaper mobile solution (the "deployed base" view).

Putting it all together: Three mobile banking scenarios

Having looked at the building blocks—the special features of mobile phones and how they might support a bank's various strategic objectives—we now construct three different deployment scenarios, shown in Table 3. These are based on the degree to which the mobile channel is geared toward retaining existing or acquiring new customers, and in the latter case whether these new customers are obtained by expanding the market or winning them over from competitors. We offer these as archetypes to illustrate three extreme cases that, in combination, span the range of strategies a bank might pursue.

Cool value add

In this scenario, a bank seeks to exploit the personal nature of the mobile handset to build a stronger relationship with its customers. The mobile proposition is used to expand the choice of channel and services to the customer. The business case is based on customer retention; the mobile service is used to create a specific point of differentiation from other banks.

ABSA was one of the first banks in South Africa to introduce mobile banking in 2002. The fact that its customers use the mobile phone as a complementary channel is illustrated by the fact that usage volumes increase significantly during holiday seasons (like

Table 3. Three mobile banking scenarios

	Cool value add	Easy bank	Virtual bank
Strategic objectives for the provider	Retain and grow value from existing customers	Increase market share (take customers from the competition)	Increase penetration (target new-to-banking or underserved people)
Role of mobile channel	Mobile is a complementary channel, with most customers using it only for specific purposes	Mobile and other channels co-exist, but are targeted (perhaps not exclusively) to different segments	Mobile is likely the only channel for most (if not all) customers
Value proposition for customers for use of the mobile channel	Service enhancements: • Enhanced customer control over own finances (e.g., alerts and notifications) • Greater targeting of messages and services from the bank (e.g., using location awareness) • 24/7 availability of service	Convenience: • Less but more relevant services • Ubiquity of service • Simple, easy to use • Low cost	Reduced barriers to access: • Very low transactional costs • Availability of service in areas not traditionally covered by banks • Use of retail outlets rather than branches (where they may not feel welcome)

Christmas): customers on vacation choose to do banking transactions via mobile phone when they can't access the Internet or ATMs. The bank has in fact sought to integrate the Mobile and Internet channels: it has introduced SMS alerts to customers every time there is a successful log-in into the customer's Internet banking application, as a security precaution.

Easy bank

In this scenario, the bank uses the mobile phone to broaden the range of channels through which it interacts with its customers. The mobile phone offers full service capabilities: it is used not just for sending out information or messaging with customers, but also to transact. It does not seek to displace established channels for existing customers, but the breadth of channels allows the bank to address more diverse segments. Low-value transactions undertaken by poorer segments of the population are conducted via mobile phone. For them, the branch may eventually become merely a sales channel, while mobile and ATM serve as their primary transactional channels.

Recently, Equity Bank created two new channels to complement its branch, ATM, and mobile van channels: a closed-loop POS network, where customers can do basic banking transactions, and a mobile phone channel, where customers can check balances, remit funds, and do other transactions. The mobile channel is likely to be used by younger customers and migrants who send frequent small amounts of money home. Customers can cash in or out at agents, branches, ATMs, or mobile vans and can use both the mobile phone and card linked to the same basic transactional account.

Virtual bank

In this scenario, a bank seeks significant outreach and growth of customers, because of new market entry or geographic expansion or a run for scale. By using mobile banking as the main customer touch point, the bank seeks growth without investing in as much physical infrastructure. Indeed, mobile banking can be a way of limiting the risk in a growth strategy. The customer experience is likely to be less-than-perfect but customers are likely to be more tolerant because they simply do not have many alternatives. Customer experience just needs to be good enough to have broad appeal and deliver scale.

Tameer Bank in Pakistan may decide that it wants to reach rural Pakistanis mainly via cell phones and

agents. It may decide that it won't open any more branches outside the two major cities and that it will partner with companies with retail presence, including the mobile operator, to create its cash-conversion platform. Tens of millions of subscribers of one of the top three mobile operators will, within a short time, become account holders at Tameer. Those customers may rarely visit a Tameer branch, if at all, but they will still come to recognize and trust the brand of the service.

Navigating through implementation choices

So far we have discussed the commercial strategy considerations surrounding the development of a mobile banking proposition. We now turn to the main implementation decisions a bank faces. The key aspects relate to the following:

- The customer experience the bank wishes to construct
- The electronic data security framework that limits the banks' liability and protects customer privacy
- The roles and activities the bank wishes to undertake itself versus what it will outsource to partners or vendors
- The degree of service interoperability the bank wants to offer its customers (interworking with other banks, operators, bill payers, etc.)

These four aspects are intimately linked and, in some cases, directly determined by the technical platform selected by the bank.

The technical choices depend on the kinds of customers the bank wishes to reach. We therefore start with a description of the main technical options that banks need to consider. Our aim is not to provide a technical recipe book, but to provide enough understanding to illustrate, in subsequent sections, how technology choices can condition the customer experience, the bank's operational processes, the relative bargaining power between bank and mobile operator, and service interoperability.

Technical choices that define the mobile banking platform

From a technical standpoint, three critical questions need to be answered: How do you transmit data from and to the phone? How do you secure the data so that they cannot be retrieved or tampered with during transmission? How do you manage the user interactions, including the presentation and capture of data to/from the user?[9]

The first key technical decision is the wireless bearer: the communications channel that is used to transmit data to and from the mobile terminal over the air (OTA). A typical GSM phone has several channels that it uses to send and receive information: the voice channel, the SMS and USSD messaging channels, and packet data channels (see Box 1 for a more detailed description of each).

The choice of bearer channel is important because it can affect the performance of the mobile banking application in several ways:

- **Speed**—bearers differ in terms of data capacity, transmission speed, and delay in sending/receiving messages.
- **Reliability**—bearers have different characteristics in terms of how they handle congestion and whether they guarantee reception of data messages.
- **Cost**—each bearer uses different network resources and is assessed tariffs differently by the operator.
- **Security**—each bearer has an intrinsic (or native) level of security.

The second key technical decision is the way the security of the communications is managed and, in particular, what encryption standards are applied and

9 For a more detailed description of the issues discussed in this section, see Krugel (2007).

Box 1. Characteristics of the main types of wireless bearers

The voice (circuit switched) bearer. This is the bearer that is normally used when we make a call. Establishing a call requires setting up a fixed transmission path (a circuit) that "locks up" network resources for the duration of the call. A fixed amount of bandwidth is used for the call. For this reason, the voice bearer tends to be charged on a timed basis. This makes it expensive for mobile payment applications, which typically require a sequence of small bursts of data. Congestion is dealt with by not allowing new calls when there are not enough network resources, but in principle calls already in progress ("busy tone") should be able to proceed without deterioration of quality or "dropping calls." So it is reliable once you start the call, but access to a call is not guaranteed. This bearer can be used in three distinct ways: to transmit voice commands from/to the user (perhaps interpreted by the bank server using speech recognition, and created by the bank server using a speech synthesizer); to issue commands through a finite set of tones associated with the keys on the phone (as are used in Interactive Voice Response or IVR systems when you enter numerical options on a menu); and to transmit data sequences (using the phone as a modem).

Two messaging bearers. Short messaging service (SMS, popularly referred to as texting) conveys strings of up to 160 characters as a standalone message. Messages are sent on a "best efforts" basis, i.e., there is no advance reservation of network capacity. In case of network congestion, new messages can still be initiated (no "busy tone") but there is no guarantee on the speed of delivery or in fact on the eventual delivery. Indeed, SMSs may never reach their destination, and the sender has no way of confirming reception at the other end. SMSs are addressed using the normal telephone numbering system, but unlike calls they are not "dialed": in an SMS, the text and the destination phone number are combined in a message and sent together. Each SMS is treated by the network as a separate message, so charging is per message. SMS works on a store-and-forward basis, i.e., the network holds up the messages if the device is turned off or out of coverage for subsequent delivery; the SIM in the phone also can store messages received. All phones are SMS-capable, and most operators sell bulk SMS services to companies wanting to send many messages to their employees or customers.

Unstructured supplementary service data (USSD) is an alternative messaging system available on almost all GSM phones. Unlike SMS, USSD entails the prior establishment of a transmission path that remains in place for the duration of the USSD "session"—the sequence of messages being exchanged between the two parties. This transmission path does not tie up network resources while there are no messages to transmit (unlike a voice call, which is being "transmitted" whether the participants are talking or not). Like voice and unlike SMS, USSD is designed for real-time interaction, with three important implications. First, users compose USSD messages by typing standardized character sets (e.g., #123*), and this prompts a return message from the network that automatically displays on the handset's screen. Second, messages cannot be stored either on the network or on the customer's handset. Hence the phone needs to be on for the messages to be delivered and read. Third, subsequent messages and responses are linked to each other through a "session," so individual messages can be interpreted with reference to information contained in prior messages. Many operators use the USSD channel fundamentally for service management purposes and do not commercialize USSD messages, in which case use of USSD by third parties may require special agreement by the operator. When they do offer them, charging tends to be based on elapsed time of the session rather than on the number of individual messages.

Data (packet switched) bearer. This is "Internet-like" in the sense that, once the bearer connection is made, there is no need to dial to individual destinations. It is "always on," and one can access different information sources using normal URL addresses (like www.cgap.org). Like SMS, transmission is on a best-efforts basis, with all messages "competing" for network resources. The data bearer can be of various maximum speeds: GPRS (2.5G), EDGE (2.75G), or WCDMA (3G).[a] This service allows customers to view Web sites and to download data and applications from them. Smaller phones use a browser called WAP, which implements a cut-down version of HTML, the general mark-up language with which Web sites are built. Hence, normal phones can access only purpose-built, WAP-enabled Web sites. However, more sophisticated phones have a full HTML browser and can display any Web site. Charging is usually capacity-based (per kilobyte of data uploaded or downloaded), although some operators have time-based tariffing. To avail themselves of these bearer services, customers must have *(i)* a data service subscription with the operator, which may or may not be included in their basic tariff plan, and *(ii)* their phone configured with the network address of the operator's gateway server (which not all operators do as a default, and which is not easy for customers to do on their own).

[a] The "G" refers to the generation of the technology. "2G" is the standard digital GSM technology ("1G" were the analog systems, which have now been largely phased out). All of the other bearer technologies listed refer to the standard evolution of GSM.

Box 2. Main data security approaches

Bearer-only encryption. GSM networks encrypt all data going OTA. It is an extremely secure form of encryption because the software encryption keys—the keys that open and close software locks—are embedded in the SIM's hardware. They are extremely hard to get at and tamper with. However, the data are decrypted within the operator's domain before flowing through its core network, where it may or may not be re-encrypted. Hence, there is a potential security vulnerability within the operator's network. A bank relying on bearer encryption would have to trust the operator (and, moreover, its employees) not to be reading messages.

End-to-end encryption. The bank can insist on end-to-end encryption (i.e., encrypting messages from the phone all the way to its servers, on top of bearer encryption). This requires holding software encryption keys at the two end-points: on the phone and at the bank server.

Within the handset, software-based keys can be embedded in the memory in either the SIM card or the phone itself. The SIM is much more secure, as described above—only the operator has access to the SIM memory and processor, hence it is much more difficult for any malicious software to find its way into the SIM.

However, for the same reason, encryption keys can be put into the SIM only with the active support of the operator. Encryption keys can be placed on the phone without the active involvement of the operator, because they can be delivered over (say) the standard GPRS bearer. However, the bank would need to protect against spoofing—imposters purporting to be the bank placing their own keys in the customer's handset. SIMs are generally preloaded with encryption keys by their manufacturer, but that need not be the case.

Terminal security. It should be noted that end-to-end encryption offers data security only between the two encryption points. There are potential vulnerabilities if the mobile phone itself is not secure. Native SMS services, for instance, although secure while in transit OTA, are not secure while they are stored on the handset in clear view: messages can be read off stolen handsets. A more insidious attack would be if malicious software is installed on the phone that reads keystrokes or intercepts data being sent to the screen for display to the user. As phones get more sophisticated (more memory, more processing power, more attachable peripheral devices), the threat from such potential attacks will get more significant.

by whom. Adequately protecting the data on the transmission channel is essential both to provide for the necessary customer trust and to limit the potential liability to the bank.

One approach is to use the encryption that is inherent with the wireless bearer (native encryption—see Box 2). This does, however, require trusting the mobile operator, because the data communication will be de-encrypted and re-encrypted as it is moved from the wireless bearer (over the air, or OTA) to the core network and then on to the bank. Alternatively, mobile applications can adopt an end-to-end encryption model, in which case the security is provided seamlessly from the customer's mobile phone all the way to the bank's server, irrespective of the bearer used. In this case, it is the bank that is putting the "lock" on the data, and the mobile operator (or any other party) cannot gain access to it.

The third key technical decision, the application environment (Box 3), is the software platform that controls how the service is presented to the user's handset and the interactions between the user and the bank's server. This can be driven from an application either in the mobile handset or in a central server. The choice of application environment can affect service usability and performance for mobile applications in several ways:

- **User interface—**the richness, intuitiveness, and customer familiarity with the user interface
- **Speed of service—**the time it takes for data to be downloaded and for menus to be refreshed (based on whether the data sit locally or need to be transmitted over the network)
- **Ease of set up—**how easily the service can be installed for new users, and whether it works universally on all mobile phones or needs adaptation

Box 3. Main application environment choices

Client based—where an application downloaded on the phone takes control of the service. For instance, the application may present a specific menu and may guide the interactions between user and bank server in a user-friendly way. It is likely to seem to work faster for two reasons: *(i)* the menu is resident on the handset and does not need to be served OTA each time it is called, and *(ii)* the application can process information before sending it so as to optimize the amount of data sent and received OTA.

The application can be resident on the SIM (using the SIM Toolkit [STK] programming environment),[a] in which case the menu can be inserted right into the phone's main menu (i.e., "My bank" will appear as one more item or icon). Or it can be resident on the phone's memory, in which case it is likely to be a Java applet.[b]

Java applets on the phone will be much more user friendly because they are less constrained by size of memory and can take full advantage of graphics. However, they are not integrated into the phone's main menu. The user has to know how to launch Java applications, which is not something many customers are familiar with. STK-based menus are much easier to find by the user, but are text-based only. In either case, the service provider needs to manage the process of installing applications on each individual phone of their user base.

Network based—where there is no specific application downloaded, and the service is presented directly in the way that it is sent from the server to the handset. In this case, the application "look and feel" is determined by the bearer, without any special user interface "packaging" it. Thus, the user interface will be the normal or "native" SMS or USSD interface or the browser (typically WAP) if using a GPRS/EDGE/WCDMA bearer. The service may seem slower because all user interactions need to be conveyed OTA from/to the network. On the other hand, the provider can control the user experience without having to worry about the edition of the client software or updating clients in the field when there are service upgrades. There also will be less device dependencies.

[a] STK requires handset support, and most but not all GSM phones in the marketplace today have this capability. There might be issues with different handset vendors' interpretation of and compliance with the STK standard.
[b] Some banks that work across both CDMA and GSM networks have considered using BREW, a content development and delivery platform that is agnostic in terms of programming language and type of device. The platform supports the development of applications in Java and other languages that reside in the phone's memory and interact with the phone's operating system.

- **Ease of upgrading**—the ease with which the service provider can upgrade the service or add new service features

Given the type of data required in mobile banking applications, generally voice is the most expensive service, followed by SMS; data-based sessions are cheapest. Network-based services tend to be more expensive than client-based services, because the former involve sending menus OTA and cannot process any information locally on the handset.

All these appear as merely technical choices. But they do condition the mobile banking service a bank can roll out in important ways.

Implications for usability

Key factors affecting usability

Beyond the specific services offered by the mobile banking platform, the technology choices made can impact the customer experience in several ways.

Ease of setup (enabling the phone for the service). Native SMS and USSD services are the easiest to implement because they work on all GSM phones. STK-based services need provisioning of the client application on the customer's SIM, which is easy for the operator to do as long as it has OTA provisioning capability and the SIMs in the market have sufficient memory and are preloaded with encryption keys.

That is easier said than done. It could take customers a while to download the application if OTA capacity is weak. Customers could be made to swap their existing SIM with one that has higher capacity or already has the application, but that could add time and cost.

Services based on WAP, and especially Java, require more advanced handsets, which would limit their applicability to a narrower market. They also require the bank's Web address to be configured on the phone (in the case of WAP) or an applet to be downloaded in the phone's memory (in the case of Java), which in principle should be possible to configure OTA. These services also require users to buy a packet-switched data subscription from their mobile operators, which many do not have as a default setting.

Ease of finding and launching the service by the user (once the phone is enabled). What happens when the customer launches the service for the first time casts a long shadow on customer experience in total and may explain why some people who sign on during a marketing campaign may not use the service moving forward.

STK-based services are the easiest for users to find because they appear prominently as a line item or icon on the phone's main menu.[10] Native SMS and USSD services do not appear on any phone menu; instead, they need to be launched by the user by sending an appropriate message. Hence, they are less intuitive. But they may be just as easy to use as long as message structures are kept simple and keywords are intuitive. Initiating USSD service is like making a phone call, which most people, even those who cannot read, would know how to do. For instance, Oxigen, a POS network operator in India, has developed a mobile wallet that people can sign on to use by typing a memorized sequence of numbers and texting it. Initiating an SMS message may not be as intuitive the first time, but most users are already familiar with that process. In contrast, most customers are not familiar with the process for launching WAP and Java applications, because use of data services is very low, and this would tend to limit their use.

Ease of navigating through the service (once it is launched). Services based on Java, WAP, and STK are more intuitive because they are inherently menu driven. Thus the user can be guided through the range of options and can be prompted to supply any necessary information. On the other hand, menus are hierarchical and may challenge people with low-levels of education or literacy.

Services based on native SMS or USSD are not menu driven. The user must remember short codes or keywords that are to be used to issue various transaction instructions; providers give chit sheets or reference guides to their customers to facilitate this. Not using menus increases the probability of error on the part of the user because there is no prompting for the right information. USSD is session-based—a customer request prompts an automatic response that is displayed directly on the phone's screen awaiting further customer input—which gives users a sense of interactivity and in fact can be used to deliver an experience very much like a menu. In comparison, SMS-based services feel rather like a disjointed set of messages, because the user must compose or retrieve a message with each interaction.

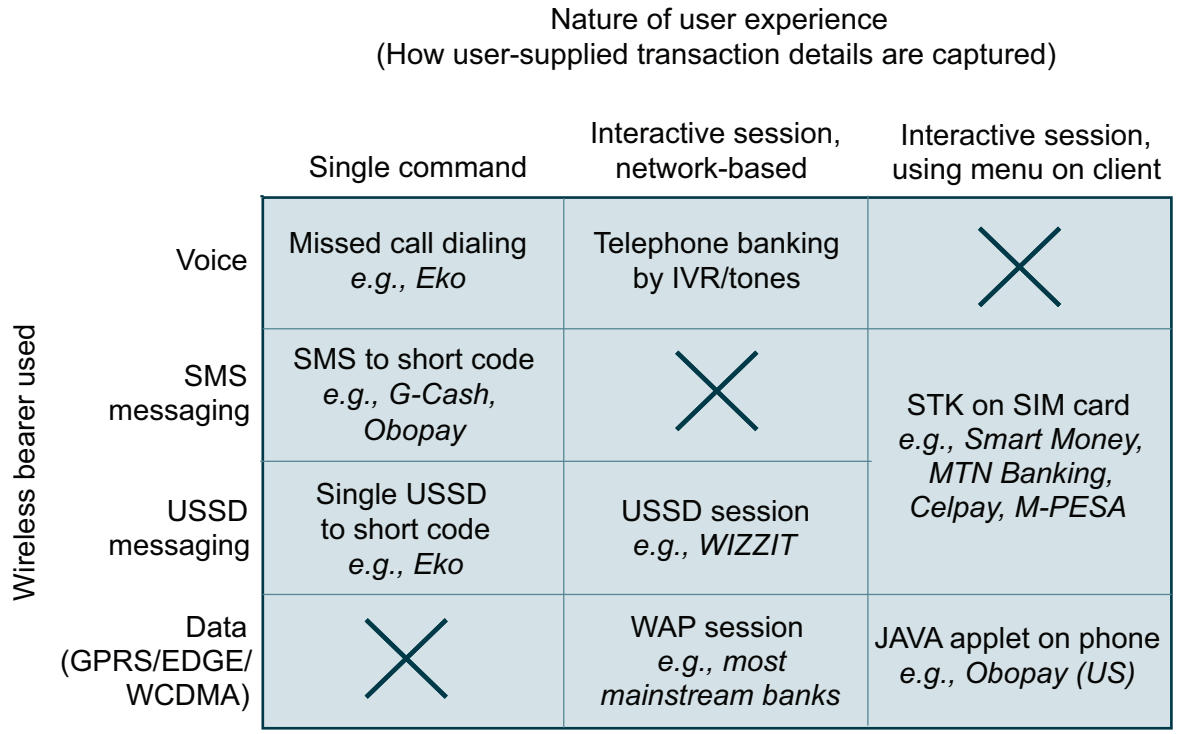
Java offers the highest quality graphical user interface, because it is the only one that can support full graphics. The menu for Java and STK resides in the handset and hence loads faster than the WAP or USSD menu, which needs to be loaded over the air each time it is accessed.

What's out there?

Figure 2 summarizes the main types of mobile banking implementations in the market today, based on how customers interact with the service (how they issue

10 However, often the services are a layer or two below under "My Applications" or equivalent other category but this could be easily fixed. These and other insights on user interfaces is drawn from CGAP's joint research from Microsoft Research Labs in India.

Figure 2. Technical choices available to banks



transaction requests and provide transaction details) and what bearer the service uses to transmit data. The customer experience can be based on the customer either issuing a single command that contains all the necessary transaction details, or engaging in a sequence of interactions through which the customer is prompted for the necessary information. In the latter case, the interactive session can be managed by an application on the user's handset that drives a menu or by a remote application controlled in the network.

STK-based applications are the most common, because they are supported by most handsets. The menu is embedded in the normal phone user interface, which makes it appear very natural, and offers a high level of security with SIM-based encryption. This method used by Smart Communications for SmartMoney in Philippines, Safaricom for M-PESA in Kenya, MTN Banking in South Africa, and Celpay in the Democratic Republic of Congo. The underlying bearer can be either SMS or USSD; because the interaction is through a client menu, the customer is not aware of which bearer is actually used.

USSD is also widely used because it is not SIM-dependent, allowing it to work across all operators. WIZZIT replicates a menu experience with a longer USSD session involving multiple messages. Rather than finding the menu on the phone, the customer calls up the service menu by dialing a USSD short code; from then on, the customer merely responds to the information requests contained in successive USSD messages. This menu-like experience cannot be replicated with SMSs alone, because SMS is intrinsically not session based.

Eko, another mobile wallet solution developed for Centurion Bank in India, uses the single-command approach by having the user dial either a voice call or a USSD message to a short code and appending transaction details as if they were supplementary dialing information.[11] In the case of a voice call, Eko captures the command sequence in the dialing instructions but will treat the call itself as a missed call—which would then make it free to the customer. G-Cash in the Philippines and Obopay in India use a similar approach, but they use SMS instead. In this case, transaction details are contained in the body of the SMS message itself, which is sent to an SMS short code. All of these approaches require the customer to be familiar with the required structure of messages and the sequence in which information needs to be supplied. Hence, they may be harder for first-time or infrequent users, although experienced users may find them highly efficient.

No major provider in developing countries bases its strategy on WAP and Java because those can target only a reduced segment of the market. However, Obopay does offer these services, in addition to its SMS-based one, in the United States. Voice-based services, whether calling a human operator at a contact center or an automated interface through an IVR, are generally too expensive for basic users.

In practice, service providers may combine a variety of these technical options to create an optimized customer experience. For instance, under MTN/Standard Banking in South Africa, the client can send a USSD message to the operator to register and is then prompted to download a SIM application to reside in the phone in the STK environment/standard phone menu.

The Annex provides a detailed description of the operation of four different mobile banking operations in place today, with a focus on the customer experience:[12]

- SmartMoney in the Philippines, which is the product of a joint venture between a bank and a mobile operator, based on STK
- G-Cash, an operator-led model based (at least initially) on native SMS
- M-PESA, an STK-based, operator-led model
- WIZZIT, a bank-based model using native USSD

Implications for operating processes around data security

Beyond the customer experience, the technology platform also will condition the operating processes that must be put in place to ensure appropriate security for banking transactions. From a security point of view, an STK-based solution would, in principle, offer the same level of security as an ATM transaction: both rely on two-factor authentication of the user, and both use the same standard of encryption for all communications.

Non-SIM-based solutions have a lower level of technical security. Poviders opting for these will need to put in place complementary processes to ensure adequate security overall. For instance, WAP-based solutions are fundamentally similar to standard Internet banking: they are both based on browsing from a Web site. Hence, a bank instituting a WAP-based solution would do well to extend its enhanced Internet security measures to the mobile banking environment. The general principle is the less secure the technology platform, the more the bank will need to institute complementary operational security measures.[13]

Implications for bank and mobile operator relationship

The technology choices also condition the relationship a bank must have with a mobile operator to create a mobile banking service:

11 For instance, the customer might dial *111*222*333*444#, where *111 is the short USSD address, 222 is the amount to be transferred, 333 is the phone number of the recipient, and 444 is the PIN of the user. A voice call would follow the same dialing instruction but omitting the leading * which is reserved for USSD in the phone addressing system. Eko uses USSD messages for customers on GSM networks, and missed calls for customers on CDMA networks (which do not have the USSD capability).

12 For useful reviews of leading mobile banking operations in developing countries, see InfoDev (2006) and Porteous (2006).

13 For more on the trade-offs between the level of encryption and the level of operational processes/controls see Bezuidenhoudt and Porteous (2008).

- STK-based applications require active support of the mobile operator, to install the menu (client program) and enable the encryption keys in the operator-controlled SIM card. The mobile operator needs to give access to the memory on the SIM card, which it controls, and needs to use its OTA platform to provision the application onto customers' SIM cards. The operator's role will be much greater if the SIM cards it issued to its customers need to be upgraded (SIM swap), which will be necessary if the encryption keys have not been preloaded or they have insufficient memory.
- Mobile banking services based on USSD may require the mobile operator's support if the operator does not have an existing commercial offer on USSD. In particular, the operator needs to allow access to its USSD server to send and receive messages to/from customers' mobile phones.
- Mobile banking services based on native SMS, WAP, or Java do not require operator support and can even be offered to customers without the knowledge of the operator.

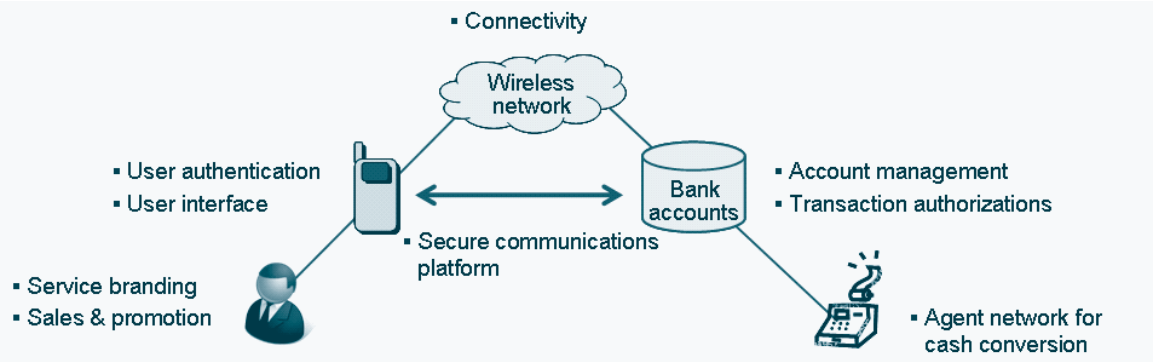
STK services that require the active support of the operator condition the bank's business model in two important ways. First, the operator may negotiate higher fees or a revenue share on mobile banking revenues in exchange for offering the services that are required. Second, it may be harder for the operator to achieve interoperability of its service across mobile operators, because that requires striking a separate deal with each mobile operator.

Moreover, there is the risk that mobile operators simply refuse to deal with smaller banks or MFIs that do not *prima facie* present enough of a business opportunity for them. This could put smaller banks at a competitive disadvantage. If this were to happen, smaller banks might consider sharing a mobile platform (which would also reduce costs for each) and establishing a single negotiation with the operators.

So what can a mobile operator bring to the table? What should a bank look to the mobile operator to provide? Next, we consider a set of incremental roles the mobile operator could fulfill on behalf of a bank wishing to offer mobile banking services to its customers. Figure 3 summarizes what banks can expect to get from partnering with mobile operators.

At a minimum, a bank will need to buy **wireless connectivity** from the operator. For that alone, no special relationship is required between the bank and the mobile operator, assuming that the operator uses one of the publicly available bearers (e.g., SMS, GPRS, or perhaps USSD). The bank and its customer can use the mobile service on standard commercial terms.

Figure 3. What the mobile operator can provide



This is what banks normally will do when they offer purely informational services (marketing messages, SMS alerts) to their customers.

The next step is for the bank to seek **SIM services** from the operator: access to the memory in the SIM to use the encryption keys and phone service menu. The operator handles OTA provisioning of the handset. From the bank's perspective, this will improve the customer experience and security of mobile banking transactions. All STK-based services get at least this level of support from operators.

The bank might look to the mobile operator to offer a more integrated **hosted secure communications platform** to a bank, whereby the mobile operator manages the entire communications between the client in the SIM all the way to the back office server of the bank. The bank completely outsources all communications aspects, so that, as far as the bank is concerned, the mobile banking channel looks like a stream of transactions coming down a single pipe. The bank retains only the purely banking bits.

A bank might go further and actually ask operators for a **hosted mobile banking platform**. The core banking system itself is hosted and run by the mobile operator, who conducts transaction authorizations on behalf of the bank. The bank owns the accounts (and they appear in its general ledger) but it delegates the operation of the system to a mobile operator. The mobile operator in effect offers a white-label mobile banking service to the bank. In the Philippines, Banco de Oro uses Smart Communications to operate its prepaid account platform just in this fashion.

The support model between the bank and the telecommunications company also needs to be considered carefully. Any issue with a mobile phone tends to result in calls to the operator's contact center, whether it involves the banking application or not. Both will need to work closely together to deal with customer service issues, but it makes sense for the operator to provide first-line customer care service to banks on the mobile banking applications and to refer cases to the bank on a second-level support basis.

Mobile operators also can offer substantial marketing support. They can engage in **cross-marketing** activities with the bank to promote and cross-sell banking services to its telephony customers. They also can use their extensive **network of stores and resellers** to sign up customers for the banking service. Moreover, by offering **mobile branding**, the bank can create an alternative proposition that appeals more directly to customers with stronger affiliations to mobile phones and mobile brands than to banking.

In fact, the prepaid account service by Banco de Oro in the Philippines is actually branded by the mobile operator, as SmartMoney. MTN and Standard Bank have the same relationship in their joint venture: marketing collaterals refer to MTN Banking, stating in small print below "A Division of Standard Bank."

Finally, a mobile operator might package its network of dealers and airtime resellers as an **agent network** for cash in/cash out to support the mobile banking proposition. The mobile operator can be an "introducer" to its distribution network, or it can function as the network manager. A case in point is Tavrichesky Bank in Russia, which uses mobile operator Beeline's distribution network as cash agents for its Pay Cash service. A mobile operator in Pakistan is considering offering Tameer Bank the use of its own distribution network for both distribution of SIMs with the STK solution and for cash in/cash out.

There is another role the mobile operator could take: the issuer of the accounts and maintainer of float. At this point, the mobile operator is the intermediary, and there is no role left for a bank. This is the situation with G-Cash in the Philippines and M-PESA in Kenya,

where mobile operators Globe and Safaricom offer the service entirely on their own. Float is held in the operator's name at one or more banks where the operator banks.

At the other extreme, the bank could seek to take some of the operator's "traditional" value chain roles and become a mobile virtual network operator (MVNO)—essentially buying wholesale access to a mobile operator's network and retailing the mobile service under its own brand. The operator essentially provides a "white label" mobile phone service to the bank. Bankinter of Spain has pushed this model furthest, even providing its own SIMs, which can then house its own applications completely independently of any operator.

In our discussion thus far, we have considered two players only: the bank or MFI and the mobile operator. However, there may be third parties performing some of the functions mentioned, acting on behalf of either the bank or the operator.

When banks use wireless connectivity or buy bulk SMS, they can choose to work with various "gateway" companies that have a direct connection to the operator's network.[14] When banks look for OTA provisioning of a SIM application, the application could be developed by a vendor for the bank or operator. The vendor develops the solution only for the bank or as part of a partnership arrangement between the bank and operator. When the bank is looking for a hosted mobile banking platform, then the vendor is usually working for the operator or the solution already exists at the operator end.

Another scenario is also possible: a third-party platform that serves as a hosted mobile banking platform for both banks on one end and operators on the other. The platform vendor is responsible for getting all the operators on board, and they market the solution to multiple banks. Here the platform vendor creates favorable economics for smaller banks and MFIs, and even smaller mobile operators.

Smaller banks and MFIs need not strike individual relationships with operators and need not own and operate their own platform. For the smallest institutions, the platform can even host the accounting function (i.e., not just payments or transactions), freeing the smaller institution to focus on its core competencies.

Our discussion has illustrated the range of choices a bank has in terms of how to structure a relationship with mobile operators. It can go from a narrow purchase of bulk SMS, to a full-fledged outsourcing of a parallel banking infrastructure. Which option a bank should pursue depends on how tightly it wants to integrate the mobile banking service into its core propositions, and its ability to implement technology-based projects.

Of course, a solution tightly linked to a particular mobile operator will restrict the use of the service to subscribers of that mobile operator, which could limit its market. So banks also must balance the need for universal, multi-operator solutions with the practicality of outsourcing more functions to a single mobile operator. Using the mobile operator's distribution and marketing channels also has revenue implications: fees are split among the operator as brand, the operator as distribution, and the bank as banking intermediary.

Approaching the regulator

There are significant regulatory factors that define the competitive field for mobile banking, and providers would do well to consider them carefully. Key regulatory factors that need to be considered include the following:

14 A mobile operator might have a wholesale model whereby it allows third parties to connect to their SMS Service Center (SMSC) via a defined interface (called SMPP).

1. **Cash in/cash out:** Regulatory restrictions on banks to outsource cash-in/cash-out functions to third-party retail establishments. These restrictions or lack of clear regulation on use of agents play a role in determining how banks can use existing retail networks—including the operators' distribution—for cash-in/cash-out points. Restrictions may relate to who can become a banking agent (e.g., in India it has to be a not-for-profit organization), agents' licensing requirements (e.g., in Brazil agents engaging in deposits and withdrawals must be individually approved by the Central Bank), and the nature of the contract between the bank and the agent.

2. **KYC:** Regulatory obligations for banks to know your customer (KYC) and maintain transaction records, and their ability to outsource this function to third-party retail establishments. For banks adopting mobile banking under a "virtual bank" approach or as part of outreach campaigns, KYC rules can impose a heavy burden on customer enrollment precisely because they lack the physical infrastructure and personnel to undertake customer interviews. Such banks need to work with regulators to find practical yet sufficiently rigorous solutions based on the risks involved.

3. **E-banking:** Rules on the use of electronic retail transactional channels, including minimum data security levels, preservation of customer privacy, customer claims and redress mechanisms, and other consumer protection rules. Regulatory clarity on these aspects serves to provide assurance to banks that the systems they build will not need to be constantly readjusted as new rules come into place and to help banks assess more precisely the legal risks involved in providing mobile banking services. On the other hand, in the initial stages of market development, banks may prefer the regulator not to be overly prescriptive while they are becoming familiar with the practical issues involved.

4. **Issuance:** Regulatory restrictions on account issuance by nonbanks, or on the outsourcing of the operation of bank accounts to nonbanks. Regulators in a number of markets permit or do not explicitly disallow operators from offering mobile payments services on their own, as is the case with G-Cash in the Philippines or M-PESA in Kenya. Banks may feel this adds operators to their competitive landscape, and this may weaken the incentive of the operator to support banks' mobile banking efforts. Regulations may also affect whether banks can let mobile operators host and manage their mobile money accounts, which may simplify the implementation of mobile banking solutions (as is the case with SmartMoney in Philippines or MTN Banking in South Africa).

5. **Taxation:** Taxes on telecommunication services. Higher sales and special taxes on communication services can restrict customer uptake. Kenya lifted its special taxes on communications in 2006 and already has seen a big uptake in mobile phone use since then.

How much service interoperability to seek

For service providers like banks and mobile operators, interoperability—working with other service providers within an agreed commercial and technical framework—creates opportunities for enhancing the services available to customers. Yet it may involve protracted negotiations with other parties and costly investments to implement.

Service providers also worry that it may make it easier for customers to switch service providers, because customers may be able to more easily find a similar

Table 4. Implications for providers of the five major types of service interoperability

Customer functionality	Significance for mobile banking provider	Requirement for interoperability
I can start using mobile banking service on my current phone/ SIM.	Operator independence: a bank can acquire customers who happen to be with any mobile operator	• STK agreement with all operators, or • Use of non-STK-based service platform, like USSD • Go through shared mobile industry platform
I can send/receive money to/ from anyone with a bank account.	Offer of full payments capability	Access to national payments system through an EFTPOS switch
I can use other people's mobile phone number to transfer money into their account.	Convenient user interface (no typing of account numbers)	Access to national payments system as above, plus a national database linking people's phone numbers and their bank account numbers
I can use my phone to deposit, withdraw, or remit cash at any ATM or authorized POS-enabled banking agent.	Maximum liquidity options for customers, with minimum own cash-handling costs	• Access to national payments system through EFTPOS switch • ATM/POS devices programmed to enable use of virtual smartcard embedded within phone; or pairing of card with mobile phone service • Contractual agreement with agent acquiring network(s)
I can switch mobile banking provider, and keep my mobile banking service.	Unlikely to be sought, because this would make it easier for customers to churn.	National interoperable mobile banking application

customer experience with another provider. More fundamentally, if a service is offered jointly by several providers, the notion of customer "ownership" becomes blurred.

This is the dilemma: you want your customers to take advantage of services offered by others, but you do not want to expose them to predation by others. Managing "co-opetition" (when you are cooperating with potential competitors to your claim of customer "ownership") is always tricky.

There are many ways in which service providers can interoperate in the context of mobile banking. Next we consider five major types of interoperability and explain how they relate to the mobile operator used, interbank payments and cash services offered to customers, and the mobile banking application itself (see Table 4).

Lessons for the road

Banking via a mobile channel is an idea that most bankers (and many bank clients) find intuitively logical, albeit daunting and confusing, to implement. In today's world of electronic-based accounts, money is "information" passing through communications networks. The customer experience at the ATM—punching in a PIN, selecting among various options, being instantly gratified—evokes our mobile phone experience. We place our mobile phones in a very exclusive location—our pocket—alongside our money and our home keys, which suggests the high value we attach and even the level of dependence we have to the phone. Why can't my mobile phone *be* my wallet?

But first an update on Ali Abbas Sikander and Tameer Bank: Abbas decided that the mobile banking

channel was probably going to be the only channel for his rural customers, and hence it was going to be a key element of an aggressive growth strategy. Abbas and his colleagues determined the level of strategic engagement with the operator and the type of solution after navigating through their technology choices (which were explained in the second part of this paper). He decided to use an STK solution, which offers the highest level of end-to-end security but also requires a more integrated partnership with the mobile operator.

He decided to use the operator's prepaid card distribution network, one of the largest retail networks in Pakistan, to distribute new SIMs and serve as cash-in/cash-out points. Although the new service is most likely to be co-branded by the operator and Tameer, the operator's brand will be more prominent, which will help market the service to millions who use cell phones but have no formal banking relationships and already know the operator's brand well.

As banks follow Abbas's lead and begin implementing their mobile banking strategy, here are some "lessons for the road."

The mobile banking opportunity will be largest for growth-oriented banks. Banks that are aiming to grow rapidly should benefit more from strategic alliances with mobile operators, leveraging several of the operator's key assets. Banks can take advantage of the mobile operator's widespread wireless coverage and extensive use of wireless devices as part of a branchless expansion program (using, for instance, manned POS devices at stores serving as banking agents). Branch economics, with heavy capital and labor costs, favor an environment for branches that is densely populated and where the customer transacts at higher values. Banks can also take advantage of mobile operator's large and tiered distribution networks to roll out their banking agents.

Telecommunications companies have substantial leverage in mobile banking, and banks need to sit down and negotiate with them. Banks need to work with mobile operators if they want to create mobile banking services that are highly customer friendly, fast, and secure. Mobile operators' control of the SIM, plus the attraction of leveraging their distribution networks, puts them in a strong negotiating position. This might create a challenge for smaller banks, who might find it more difficult to strike the right deal with mightier operators, or who might simply struggle to get them at the negotiating table. It also may create a tension with the principle of interoperability across networks, because tighter relationships might not be achievable with all networks.

Liquidity (conversion to/from cash) remains the anchor of the value proposition for mobile banking customers. To derive the most value from remote transactions—using the cell phone just like an Internet terminal—begins with getting people to leave more cash in their accounts. This might happen when people see that there are many ways in which they can cash out. In the language of payments, there needs to be a wide acceptance network. Once that cash-in/cash-out network is established, the value of transacting remotely may become more apparent. There may be cash substitution, but it will be only a very gradual process.

Banks who want to use mobile banking to reach out to unbanked customers need to develop strong partnerships for mass-market promotion of the service. Most banks do not have the capacity to aggressively market mobile banking on their own. Banks that want to use mobile banking to reach unbanked customers need access to marketing channels to and brand credibility with precisely those customers who have been excluded from banking. Unlike most banks, mobile operators traditionally use a mass market approach and aim to get into the pocket of every citizen.

Banks can learn from the mass-marketing approaches of mobile operators, or better still, can partner with them—and that's on the marketing and branding side, not just on the technical service delivery side. Also, there may be other types of service providers or retailers that banks could seek out as marketing partners.

Mobile banking does not raise any inherently new security issues; still, ensuring adequate security through a combination of technology and operating processes is paramount. Any bank with an Internet banking channel can offer mobile banking today: all the bank would need to do is "reformat" its Internet banking content from HTML to WAP, to make it accessible to devices with smaller screens and a mobile-specific browser.

The security solutions to the problem of Internet banking (fundamentally, communicating through a customer device and over a network that cannot be assumed to be totally secure) apply equally to mobile banking. Moreover, mobile banking introduces the opportunity of using SIM-based security, which is more analogous to the ATM banking model in its use of cards (physical bank cards or embedded in the SIM card). Whatever the security of the technical solution, operators will need to ensure that operating procedures around it do not open up vulnerabilities.

References

Bezuidenhoudt, Johann, and David Porteous. 2008. "Managing the risk of mobile banking technologies." Johannesburg, South Africa: FinMark Trust. http://www.finmark.org.za/documents/MBTechnologies_risks.pdf.

InfoDev. 2006. "Micro-payments Systems and their Application to Mobile Networks." Washington, D.C.: InfoDev. http://www.infodev.org/en/Publication.43.html.

Ivatury, Gautam, and Ignacio Mas. 2008. "The Early Experience with Branchless Banking." Focus Note 46. Washington, D.C.: CGAP.

Krugel, G. 2007. "Mobile Banking Technology Options." Johannesburg, South Africa: FinMark Trust. http://216.239.213.7/mmt/downloads/finmark_mbt_aug_07.pdf.

Mas, Ignacio, and Hannah Siedek. 2008. "Banking through Networks of Retail Agents." Focus Note 47. Washington, D.C.: CGAP.

Porteous, David. 2006. "The Enabling Environment for Mobile Banking in Africa." Boston: Bankable Frontiers. http://www.bankablefrontier.com/assets/ee.mobil.banking.report.v3.1.pdf.

The Economist. 2007. "The Future of Money." *The Economist*, 15 February 2007.

Annex. Comparison of selected mobile payments systems

	Smart Money	GCash (pre-STK)	M-PESA	WIZZIT
Country	Philippines	Philippines	Kenya	South Africa
Technology platform	STK using SMS bearer	Native SMS (STK solution in place, but not discussed here)	STK using SMS bearer	USSD
When started?	December 2003	November 2004	Trial 2006, launched April 2007	November 2005
Exchange rate to USD	1 USD = 42 PHP	1 USD = 42 PHP	1 USD = 64 KES	1 USD = 6.8 ZAR
The Players				
Who brands the service?	Smart Communications, as Smart Money	GXchange (GXI), a wholly owned subsidiary of Globe Telecom, as GCash	Safaricom, a Vodafone Group affiliate, as M-PESA	WIZZIT, an independent company (with stakes by IFC, Africap and Oiko Credit)
Which mobile networks may be used by users?	Smart only	Globe or Touch Mobile only (a subsidiary of Globe Telecom)	Safaricom only (transfers can be sent to users of any mobile network)	Any
What kinds of accounts are offered?	Prepaid accounts	Prepaid accounts	Prepaid accounts	Individual Exemption 17 accounts
Who are the issuers?	Banco de Oro; account data is maintained by Smart on its servers	Held by GCash	Held by the M-PESA Trust Company, of which Vodafone is the trustee	Held by a division of the South African Bank of Athens (SABA).
What license does the issuer have? What are the reserve or capital requirements?	Full banking license (Banco de Oro).	Licensed as remittance agent; 100% of prepaid balances are deposited as a pooled account (in GXI's name) at 16 licensed banks	Unlicensed; 100% of prepaid balances are deposited as a pooled account at a bank (CBA)	Full banking license, under Exemption 17, which reduces KYC requirements in exchange for balance, transaction, and other limits on accounts
Which payment networks are used; who manages them?	Smart's platform for transactions between users built by GFG; Mastercard for card transactions at POS transactions	GXI's proprietary platform, built by Utiba	Safaricom's proprietary platform	Bank of Athens; leading to BankServ payments switch, including Mastercard; WIZZIT developed a proprietary system that links incoming data over USSD to the bank's core banking system and that shows the menu on the handset
Account Opening				
Where and how do customers register for the service?	User completes form at Smart Wireless Center and shows valid ID; OTA activation is also possible.	From mobile by sending SMS with keyword REG followed by a user-defined PIN, mother's maiden name, first and last name, address, and landline number	At M-PESA agent; users provide name, national ID or passport number, phone number	Performed by roving WIZZkids or at Dunn's clothing stores; users provide name, date of birth, national ID number
When does the customer go through KYC procedures and by whom?	At Smart Wireless Center, at time of sign-up, or before any cash withdrawals or purchases	At time of first cash transaction (in or out), by the agent; user shows ID and fills out a 1-page form.	At agent, at time of sign-up	By WIZZkids or by agent, at time of sign-up; greater KYC requirements for balances > ZAR25k or transactions > ZAR5k.
Account opening requirements and fees	Free for mobile banking plus PHP220 charge for card; no minimum deposit	Free; no minimum deposit	Free; no minimum deposit	ZAR 40 for a starter pack (card and user manual); no minimum deposit
What customer setup is required for the mobile service?	New 64K SIM may be required (STK applet can be sent OTA)	None (based on SMS)	Requires new SIM card with preloaded menu (preloaded STK application)	None (based on USSD)
How does the user get a PIN?	User selected; on first-time use of STK menu, user is asked to enter a W-PIN, which is then stored on the SIM	User selected, at the time of registration	Customer gets initial SMS with initial PIN; on first use, customer enters initial PIN and ID number, then is asked to enter new PIN	User selected, at the time of registration
Is a card associated with the account?	Optional Maestro-branded debit card	No	No	Mandatory Maestro-branded debit card
Can a user have multiple accounts?	Yes; menu prompts for account selection when user wants to transact	Not on the same phone number	Not on the same phone number	No

	Smart Money	GCash (pre-STK)	M-PESA	WIZZIT
Country	Philippines	Philippines	Kenya	South Africa
Account Maintenance				
Are there limits on account size?	Maximum PHP50k on wallet	Maximum PHP40k on wallet	Maximum KES50k	Maximum ZAR 25k; otherwise need full KYC
Is there a recurrent or maintenance charge?	Only annual subscription charge for the debit card	No	No	No
Are accounts remunerated? Who keeps float?	Not remunerated; issuing bank keeps float	Not remunerated; GXI keeps float	Not remunerated; Safaricom keeps float	Interest paid for large balances; float held by SABA, but interest on float is split with WIZZIT
Electronic Transfer of Money (Basic P2P)				
Are there limits on size, number, or frequency of transactions?	100k per month	Minimum PHP100 per transaction; maximum PHP10k per transaction, 40k per day, 100k per month	Maximum KES35k	Yes; for Exemption 17 accounts, maximum balance ZAR 25k, maximum transaction size ZAR 5k
How does the user initiate a transaction?	User selects transaction type from STK menu on phone; handset prompts user for necessary data, one piece at a time (e.g., phone number, amount, PIN), and then presents transaction summary for confirmation by sender, before sending by SMS	User composes SMS with amount and PIN and sends it to 2882+10-digit mobile number of sender	User selects transaction type from (STK-based) menu on phone; handset prompts user for necessary data, one piece at a time (```phone #, amount, PIN), and then presents transaction summary for confirmation by sender, before sending by SMS	User sends USSD using transaction-specific codes (from chit sheet available to users); phone prompts user for phone number, amount, and PIN on separate USSD messages, and then presents transaction summary for confirmation by sender
How does the user authorize the transaction? How is the user authenticated?	User-entered PIN is not in clear view and is validated by SIM	User enters PIN in SMS request, not in clear view; SMS remains in phone's message history unless erased	User-entered PIN is not in clear view and is validated by SIM	PIN goes over the network in a USSD message; it is not stored in message history
Who authorizes the transaction?	Smart	GXI	Safaricom	WIZZIT, on behalf of SABA
How are sender and he recipient notified of the transaction?	Both get confirmation by SMS	Recipient must first accept transfer; both get confirmation by SMS	Both get confirmation by SMS	Both get confirmation by SMS
Can the user transact from another person's SIM/phone?	No, but user can transact using the associated MasterCard	No	No	No, but user can transact using the associated Maestro card or at SABA branches
Who monitors and reports on suspicious transactions?	Smart, in delegation from the issuing bank	GXI	Safaricom (it is adopting higher UK/US standards)	WIZZIT, though SABA has responsibility to central bank
Fee for person-to-person transfers	PHP2.5	User pays no charge (plus PHP1 for the SMS)	KES30 (plus standard SMS charge)	ZAR 2.99 to other WIZZIT clients, ZAR 4.99 to others, plus standard SMS charge
Transacting to/from Nonusers and Other Bank Accounts Held by Users				
Can users send money to nonusers?	No	No	Yes; recipient can cash out at retail outlet showing code that will be sent to their phone by SMS	Yes
Can users receive money from nonusers?	Yes (Domestic Padala service); PHP10 fee	No	No	Yes
Can user top up from other accounts it holds at other banks?	Yes, from customer accounts at 15 mobile banking partner banks	Yes, from select banks only (like BPI)	No	Yes, from any bank via electronic funds transfer
Allow payments to third-party bank accounts?	No	No	No	Yes to any bank

	Smart Money	GCash (pre-STK)	M-PESA	WIZZIT
Country	Philippines	Philippines	Kenya	South Africa
Merchant Transactions for Cash or Purchase of Goods				
What device does the merchant use?	POS device or mobile phone	Mobile phone	Mobile phone	POS device
Who acquires the merchants?	MasterCard for card-based POS; Smart for cash retailers	GXI	Nobody (they operate as a standard P2P transaction)	MasterCard
Who initiates phone-based purchase of goods and how?	Merchant; user gets SMS with amount to pay, and confirms transaction	Merchant; user gets SMS with amount to pay, and confirms with return SMS (YES + PIN)	Paying party (i.e., customer). Merchant is identified by his phone number	Paying party
Who initiates phone-based cash deposit transactions and how?	User fills in deposit slip, goes to cashier, and shows valid ID; merchant sends SMS request	User fills in a slip, goes to cashier, and shows valid ID; merchant sends standard P2P payment request by SMS	Similar to basic P2P transaction; no paper receipt is given	Not applicable (deposits via branches and ATMs of Postbank, ABSA, SABA)
Who initiates cash withdrawal transaction and how?	User fills in deposit slip, goes to cashier, and shows valid ID	User fills in same slip, goes to cashier, and shows valid ID; user sends standard P2P payment request by SMS	User gives mobile number to agent and shows ID; user then selects "withdraw cash" from STK menu, enters agent number, cash value, and PIN; handset prompts user with summary of transaction, for user confirmation	Not applicable (withdrawals via branches and ATMs of Postbank, ABSA, SABA)
Fee for cash deposits	User pays 1% of amount deposited through cashier (free if using a card)	User pays 1% of amount deposited, with a minimum fee of PHP10	Free	User pays 1% for cash deposits (minimum ZAR 4.99); flat ZAR 4.99 for check deposits
Fee for cash withdrawals	ATM charge of PHP3-11 (depending on whose ATM)	User pays 1% of amount withdrawn, with a minimum fee of PHP10	KES25-170, depending on size of transaction	At ATMs, ZAR 4.99 plus ZAR 0.99 per ZAR 100; ZAR 1.99 for cash back at merchants
Other Available Services and Transaction Charges				
Account management (change PIN, check balance, etc.)	Free access to the current credit balance	PHP1 for the cost of the SMS to make the request	KES1 (plus cost of SMS)	ZAR 1 for account balance via mobile, ZAR 5 via ATM
Buy airtime	Minimum top-up of PHP30	Free, and get 10% rebate (as a promotion) for users' or third-party phone	Free	Free
Bill paying	Yes	Yes	Not applicable	Yes
Direct deposit of salaries	Yes (similar to Smart Padala model)	Only for rural bank employees	Not applicable	Yes
International remittances	Yes, in conjunction with 47 overseas remittance partners in 19 countries	Yes, partnering with United Coconut Planters Bank or partner retail franchises like 7/11 to allow cash deposits	Not applicable	No

No. 48
June 2008

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

CGAP welcomes your comments on this paper.

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

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

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

Email:
cgap@worldbank.org
© CGAP, 2008

The authors of this Focus Note are Ignacio Mas, an adviser in the Technology Program, and Kabir Kumar, a microfinance analyst in the Technology Program at CGAP. The authors wish to thank Gautam Ivatury, Hannah Siedek, and Mark Pickens of CGAP and David Porteous and Abbas Ali Sikander for very helpful discussions.

CGAP materials are frequently cited in other works. The following is a suggested citation for this Focus Note:
Mas, Ignacio, and Kabir Kumar. 2008. "Banking on Mobiles: Why, How, for Whom?" Focus Note 48. Washington, D.C.: CGAP, June.