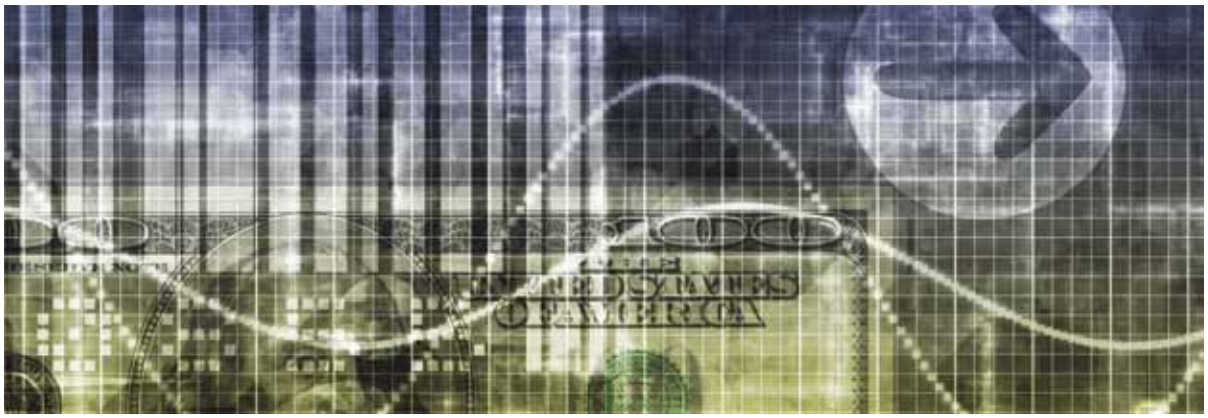

RECOGNIZING THE VALUE AND OPPORTUNITY OF MOBILE MONEY

By Carol Realini

There are five billion mobile phones in use around the world, providing unparalleled access to communications and mobile applications.[1] This is having a profound effect on the lives of consumers, business infrastructure, and the way governments tackle challenges. Specifically, mobile ubiquity has brought extraordinary communication access to those that never had it before.

Now, a growing number of mobile money applications are expanding upon this and, in the process, changing the way traditional bank customers choose to be served, which opens up opportunities to reach an unprecedented number of new customers. With this new access come great opportunities and challenges. The challenges include ensuring security and risk management when offering financial services through these new channels and with this vastly expanded access. In addition, mobile money applications represent an opportunity for governments everywhere to improve financial efficiency and security.

The vast majority of people worldwide are unbanked or under-served. In the U.S. alone there are over 40 million families who are underserved by traditional banking models.[2] Additionally, it is not just consumers that are underserved. The vast majority of sellers of goods and services accept payment by only cash and checks. According to studies from the Philadelphia Federal Reserve, 80 percent do not accept electronic payments today. Some predict recent legislation and economic conditions will mean that this number will increase in the coming years. At the same time, the number of mobile banking users around the world is expected to surge more than 16-fold to 894 million by 2015, according to Berg Insight, an industry research firm based in Stockholm. Clearly, this represents a fundamental shift in how people bank, send and receive money, and pay for goods and services.

What is Mobile Money?

As a roundabout way of defining mobile money (aka mobile financial services, mobile banking, mobile payments), let's first answer the question "How does mobile money get started?" For consumers, adoption of mobile money typically starts with one specific need then quickly moves to multiple, more complex uses as consumers gain experience and comfort. Three specific use cases stand out as driving adoption in the U.S.: sending money; getting paid money; and transferring money — instantly, securely, and easily

[1] International Telecommunication Union (ITU) http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf
[2] The Center for Financial Services Innovation http://cdcu.coop/files/public/AbateD2.ppt

with a simple command, text message, or smart phone app based on user prefers.

Next, let's look at what form mobile money takes or the structure of mobile money. Is mobile money a way to initiate a credit or debit transaction from an existing bank or credit card account? Is it a new account where money is loaded into the mobile account and then transactions happen from this new account? Is it a "wallet" where consumers have all their financial options available and then make choices depending on what they are buying? The answer is that mobile money is all of the above. Consumers want the option to move money directly from their own bank account, set up a companion mobile account similar to how PayPal operates online, or use a debit or credit card. Providers need to provide and regulators need to allow for a spectrum of options if they want to provide mass market solutions. In all cases, since mobile users have an expectation of immediate results, solutions that allow instant movement and access are strongly favored in an increasingly mobile-centric world.

Mobile money has the power to change the global economic picture — and it is due to more than just technology and mobile communications infrastructure. Mobile phones have extensive distribution networks built out to sell handsets and prepaid minutes. In countries that lack good physical banking infrastructure, like Kenya and India, the mobile players are transforming their retail networks into banking access points which enable enrollment, cash loading, and unloading (agent banking). This brings new access to large numbers of consumers and businesses, offering them their first banking products while addressing the physical infrastructure limitations of the current bank branches and ATMs. It may start by providing them with simple mobile prepaid accounts for money transfer or mobile recharge, but that is just the tip of the iceberg. Once the enrollment is done and the user starts transacting, they easily migrate to, and demand, a more complete banking relationship and value added services. We see this in both Kenya and India where Obopay offers both types of services — mobile prepaid and mobile bank accounts. Experience leads to the conclusion that these same consumers will adopt other services when they are offered.

Risk and Security

As a front end channel to a financial transaction system, the mobile device is in many ways similar to a PC. There are risks associated with data security, financial fraud, and money laundering that need to be managed. And, while there are significant differences in the data and tools available in developed versus developing markets, in order to manage risk and security, mobile financial service providers have to know something about the identities of users, the origin and destination of funds, and have the authority to conduct transactions with those funds. Addressing these challenges in developing markets also creates an opportunity to migrate existing underserved users to a more secure transaction environment than those they currently use. For example, there is certainly opportunity to migrate government disbursements to underbanked recipients to a much more secure process, and there is an opportunity to develop greater transaction transparency by moving cask and check transactions to digital transactions initiated through a mobile device.

Managing risk in a mobile environment requires that providers collect and store data in a secure manner and make that data available only to those that must have access. Providers use the following methods to accomplish these goals.

Know Your Customer (KYC)

To conduct mobile payment transactions, the provider must be able to authenticate the identities of both the sender and receiver. This is required to prevent both money laundering and financial risk to the provider. Normally, this involves the collection of personal identifying information (PII) such as name, address, date of birth, and identity credentials from prospective users. In less developed regions, identity credentials can be an issue and solutions are often tailored to meet regional realities. This PII is validated against third party databases, such as credit bureaus or banks, and checked against Office of Foreign Assets Control (OFAC) and other restricted entity lists. Lastly, users can be subjected to knowledge-based authentication in which they are presented with questions to which only they should know the answers. Where ID failures occur, there are follow up discussions with the prospective user and requests for hard copy identity documentation.

In addition, transactions involving movement of funds from individuals to businesses present a financial and credit risk to the service provider. In these cases, it is incumbent upon the provider and the banks that stand behind the transactions to understand the nature of the business and the financial health of the business or retailer.

Mobile money has the power to change the global economic picture — and it is due to more than just technology and mobile communications infrastructure.

Funding Source Authentication

A mobile financial system must provide ways to get money into and out of the network. Providers must adhere to basic anti-money laundering requirements, including proper KYC, understanding the source funds, and being on the lookout for evidence of structuring or layering. Providers and their agents must also monitor and report on large cash transactions and patterns as required by the PATRIOT Act and other regulations.

Account funding can be as simple as taking and dispensing cash at physical locations such as retail stores. It can also include enabling electronic funding and withdrawal from the network. This is usually done by a debit to the user's checking account, accomplished in the U.S. via the Automated Clearing House (ACH) system, or by charges to user's credit or debit card. When enabling electronic funds, the first challenge is to determine if the account is valid and if the user has authorization to transact on those accounts. Account ownership verification can be accomplished by having the user verify two small random credits to the account. In the case of credit or debit cards, the provider will initiate an authorization against the card, usually requiring the full billing address and the card security code to authenticate ownership of the account.

Multifactor Authentication

Once a user has authenticated his or her identity and ownership of funding sources, access to the mobile financial account is controlled by a set of credentials (i.e. user name and password), as well as a series of system authentications of the user's phone and PC.

In the case of a mobile phone, the account registration process can include an automated call to the phone requesting the user input a mobile PIN. This establishes that the phone is in the possession of the user at time of registration. From that point, that one phone is the only mobile device allowed to access the user's account. Transactions on that device will require the input of the mobile PIN that was established at registration.

In the case of PCs accessing an account, the provider uses methods to establish and ensure a trusted device is used for transactions. Providers will record the device ID of the PC. If subsequent attempts to access the account are made by a PC that the provider's system has not previously recorded (an untrusted device), again, an automated call can be made to the user's mobile phone requesting input of the mobile PIN. This prevents the takeover of an account by someone who may have gained access to the user's credentials.

Transaction Monitoring

After the provider has authenticated a user's identity, account access, and devices, the user is ready to transact. Transactions can be governed by a set of hard limits and by a flexible set of parameters established by modeling the behavior of the user and the account over time. These limits are generally the number of transactions and the value of those transactions in any given time period. These parameters may also govern how much and how often a user can send or receive money.

Limits and parameters are used to limit both financial and money laundering exposure, but they also establish benchmarks against which suspicious activity is monitored, allowing the provider to look for red flags.

Access Monitoring

In addition to transaction monitoring, providers also look to see who accesses their system, how often they do it, and who their customers might be associated with. For example, a fraud or money laundering ring may use a single PC to set up and transact on multiple accounts. A provider may notice suspicious access or

transaction patterns on one of those accounts that can be used to identify other problem accounts.

Data Security

Setting up and maintaining a financial transaction system requires the collection of and access to sensitive data. Providers should adhere to industry best practices regarding data collection, encryption, storage, and access. At the very least, providers who store this type of data should be PCI DSS Level 1 certified.

Further, in extending access to mobile channels, providers should be very attentive to data that is sent to or stored on the mobile device. Sensitive data should not be stored on the device. Similarly, data sent to the device via SMS or within a mobile application should not expose sensitive data.

The Role and Opportunity for Governments

Recently, I attended the Gates Foundation Global Savings conference in Seattle which focused on financial inclusion — thought leaders and innovators from around the world met with Bill and Melinda Gates to discuss leveraging mobile ubiquity to bring banking and savings offerings to those who need it most. On a panel with Bill Gates and other luminaries I suggested a link between m-government initiatives and financial inclusion. Governments can benefit greatly from mobile financial applications; mobile disbursements of emergency funds, social security, and tax refunds are a few examples. These solutions are greener (eliminating use of paper checks and cash), safer for consumers (no stolen checks), and more efficient (reduce time and cost compared with cash or check disbursements — for government and the receiver).

Since more people have phones than bank accounts, these government applications can serve an unprecedented number of people. At the same time, governments can help create a critical mass of users, which then creates the momentum for mobile money solutions. Once momentum is built, other applications and benefits will follow. Since adoption of mobile payments typically starts with one application then quickly moves to more complex uses as consumers gain experience and comfort, m-government applications can drive mass market adoption by getting a large number of people to start using mobile money. Government involvement can also ensure that safety and security standards are met and the regulatory environment is fostered for mass adoption.

Governments should implement m-government mobile money applications for government disbursements and collections. This will kick start the greater market and have the added benefit of driving down the cost of mobile money for the individual consumer. One of the biggest cost factors for mobile money is moving funds or converting cash into mobile money. Government disbursements would mean that funds would be mobile funds from the beginning. Additionally, foundations or government aid organizations considering subsidizing mobile financial inclusion should rethink their tactics. Don't subsidize these solutions in the private sector — instead, work to implement m-government solutions and the private sector solutions will blossom.

In the U.S., the private sector has already started delivering mobile banking and mobile payments. Banks are offering consumers and small businesses more and better choices in how they access bank information, deposit checks, and make and accept payments through mobile phones. Two factors are influencing the increase in mobile banking. The first, as previously outlined, is the growth of smart phones. According to IDC, smart phone shipments jumped by 55 percent in 2010 — 10 percent more than the research firm projected earlier that year. They have enhanced the user experience and increased expectations about what can be done from a mobile phone.

The second, equally significant, has been the development of use cases that are compelling and address consumer pain points. Yet, I worry that without government applications the benefits will fall short of their potential here. That it will be primarily used to improve access for those who already have solutions. U.S. Government m-government applications can take mobile money to its full potential — improving access and driving down costs for all. In addition, it can create greener, more efficient, and safer government solutions. Q

Carol Realini *is the Executive Chairman and Founder of Obopay, Inc., a leading global mobile banking and payment provider. Carol, a recognized international expert in mobile money, has presented to world business and political leaders at events including those hosted by the U.S. State Department, the World Economic Forum, and the Gates Foundation. She has three decades of technology experience, successfully leading companies through initial public offerings as well as into acquisitions. In 2008, Carol was named one of the 50 Top Women in Technology by Corporate Board Member magazine, and in 2010, was recognized as one of the most influential women in Silicon Valley by the Silicon Valley Business Journal.*