

**Mobile Money Transfer Services:
The Next Phase in the Evolution in Person-to-Person Payments**

Cynthia Merritt

Retail Payments Risk Forum White Paper

Federal Reserve Bank of Atlanta

August 2010

ABSTRACT

Money transfer schemes have evolved to the next generation of electronic payments, the mobile channel. Money transfer services for both domestic and international remittances are shifting from traditional providers to wireless carriers who are able to compete for consumer market share on the basis of technological ubiquity and lower cost services. This paper reviews developments in mobile money transfers, the emerging ecosystem, and its participants and business models. It also examines the implications of payment systems roaming across geographic borders with their respective legal and regulatory jurisdictions, as well as the emergence of mobile airtime as an alternative currency. The risk environment for mobile money is examined in the context of both developed and emerging countries and in light of the participation of banks and nonbank telecom firms.

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Federal Reserve Bank of Atlanta or the Board of Governors of the Federal Reserve System

Thanks to the following individuals for lending their expertise and insight to the development of this paper: Richard Oliver of the Federal Reserve Bank of Atlanta, Marianne Crowe and Darin Contini of the Federal Reserve Bank of Boston, Steve Mott of Better by Design, Maria Stephens of the USAID, and Lisa Dawson of Booz, Allen, Hamilton.

1. Introduction

Person-to-person (P2P) payments are evolving to the next generation of electronic payments, the mobile channel. Advances in technology have enabled alternative functionalities for mobile handsets beyond the original visions of the designers of handsets or wireless communication architectures to supporting a new and viable channel for mobile financial services, including bill payment and account transfers, domestic and international P2P transfers, proximity payments at the point of sale, and remote payments to purchase goods and services.

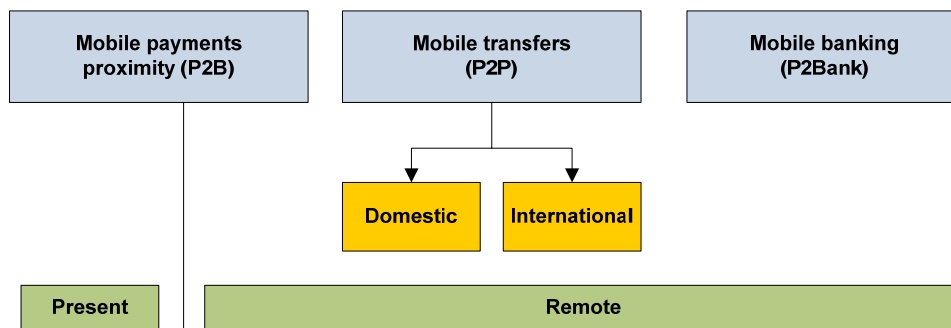
Mobile-enabled person-to-person payments, or mobile money transfer services (MMT), are experiencing rapid adoption in many markets, in response to steady growth in remittances, the worldwide ubiquity of cell phones, and the need for an electronic P2P payment alternative to paper-based mechanisms like cash and checks. More than a billion people worldwide lack access to traditional financial services, particularly in emerging countries, although they have mobile phones (Pickens 2009). As of 2009, 68 percent of the world's population had mobile cellular subscriptions (ITU 2009). The growth in mobile telecommunication service availability is expanding the reach of financial services across wireless networks in less developed countries, creating the potential for significant growth in mobile commerce and financial inclusion. Initiatives such as the Mobile Money for the Unbanked (MMU) program, supported in part by the Bill and Melinda Gates Foundation, are contributing to expanded financial inclusion in emerging markets by investing in mobile-enabled financial services and their supporting technologies. This growing ubiquity has the potential to extend even more financial services to unbanked peoples throughout the world, with industry experts projecting that 364 million people will rely upon mobile money by 2012. A recent FDIC report found that in the United States an estimated 7.7 percent of U.S. households are unbanked, while an additional 18 percent are underbanked (2009). As more citizens of developed countries become unbanked as a consequence of widespread economic crises, financial services companies are beginning to explore the potential for importing these newer payment systems that are emerging from the third world to meet consumer payment needs (Maurer n.d.).

While the money transfer market is well established by organizations such as Western Union and Moneygram, developments in mobile services are expected to increase competition and lower prices, thereby discouraging the flow of money through informal channels. MMT services are expected to account for the majority of mobile financial transactions in the near term because

of the functional appeal to the underbanked in developing countries around the world and potentially in the United States. Current market conditions may be ripe for the adoption of P2P payments by financially mainstream U.S. consumers, judging by the vast number of P2P pilots introduced since late 2009 and the recent growth of online commerce generally (Robertson 2010).

As figure 1 illustrates, MMT has the potential to catalyze the entire mobile financial services market—including mobile payments, banking, and transfers—because it enables the infrastructure for remote mobile transactions and the concept of the mobile wallet (GSMA 2008a).

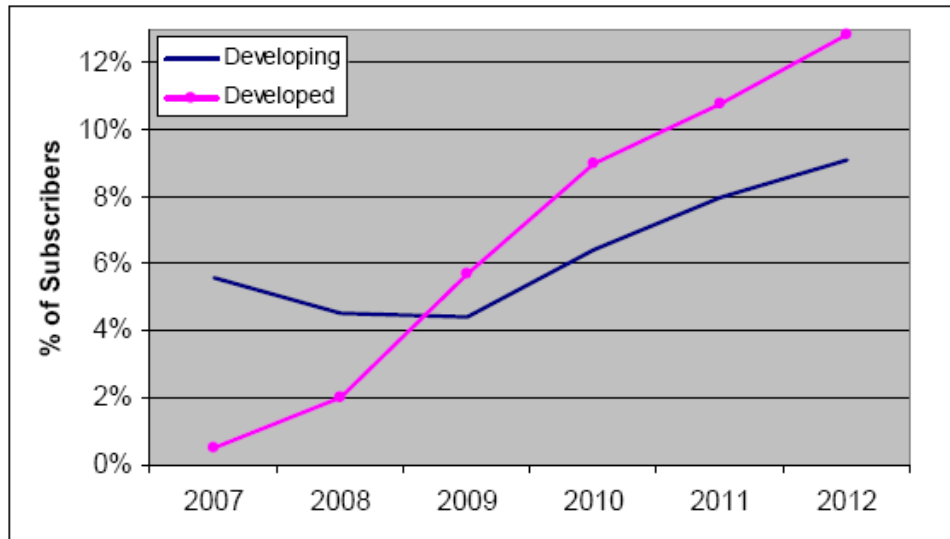
Figure 1: Structure of the mobile financial services market



Source: GSMA 2008a

In fact, a 2007 survey on mobile wallets and mobile financial services showed that respondents expected the number of subscribers using mobile domestic money transfers to grow more rapidly for developed markets than for developing markets (GSMA 2008b). These results imply that consumers in developed markets are interested in electronic P2P payment options and would be willing to conduct them via the mobile device. The survey found similarly that cross-border remittances are expected to grow significantly over the same projected time period.

Figure 2: Outlook for mobile domestic money transfers



Source: GSMA 2008b

The approach to adopting mobile financial services differs throughout the world due to a variety of factors, including the regulatory and legal environments, access to supporting technologies, and economic constraints, as well as experience with antecedent products and services. Consumer need and experience represent key components of each of these variables and are the ultimate determinants of adoption. The vast diffusion of cellular networks allows telecom firms to extend services to broad geographic areas unreachable by traditional financial service providers dependent upon landline networks. In many emerging markets the rapid adoption of mobile payments has led to the unanticipated utility of prepaid airtime as an alternative currency.¹ Expanded airtime distribution channels can accommodate a large customer market increasingly agnostic of geographic borders. Bilateral and multilateral partnerships between carriers expand the wireless network reach to facilitate the distribution of mobile payments services to a greater number of available users.

Mobile payment adoption is currently lower in more developed countries like the United States, where most people have banks accounts and the mobile phone is evolving as merely another payments delivery channel augmenting existing financial products and services. U.S. financial institutions have approached mobile financial services, including both banking and

¹ According to the World Bank, in some countries, airtime created by a nonbank such as a telecom firm can be used as a form of currency, allowing users to transfer electronic currency to each other or purchase items (Chatain, Hernandez-Coss, Borowik, and Zerzan 2008).

payment services, with caution due to concerns about limited opportunities for revenue, the complexity of revenue-sharing agreements with telecom firms, and the belief that mobile payments could cannibalize existing electronic payment services, providing limited return on investment (EDC 2009). Telecom firms, on the other hand, have different incentives for engaging in financial services, namely, the ability to increase revenue from voice services by the addition of data transmissions, particularly in developed countries where mobile markets are reaching saturation levels (Bourreau and Verdier 2010).

The proliferation of new service providers, including telecom firms, money transmitters, and technology developers and service providers, is driving the development of innovative payment schemes for conducting mobile financial transactions. The degree to which these participants work together or independently depends on the business model, which in turn is shaped by the economy, demographics, and regulatory domain of each country. It should be noted that the emergence of mobile commerce and P2P transactions in lightly regulated environments is prompting the central banks of some countries to begin to investigate consumer issues such as security, consumer protection, fraud, and money laundering.

2. The mobile money transfer environment and its stakeholders

The following table shows that the mobile ecosystem embraces a variety of participants, whose collaboration is necessary for the success of the mobile money network, including the mobile network operators (MNO),² financial institutions, airtime agents, telecom retailers, and regulators (Jenkins 2008).

² An MNO is a telecom firm that provides wireless voice and data services for mobile phone subscribers.

Key players in the mobile money ecosystem

Players	Roles	Limitations and Constraints
Mobile network operators	<ul style="list-style-type: none"> • Provide infrastructure and communications service • Provide agent oversight and quality control • Issue e-money (where permitted by law) • Exercise leadership in drawing mobile money ecosystem together • Advise other businesses (banks, utilities, etc.) on their mobile money strategies 	<ul style="list-style-type: none"> • Regulatory limitations on providing financial services • Shareholder pressure for faster, higher returns • Strategic focus that may not include mobile money
Financial institutions	<ul style="list-style-type: none"> • Offer banking services via mobile • Hold float or accounts in customers' names • Handle cross-border transactions, manage foreign exchange risk • Ensure compliance with financial sector regulation 	<ul style="list-style-type: none"> • Narrow customer base • Lack of experience with or interest in low-income customers • Stringent regulatory requirements with significant compliance burdens
Agents	<ul style="list-style-type: none"> • Perform cash-in and cash-out functions • Handle account opening procedures, including customer due diligence • Report suspicious transactions in accordance with AML/CFT requirements • Identify potential new mobile money applications 	<ul style="list-style-type: none"> • Liquidity shortfalls • Basic business skill gaps • Lack of customer trust (in some cases) • Limited ability to partner with large corporations
Regulators	<ul style="list-style-type: none"> • Provide enabling environment for mobile money • Protect stability of financial system • Demonstrate leadership to encourage and protect behavior change 	<ul style="list-style-type: none"> • Lack of experience with convergence of financial and telecommunications regulatory schemes • Lack of financial and technical capacity
Consumers	<ul style="list-style-type: none"> • Use mobile money to improve their lives 	<ul style="list-style-type: none"> • Lack of awareness • Limited financial literacy • Cultural and psychological resistance

Source: Jenkins 2008

While the use of prepaid airtime is beginning to be used as a mechanism for purchasing goods and services in some countries, this discussion is specific to the environment for mobile money transfer payments as opposed to proximity payments, which are evolving in developed countries to include a broader set of use cases, enabling technologies, and number of players in the payments process, including, for example, card issuers and networks.

Mobile network operators

In the most successful mobile payments initiatives, which are predominately focused on the unbanked in emerging markets, the mobile network operator fills the role of drawing the ecosystem together, providing the infrastructure for the payment system and oversight for the agent network. In the process, mobile operators can recognize incremental revenue for the addition of data transmission to their voice network operating systems, either in cooperation with a bank partner or independently. The mobile carriers own the customer billing relationships and exercise control over the distribution of mobile phones through their relationships with the handset manufacturers (Bourreau and Verdier 2010). MNOs generally lack experience in financial services and payments risk and the regulatory and legal governance of payment systems. Where MNOs offer mobile money to consumers through the use of agent networks absent a bank partnership, they also provide the clearing and settlement for the prepaid airtime on the mobile handset.

Financial institutions

In most countries, retail payment systems have been dominated by banks whose primary function in the most basic sense is to gather deposits for deployment in loans and other permissible investments. While financial institutions in developed countries have been slow to offer mobile financial services because of the perceived lack of return on capital investment, recent pilot deployments signal this may be changing. Financial institutions have the opportunity to add value to customer depository services with the addition of mobile technology and realize customer retention benefits as a result. Financial institutions are best positioned to employ risk management programs that ensure regulatory compliance for money laundering and other risks.

Role of agent networks

Agents are nonbank entities such as retailers (either the MNO's own retail center or another retailer such as a village store) that handle customer registration and liquidity needs for the mobile money users, on behalf of the MNOs. In the simplest of examples, the MNO acts as agent, using its own retail distribution network; however, in some countries, airtime resellers have emerged as sub-agents to expand service distribution to more rural locales. The primary

role of an agent is to accept and disburse cash, in essence providing cash-in and cash-out services from the consumer's mobile handset. In this role, the agents serve as branches for the mobile network operators and act as the primary touch point for the customer relationship. As the liaison between the MNO and the consumer, the agent bears responsibility for account opening, customer due diligence, and know-your-customer program compliance.

Retail sales stores and airtime resellers are typical candidates for MMT agents because they tend to have sufficient liquidity to satisfy consumers' needs to deposit and withdraw cash. This network of local agents can expand the mobile operator's reach to rural areas in order to achieve a higher level of penetration in unbanked markets where there is no physical bank presence, essentially enabling a branchless payment system, outside the traditional bank-led business model. Agents typically provide liquidity with funding from other business activities including selling airtime in addition to general merchandise (Bangens and Soderberg 2008).

One example of an efficient agent network is the Safaricom M-PESA model. Safaricom's agent network has evolved into a two-tier structure with master agents who manage liquidity as the liaison between Safaricom and the individual stores, or sub-agents under their management framework. The master agent buys and sells cash from Safaricom, makes it available to the sub-agents, and distributes agent commissions (Bangens and Soderberg 2008). Agents receive commissions for transactions, holding the balances on their own cell phones (Jack and Suri 2010). These mobile airtime balances and cash on premises are the critical elements of the agents' liquidity management system.

Regulators

Regulators also fill a critical role in the ecosystem, as they work to strike a balance between providing prudential, risk-based oversight and encouraging innovation, efficiency, and financial inclusion. Regulators will be challenged by the pace of innovation in mobile payment services and the increasing opaqueness in payment transactions from a regulatory oversight perspective. Mobile transfer systems are giving rise to new challenges in how to establish effective regulatory infrastructures to provide oversight for converged banking and telecom industries in a cross-border context. The telecommunications industry in most

countries is regulated on the basis of a public utility, whereas the banking sector is regulated on the basis of safety and soundness and capital adequacy.

The telecom industry in most countries lacks experience in financial services and the business risks associated with this expanded role. Furthermore, the regulatory infrastructures for mobile carriers in many countries are in nascent stages of development with respect to mobile financial services. GSMA has published guidance on developing a regulatory framework for mobile money transfers with a focus on the remittance segment, recognizing that mobile operators lack experience in payment regulation. The aim of its report is to explain potential regulatory issues arising from mobile operator payment services (GSMA 2007).

3. Business models

Different mobile payments business models have emerged depending on the applicable regulatory climate, consumer culture, and demographics. In the most basic sense, a business model may be bank-centric, mobile-operator led, or partnership led (Boer and de Boer 2010), with technology service firms often included to enable the application or platform for payment service delivery. A number of mobile payment solutions have been introduced recently that cooperate with the major card networks as a funding mechanism and payment channel for P2P mobile transfers. While there are numerous pilots introduced and in various stages of development, many of the card-funded solutions recently introduced, the payments that are initiated by the mobile device are then postpaid by the consumer. While this paper discusses developments in the use of airtime beyond P2P transfers to point-of-sale purchases, the paper's scope does not extend to mobile proximity payments enabled with contactless technologies such as near field communication (NFC).³

Bank-led models

In the bank-led model, the financial institution controls the customer relationship and provides mobile services primarily as a new channel to existing services. The mobile operator provides the channel for the domestic transfers and international remittances conducted by the financial institution. There are fewer examples of bank-led models in

³ NFC is a short-range wireless technology that stores account information in a chip embedded in a card, mobile handset, or some other device for the purpose of enabling proximity payments.

mobile payments services because of the perceived value proposition relative to legacy payment services and the limited ability to reach the unbanked market segment that has driven adoption in most markets. One example is Rabobank in the Netherlands, which in 2006 launched its own mobile virtual network operator service (Boer and de Boer 2010). However, the uptake in this service has been slow and the bank has struggled to gain critical mass adoption.

Mobile network operator-led models

A mobile network operator-led business model limits or eliminates the involvement of the financial institution in the payment delivery, clearing, and settlement. In emerging markets, mobile network operators are dominating the mobile money transfer market, creating the customer relationship and providing the service distribution channel, with clearing and settlement functions often agnostic to the participation of mainstream financial institutions or central banks. Mobile network operator models thrive in developing markets because of their ability to reach large numbers of unbanked people in physically remote locations beyond the presence of bank and landline infrastructures. The geographic reach of this model may be extended through bilateral and multilateral agreements with other wireless carriers, which allow them to expand their remittance services beyond their own geographic borders and regulatory jurisdictions. Some international remittance mobile operators have begun to establish partnerships with service providers such as Western Union and MasterCard, for example, to expand their subscription and payment system networks. GSMA provides guidance to mobile operators and advocates a multilateral or networked hub model to ultimately establish broad-reaching, ubiquitous network coverage—in a sense, consolidating various proprietary models in support of interoperability (Jenkins 2008).

Safaricom's M-PESA and Austria's Mobilkorn represent successful models where the mobile operator controls and manages the payment system (Boer and de Boer 2010). These MNO-led systems typically rely on short message service (SMS)-based low-value payments. In some of the emerging payment schemes, the wireless carriers sometimes charge the mobile-enabled payment sent via text message to the consumer's mobile phone bill, as in the example of the Haiti earthquake relief efforts. In this example, consumers sent a text message to provide the desired donation amount to the selected charity in Haiti in a postpaid scheme

with the telecom remitting the funds immediately and collecting from the consumer after the fact. In this mobile-centric business model, human agents serve as a backbone for the ecosystem, providing a system of branchless banking, with users making transactions often without bank accounts.

Partnership models

In the partnership model, the financial institutions, mobile network operators and third-party service providers that make up the ecosystem partner and collaborate to provide payment services. In this model it may be possible to capitalize on each organization's respective strengths in terms of providing customer service, introducing innovation, and ensuring an environment of sound regulatory compliance. New payments solution providers face limited barriers to market entry with less stringent regulatory oversight and lower capital requirements than traditional bank counterparts. Companies such as PayPal, Obopay, and Cashedge, to name a few, have launched P2P payment services in the United States and abroad independently and in partnership with financial institutions. Other entrants in the mobile payments space, such as Visa and MasterCard, have announced numerous money transfer initiatives in 2010 in partnership with financial institutions and money service businesses like Moneygram and Western Union.

4. The mechanics of airtime exchange and mobile money

At some point in the early evolution of mobile payments, mobile network operators discovered that consumers in developing countries wanted the ability to fund other phone accounts, typically friends and family members with whom they exchange remittances. Oftentimes the recipient of the airtime would desire to cash out the value, as a means of delivering actual money (Beccue 2009). Telecoms responded to this consumer need and as a result, airtime is now being commoditized to replace cash and barter-based transfer systems in many countries that have traditionally relied upon informal value exchange systems. In addition to money transfers, in some countries, airtime is beginning to be used to pay for everyday goods and services, essentially transforming the mobile device into an airtime wallet (MMT Global Gateway 2008).

A user may fund the mobile transaction either by prepaying for airtime, thereby “topping up” the account and then using the value as a medium of exchange, or by establishing a stored-value account maintained by the carrier for the mobile phone holder, which can then be used for transactions. A mobile top-up request can be executed through the mobile operator’s network to debit the account of the payment initiator and credit the account of the recipient. Some networks permit roaming prepaid users to top up their accounts using vouchers purchased from other network operators, which may be impacted by foreign currency conversion charges.

Some telecommunication network providers also permit the transfer or resale of airtime credit on the mobile device, in a fashion similar to currency or other payment vehicles (ICT 2010). In this practice, the telecommunications firm authorizes its retailers to market and sell mobile phone airtime credits in return for a small fee, which permits consumers to sell surplus credits for unused minutes to a third party. This commoditization of airtime permits the operator to efficiently expand its agent network to remote and rural geographies typically underserved by mainstream financial services providers. Airtime credits provide a means for consumers to cover losses on unused airtime minutes by selling it to a third party at a discount or in exchange for cash or services. The agent or other airtime reseller purchases the airtime from the mobile network operator at a discount and then sells to mobile subscribers at full price, thereby gaining a revenue margin (Skoczkowski 2008).

In African countries that have witnessed rapid adoption of mobile payment services, MNOs have begun to provide discounts to customers for purchasing mobile airtime directly from the operator instead of through the retail agent to bypass distribution layers and their respective commissions. The success of this relationship is predicated upon the reduced overhead and distribution costs for the mobile operator along with the income from the airtime markup that goes to the reseller. The utility of this emerging airtime transfer model has contributed to its success in financially underserved markets such as in South Africa, Kenya, and the Philippines (ICT 2010). However, some discounting practices may occur informally, which limits the ability of transaction participants to confirm or dispute the terms of the transfer arrangement.

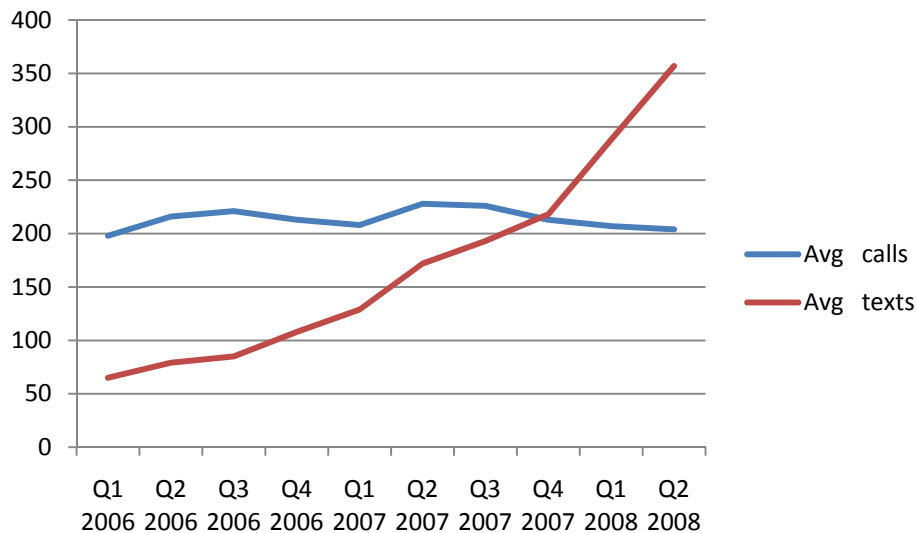
In the United States, the telecom firms have introduced pilots that allow customers to make payments for low-value goods and services with the charges posted to the customer’s phone bill to be postpaid. Carriers are beginning to provide credit for digital goods in computer games, ring tones, and for charitable donations. The Haiti earthquake relief effort engaged the participation

of major U.S. carriers and raised millions in donation payments, demonstrating a potential willingness on behalf of consumers and telecom firms to adopt the mobile payment method.

Technologies supporting mobile payment transfers

There are two primary technical protocols for conducting mobile money transfers, including short messaging service (SMS) and wireless application protocol (WAP), a basic form of Internet web-browsing similar to PC-based online banking. Recently, new downloadable applications for smart phones have been introduced for mobile P2P transfers, which may leverage SMS or WAP technologies, to facilitate consumer payments. While both protocols have been used in various pilots, SMS is emerging as the most common method for small-value P2P transfers because of its simplicity and compatibility for usage in a variety of mobile phones, including low-end handsets. Since almost all handsets manufactured today support SMS as a utility, there is an established user habit that supports expanded use. As figure 3 shows, SMS text messaging is so prevalent today that the typical U.S. mobile subscriber sends and receives more messages than telephone calls (Covey 2008).

Figure 3: U.S. mobile calls versus text messages



Source: Covey 2008

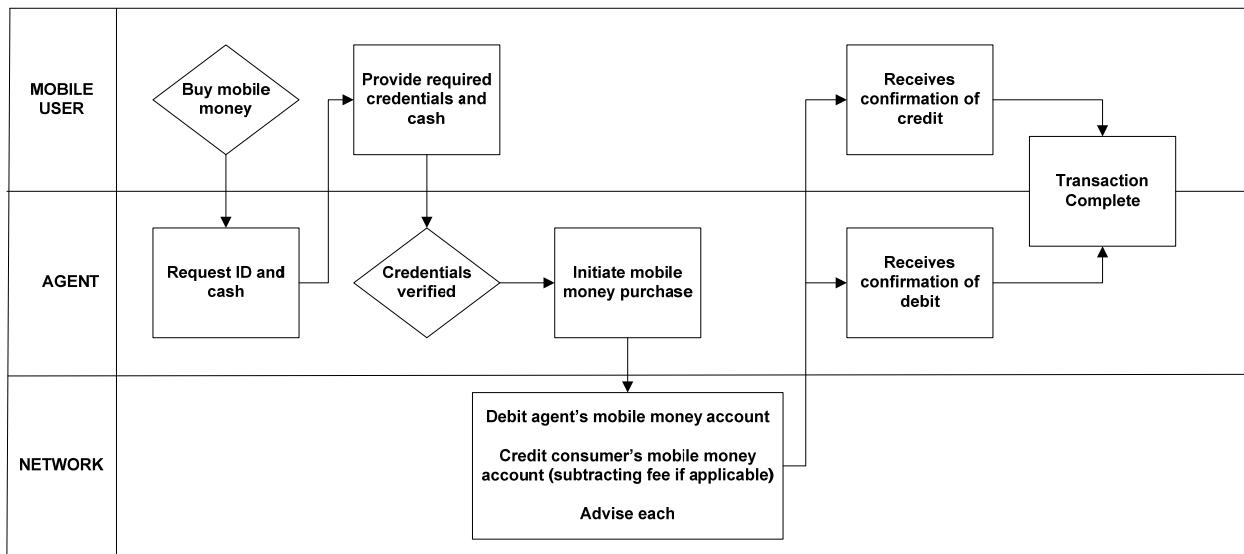
While the use of SMS is on the rise, it may not be widely adopted for retail payments in the United States (Crowe, Rysman, and Stavins 2010) because of security limitations due to

the fact that messages travel and are stored on the handset in plain text without encryption (Mahmoud, Abdel-latef, Ahmed, and Ahmed 2009). Today, the leading examples of U.S. mobile money service provider P2P offerings via SMS include Obopay and Paypal (Crowe, Rysman, and Stavins 2010).

Funding and transaction flows

The most basic mobile transfer schemes include the initial funding of the mobile account, typically with cash in emerging markets, but possibly with another payment vehicle such as a card-based payment and, conversely, the withdrawal of funds from a mobile account. Figure 4 illustrates a simple transaction flow for an MNO-based business model, such as M-PESA, in which the individual account holder is purchasing mobile money by depositing funds with an agent acting as an intermediary on behalf of the mobile network operator. Agents facilitate the movement of funds to (cash in) and from (cash out) the cell phone, depositing surplus cash in the MNO trust account or obtaining cash liquidity for operations by selling back airtime to the MNO.

Figure 4: Cash in: MNO model⁴



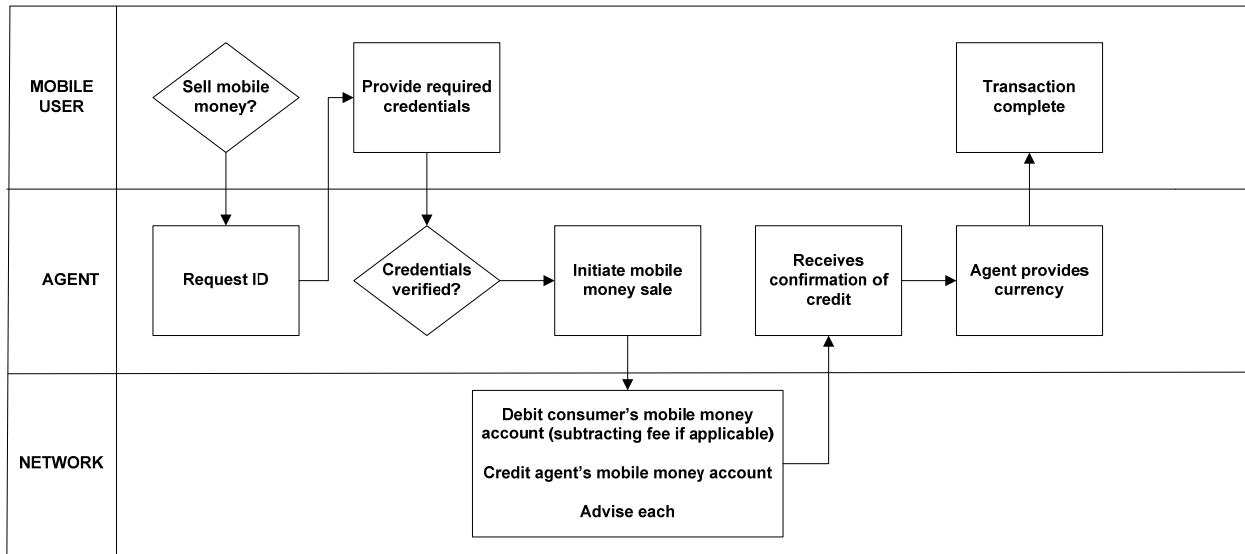
Source: KSMS, USAID, and BAH 2010

⁴ Figures 4–6 are simplifications of the more detailed transaction flow included in the source risk matrix.

Figure 4 depicts an example of a transaction in which an account holder purchases airtime from the agent, after producing identification documentation to allow the agent to verify his or her credentials and apply “know-your-customer” (KYC) due diligence procedures. Upon receiving the deposit (cash, in this instance), the agent credits the mobile money account, topping up the airtime or mobile money, with a corresponding debit to the account held in trust with the MNO. The agent sends a confirmation to the account holder via text messaging, and the transaction is complete. The mobile user has exchanged physical for virtual money, also known as e-float, which is now readily transferable to other mobile phone users who can likewise exchange it for cash with another agent in a separate location.

To better understand the payment transaction mechanics, it is instructive to view the M-PESA example. Safaricom accepts cash deposits from customers who have registered as M-PESA users (Jack and Suri 2009). Consumers register by providing an official form of identification such as a national ID card or a passport. Safaricom issues electronic credit measured in the same units as money in exchange for cash deposits and records the amount to the consumer’s account. This e-float is then available to transfer from one registered user to another using SMS texting, or alternatively cashed out at a later time. Initially, the M-PESA service was designed to fulfill remittance needs but has been repurposed to allow consumers to use the electronic credits or prepaid airtime for paying for other goods and services (KSMS, USAID, and BAH 2010). Figure 5 depicts a simple transaction flow for receiving cash from a cellular account. In this transaction, the consumer may have received a transfer as a gift or a salary payment, for example, and chooses to withdraw some or all of those funds in the form of cash currency through the MNO agent. In a reverse sequence to the transaction described above, the agent or airtime reseller purchases airtime from a consumer after verifying the consumer’s identification and credentials for authenticity and then debits the mobile account, with a corresponding credit to the agent’s account with the MNO.

Figure 5: Cash out: MNO model



Source: KSMS, USAID, and BAH 2010

Figure 6 illustrates an example of the funds flow in a P2P mobile money transfer. In this simple example, the network operator performs clearing functions for the sender and recipient of the funds in order to complete the transaction. The mobile user first sends a text message to instruct the mobile operator to execute a transfer; the message includes the dollar amount to be transferred along with the mobile phone number of the receiver. The mobile network operator then routes those messages through its networks, debits funds from the message sender's source account, such as a prepaid account in the subscriber's network or possibly a bank account or card, and then credits the destination account, also possibly a prepaid account in the subscriber's network. The mobile phone service provider typically transmits a text message back requesting the sender's personal identification number (PIN) to authenticate his or her identity and confirm the transaction.

impact on their economies resulting from influences on money supply, inflation, and interest rates (Pickens and Richardson 2007).

5. Mobile money risk environment

The risks that are inherent in all retail payments systems are also present in the mobile space, including money laundering, privacy and security, consumer protection, fraud, and credit and liquidity risks. In many countries, mobile payments are reducing the inherent risks in cash-based payment systems, improving transparency in fund flows and enhancing the potential for risk detection and mitigation as payment systems shift to a regulated environment. As mobile financial services evolve, however, there are numerous issues to consider for managing the risks that mobile phone-based payments may introduce. The large number of nonbank participants in the distribution of mobile payments, such as telecom firms and their agents, as well as technology vendors, may create additional risk considerations for payment regulators. In addition, there are other risks more unique to telecom firms that financial institutions and their regulators lack experience in detecting and monitoring. The multiple regulatory domains governing banking and telecommunications have been accustomed to operating autonomously from one another and will be challenged to learn how to effectively cooperate to provide oversight for mobile money transfers. The conjoining of these two previously distinct sectors will require a new cooperative regulatory environment across industries and geographical jurisdictions to employ risk-based and proportionate oversight.

Money laundering risks

As telecom firms engage in financial services across shared networks in cross-border jurisdictions, the benefits of mobile payments, ubiquity, and rapid settlement may also increase the risk of money laundering in mobile transfer services. With potential gaps in regulatory oversight, rogue actors may find it possible to evade detection by dividing a large transfer of funds into small ones using multiple mobile phones and accounts. This new landscape may require a service-based risk analysis by regulators to determine new approaches to the oversight of money laundering risk (Chatain, Hernandez, Borowik, and Zerzan 2008). Money-laundering and terrorism-financing mitigation programs require service providers to institute a meaningful KYC process that is trusted by all parties to the

mobile payment transaction. In the United States, anti-money laundering efforts have focused traditionally on high-value transfers,⁶ but in this brave new world, criminals may use mobile technology to evade detection by sending multiple small transfers, using multiple phones and accounts (GSMA 2009). Since mobile technology-enabled payments do not require the face-to-face interaction that takes place with traditional banking, a more opaque and anonymous experience is created that may permit the opportunity for criminal activity. This is increasingly important as mobile retail payments can occur rapidly and in cross-border environments.

There are numerous schemes for money laundering and terrorist financing that may migrate to the mobile channel, but “digital value smurfing”⁷ in particular poses a clear threat. In this scheme, runners—that is, the smurfs—bypass banks and regulatory reporting requirements by exchanging ill-gotten funds for digital value in the form of stored value. Smurfing used to involve stored-value cards but now the criminals rely on prepaid mobile credit on the cellular device. This scheme makes it possible for the proceeds of crime or terrorist financing to be transmitted over airwaves with the use of cellular phones (INL 2008). These opaque mobile transfers may move rapidly around the world in a digital format, immune to traditional regulatory oversight. Since there is limited expertise in identifying electronic payments crime in the communication systems, the potential for abuse should be considered.

Another issue is the implementation of money laundering risk controls and suspicious transaction reporting for telecom firms. Compliance with these anti-crime laws is a challenging proposition for telecoms because it represents unfamiliar territory to the telecom industry (GSMA 2008c). Similarly, because telecom regulatory oversight has not included financial services, knowledge of suspicious activity reporting may be limited. Compliance can be complicated further by the fact that in many countries nonbanks may not conduct customer due diligence and “know your customer” procedures because of regulatory restrictions (GSMA 2008d). In the United States, many mobile payment service providers are classified as money transmitters or money service businesses, requiring registration in

⁶ Bank Secrecy Act regulations, for example, require more complete information on transactions involving \$3,000 or more.

⁷ Smurfing is a term coined by the Asian Development Bank

individual states where they do business, as well as with the Financial Crimes Enforcement Network (FinCEN); but according to the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs, many of these firms do not register as required and there is limited enforcement of regulations that govern them (INL 2008).

Privacy and security

The concerns for securing the mobile channel mirror the risks seen in the online environment, including authenticating the consumer's identity and protecting transmission of data from interception enabled by viruses, malware, and phishing attacks. Anecdotally, the mobile environment to date has been relatively secure compared to the online channel where privacy and security of personal and business data is frequently compromised through the use of malicious computer viruses, identity theft, and phishing schemes. The diversity of platforms and wide range of operating systems make mobile phones less vulnerable to attack than personal computers. The recent surge in smart phone applications may introduce vulnerabilities to malware attacks, which may increase payments risk going forward as bad actors gain access to personal information stored in the handset or accessed through a phone application. Finally, the growing use of SMS as a common technology for sending a payments message may demand further examination of the need to strengthen data encryption technology.

As the mobile industry is in its infancy, the optimal solutions to devising a secure and resilient payment channel are still in play. Creating transparency is a key consideration in addressing security issues—when consumers have the ready ability to view transaction histories on their handsets, the risk of account fraud and other risks can be avoided or mitigated.

Consumer protections

Telecom-specific consumer protections in most countries, including the United States, were not created with the need for financial services regulation in mind. The limitations of traditional financial regulation for emerging mobile commerce may result in gaps in legal governance and ambiguity with respect to the responsibilities and liability among parties involved in the payment service. The mobile commerce environment will demand that

financial regulations be adapted to provide oversight for the proliferation of new services, business models, and nonbank service providers.

New regulatory policy will require a comprehensive understanding of the new risks that mobile transactions introduce to consumers, including lost payments through faulty transmissions, fraudulent transactions, identity theft, or criminal activity on the part of the mobile operator, agent, or other payment service provider. In the United States, for example, the applicability of payment law to mobile payments is unclear since MNOs may not be required to provide consumer protections equivalent to those of the banking industry.

For example, Regulation E governing electronic fund transfers includes any entity that holds consumer accounts or issues a payment access device and provides electronic fund transfer services. While mobile money service providers in the United States typically comply voluntarily with Regulation E and other consumer protection laws, actual enforcement authority is fragmented, according to the state authorities where they are licensed. In the absence of Regulation E protections, it is unclear who will assume responsibility or liability for dispute resolution for billing errors, misdirected payment messages, fraudulent charges stemming from identity theft, or compromised mobile accounts resulting from lost handsets when authentication controls are intercepted. Some of these issues may fall within the scope of the Federal Communications Commission's Truth in Billing Requirements, but enforcement at this nascent stage will lag product and service deployment.

The GSMA provides general guidance for establishing regulatory environments for MMT that underscores the need to coordinate the consumer protection efforts of both the telecom and financial services industry. The cellular telecommunications trade association has also published best practices for telecoms in financial services as a proactive measure, in order to guide the offering of safe and trusted mobile payments and maintain public confidence.

Roaming fraud

Recent successes in global-standards setting to promote interoperability among carriers⁸ have simplified the ability for mobile users to roam across geographic markets. The roaming agreements used by international operators to facilitate voice transfers can now be used to

⁸ GSMA has been active in developing international standards for interoperability in MMT.

send data in the form of cross-border payments. However, wireless data transmissions may be vulnerable to access by unauthorized parties who identify some means to intercept the communication between mobile devices. The growth in wireless telecom services has led to an increasing number of roaming agreements between telecommunications companies in different countries, enabling the transmission of international remittances via mobile phones. Roaming fraud represents a potential threat to the security of cross-border mobile payments. GSMA has recommended that near-real-time roaming data exchange technology be implemented for all GSMA members in order to reduce the occurrence of roaming fraud. The technology involves faster roaming-activity reporting and requires operators to send roaming data to partners within a prescribed time limit. The data includes key call information that can be analyzed if it is received quickly, in sufficient time to detect and mitigate roaming fraud.

Credit risk

Credit risk may emerge in a postpaid scheme whereby the transaction is applied to the user's phone bill to be paid later. Possibly because of their lack of experience in managing credit risk associated with financial services, telecoms in global markets have largely focused on providing prepaid services in order to manage liquidity and mitigate risk, particularly in telecom-led models that do not rely on a bank partnership. In most countries, nonbank payment service providers are prohibited from accepting consumer deposits or using funds in financing payment activities, which serves to protect the consumer and limits financial system risk (GSMA 2009). For example, Safaricom's M-PESA mitigates credit risk by collecting prepaid funds from agents. Safaricom deposits into a trust account managed by a leading Kenyan commercial bank, which provides the legal protection for consumers.

In the United States, new P2P services typically involve an established payment vehicle such as a depository account at a financial institution or a credit card to fund the mobile payment. Programs in which the carrier posts charges to the consumer's phone bill to be postpaid have been largely limited to micropayments for charitable donations, as in the Haiti relief effort discussed earlier, and for small purchases for ring tones and virtual goods in online games. There is no current evidence to suggest that carriers have an appetite for managing credit risk in MMT.

6. Mitigating risk in mobile money transfer systems

Since the success of any payment system is predicated on ubiquity, convenience, and trust, it is necessary to address emerging risk issues in order to maintain public confidence in mobile money. The risk of anonymity in mobile payments may require new authentication technologies such as voice recognition and fingerprinting to verify identification and to employ appropriate know-your-customer programs, particularly at vulnerable points of a transaction when cash withdrawals may be conducted. The use of more sophisticated control systems to flag unusual account activity, based on a customer's user profile, will be needed to detect increasingly complex money laundering schemes. Since mobile financial transactions occur rapidly, with funds being sent and received in fractions of a second, payment service providers may not detect suspicious activity in time to suspend a transaction. As mobile commerce advances, it will be necessary for mobile payment service providers to establish integrated systems of internal controls that respond quickly to suspicious activity.

The risk of inadequate regulatory oversight stemming from a lack of understanding about the risk exposure inherent in new mobile payment innovations- results in payment system vulnerabilities. Education and collaboration across organizational jurisdictions and the telecom and financial services industries will be necessary to detect and mitigate criminal activity, fraud, and other payment system risks.

Certain aspects of mobile handset technology may be leveraged to provide more secure transactions—by using identification tools to authenticate the user, for example, thereby reducing the risk associated with anonymous transactions. Digital wallets contained in the mobile handset that are provisioned with a secure element and empowered with multifactor authentication may also provide a more secure payment environment in the future. Location-based services available in smart phone applications may also help payment service providers to authenticate the credentials of mobile users engaging in payments transactions. Finally, transaction limits imposed by carriers and financial institutions based on the customer profile and historical usage can mitigate the risk of unauthorized payments.

7. Policy and regulatory considerations

Mobile money merges the regulatory environments of both telecommunications and banking into a new paradigm that ultimately demands a collaborative dialogue to balance intervention for risk mitigation with market innovation. The primary goal of prudential regulation is to protect the interests of consumers and to enhance the integrity of a payment system by ensuring that participants have sound means for identifying, measuring, and managing business risk (GSMA 2008d). As mobile commerce evolves, gaps in legal and regulatory frameworks that ensure effective consumer protections and payment system integrity should become evident and will need to be addressed. This is a formidable task in an ecosystem comprised of new nonfinancial services providers such as telecoms, payments service providers, and payment application vendors, each with the ability to transact in a cross-border environment that spans different legal and regulatory jurisdictions.

The regulatory landscape is likely to evolve and to differ by country and business model. As a result, it will be important for telecom and financial regulators to coordinate a risk-based approach to understanding risks in mobile money transfer services and establishing oversight for mobile money and payment regulation. For example, a business model that involves deposit taking demands higher levels of consumer protections accompanied by regulatory oversight to ensure that the deposit taker and payment service provider are operating under safe and sound principles. In theory, the regulator should exercise sufficient control over the payment service providers such that public trust in the payments system ensures sufficient critical mass in adoption necessary for a safe and effective payments network.

Looking to the future, policy and regulation on an international basis will need to consider shared infrastructures that work harmoniously to address emerging risks in retail payments while recognizing the benefits of innovation and increased financial inclusion. Ultimately, mobile money transfer services will demand a paradigm shift in the way retail payment systems are analyzed from a regulatory oversight perspective, first within a country view and then in a cross-border environment. The new regulatory ecosystem for mobile P2P will need to clearly define the authority for supervising the payment provider. The oversight entity must have the authority to ensure that personal data is protected and that payment service providers bear responsibility and liability for customer relationships and provide reliable service.

The regulatory environment for mobile is complicated by different geographic jurisdictions, varying degrees of involvement by different central banks, and, most importantly, the conflict between regulatory systems that oversee banking versus telecommunications industries. The lack of standardization in this emerging industry segment means that no roadmap exists for implementation in countries where security and registration processes may be lacking. Obvious concerns are rising with regard to money laundering both domestically and cross-border, in addition to other frauds such as identity theft.

Cross-border fund transfers in the telecom-centric model pose the greatest regulatory challenges for retail payment systems as bank regulators have no jurisdiction over the actions of telecom firms. On the other hand, telecom regulators are unfamiliar with the risks and fraudulent schemes perpetrated in retail payments or may determine that customer protections for payments extend beyond their scope of authority and, as a result, collective regulatory oversight may provide insufficient governance. Furthermore, the absence of bank participation in telecom-centric business models raises questions regarding responsibility and authority for ensuring customer protections and efficient funds settlement.

One of the growing challenges presented by payment innovations is the creation of new laws and rule sets that provide different protections according to the payment type. This challenge is further complicated as payments converge and assume different formats along the supply chain. For example, a payment initiated via a credit card on a mobile device is subject to error resolution procedures and consumer protection standards established by the card networks. Similarly, Regulation E covers electronic transactions initiated from a bank deposit account, but that provision may not extend to airtime stored on the mobile device or with the MNO.

8. Conclusion

The ubiquity of mobile technology is advancing the adoption of mobile money transfer services for people in developing countries, providing a safer and more efficient environment for conducting transactions and improving financial inclusion. In developed countries, the increased functionality of smart phones with innovative payment applications is driving the potential development of new P2P services, as evidenced from pilot trials and recent partnership initiatives with traditional money transmitters and mainstream financial institutions with wireless carriers. As geographic borders lose their relevance, these services are likely to migrate to the United

States as they represent a viable alternative for underbanked consumers, immigrants, and financially mainstream consumers seeking an electronic P2P payment solution.

In the interest of preserving the integrity and safety of domestic and cross-border retail payment systems, industry stakeholders, policymakers, and regulators should cooperatively share information about service developments and consider potential gaps in regulation, with the following considerations in mind:

- ***The new mobile payments landscape requires the establishment of a dialogue between regulatory authorities for financial services and telecom sectors.***

New mobile financial services introduce unanticipated risk vulnerabilities that are not well understood by regulators of converged industries. Consequently, financial and telecom sector regulators need to understand the risks involved in MMT services and keep an eye toward establishing new regulatory concepts of electronic money and payment regulation. A program for routine communication should be established to ensure that regulators understand payment system risk issues and provide effective risk-based supervision for payment service providers.

- ***An oversight infrastructure for mobile payments, including the financial services of telecom firms, should be established either in partnership with existing authorities or as a new organization.***

While consortia and trade associations have acted proactively in providing guidance for telecoms engaged in financial services, there is currently no industry overseer to enforce that guidance and police rogue actors. In order to protect the integrity and ensure continued security of retail payment systems in the United States, an oversight framework for telecom-led financial services is needed to mitigate the risk of abuse, fraud, and other illegal activity. This oversight might be established through the creation of a routinely convening workgroup represented by applicable regulatory authorities, or through the delegation of a new organization with specialized expertise and understanding of the unique and dynamic risk issues in mobile services.

- ***Cross-border mobile remittances may require improved customer-data sharing on an international basis by central banks, regulators, and law enforcement organizations, as money transfer businesses are established in multiple geographic and legal jurisdictions.***

The increased interoperability among shared carrier networks is facilitating data transmission across geographic borders, whereby information about the parties to the mobile money transaction may go undetected by regulators and central banks of customers in the originating or receiving countries. International roaming and the wireless nature of financial transfers may create opportunities for money laundering abuse and other unforeseen financial crimes. The anticipated growth in mobile-enabled remittances requires that regulators contemplate a new environment of international cooperation and sharing of customer data and analysis. Regulators and other investigators of financial crimes also share a heightened need to understand the data processing capabilities in smart handsets and the complexities inherent in the multi-dimensional relationships among all participants in emerging m-commerce business models.

- ***Mobile payment service providers in the United States should be required to establish programs to mitigate the risk of money laundering.***

As mobile networks expand through provider partnership agreements, the strategies used to detect the risks of fraud such as identity theft and money laundering will need to be more proactive and sophisticated. Evidence needed by law enforcement agencies to prosecute financial crimes in the future now exists in a digital versus physical state, requiring new methods for detection and monitoring data flows. All service providers, including telecoms, should establish anti-money laundering and KYC programs commensurate with the risk inherent in their mobile financial service offerings. Carriers should impose transaction limits for customer activity and use customer behavior to flag suspicious activity and avoid unauthorized transactions.

- ***Converged regulatory authorities should examine consumer protection risks for potential gaps in regulatory oversight.***

The applicability of Regulation E protections to stored-value payments should be reexamined in the context of mobile money transfers to prevent consumer confusion in error resolution

scenarios. Consumer protection regulation should clearly delineate which service provider is responsible and whom to contact when a transaction is improperly executed. The consumer protections for financial services should be expanded in scope to include nonbank service providers like telecom firms and money transmitters.

As domestic and international mobile money transfer services grow more prevalent, discussions on risk management and payment system integrity will be imperative. Dialogue with all industry stakeholders, including regulators and policymakers, is essential to creating an environment in which payments risk issues are clearly understood. In this way, risk-based regulation that is proportionate with the need to encourage innovation and efficiency in retail payments can be best achieved.

References

- Bangens, Lennart, and Bjorn Soderberg. 2008. "Mobile Banking—Financial Services for the Unbanked?" SPIDER, The Swedish Program for Information and Communication Technology in Developing Regions. http://www.spidercenter.org/files/m-banking_study.pdf.
- Beccue, Mark. August 27, 2009. *Nokia Money—An Uphill Battle* (blog). http://webcache.googleusercontent.com/search?q=cache:EckLeLEgO_AJ:www.abiresearch.com/research_blog/670+http://www.abiresearch.com/research_blog/670&cd=1&hl=en&ct=clnk&gl=us
- Boer, Remco, and Tonnis de Boer. 2009. *Mobile Payments 2010: Market Analysis and Overview*, version 1.01. Innopay. https://www.ebaportal.eu/Download/Research%20and%20Analysis/2010/Mobile_payments_2010_Innopay.pdf.
- Bourreau, Marc, and Marianne Verdier. 2010. "Cooperation for Innovation in Payment Systems: The Case of Mobile Payments." Economix Working Paper 2010-05, Université de Paris Ouest Nanterre La Défense, Nanterre, France. http://economix.u-paris10.fr/pdf/dt/2010/WP_EcoX_2010-05.pdf.
- Chatain, Pierre-Laurent, Raul Hernandez-Coss, Kamil Borowik, and Andrew Zerzan. 2008. "Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing." World Bank Working Paper No. 146. World Bank, Washington, D.C.
- Covey, Nic. 2008. "In U.S., SMS Text Messaging Tops Mobile Phone Calling." *nielsenwire online+mobile* (blog). http://blog.nielsen.com/nielsenwire/online_mobile/in-us-text-messaging-tops-mobile-phone-calling.
- Crowe, Marianne, Marc Rysman, and Joanne Stavins. 2010. "Mobile Payments in the United States at Retail Point of Sale: Current Market and Future Prospects." Public Policy

Discussion Paper No. 10-2, Federal Reserve Bank of Boston.

<http://www.bos.frb.org/economic/ppdp/2010/ppdp1002.htm>.

Edgar, Dunn & Company (EDC). 2009. "Realizing the Full Potential of Mobile Commerce: Orchestrating Mobile Payments and Money Transfers."

<http://www.paytriot.net/files/ampDRIVE/1/mCommerce9050301.pdf>

Federal Deposit Insurance Corporation (FDIC). 2009. "FDIC National Survey of Unbanked and Underbanked Households." http://www.fdic.gov/householdsurvey/executive_summary.pdf.

GSM Association (GSMA). 2007. Regulatory Framework for Mobile Money Transfers.

<http://www.mobilemoneyexchange.org/Files/8e31752b>.

———. 2008a. "Introduction to MMT."

http://www.gsmworld.com/documents/GSMA_Introduction_to_MMT_0908.pdf

———. 2008b. "Outlook for Mobile Wallets and Mobile Financial Services: Results of EDC–GSMA Mobil Financial Services Survey 2007."

———. 2008c. "Understanding Financial Regulation and How it Works."

http://www.gsmworld.com/documents/GSMA-Understanding_Financial_Regulation_0908.pdf.

———. 2008d. "An Introduction to the MMT Regulatory Environment." Mobile Money Transfer project. <http://216.239.213.7/mmt/regulatory.asp>.

———. 2009. "Mitigating the Risks that Accompany Mobile Money." *Mobile money for the unbanked: Quarterly update* 1 (March): 35–36.

http://www.gsmworld.com/mmu/mmu_quarterly_update.pdf.

ICT Regulation Toolkit. 2010. “Examples of Financial Services Using Mobile Phones.”
<http://www.ictregulationtoolkit.org/en/PracticeNote.3096.html>.

International Telecommunications Union (ITU). 2009. World Telecommunication/ICT Indicators Database. http://www.itu.int/ITU-D/ict/statistics/material/graphs/Global_mobile_cellular_00-09.jpg

Jack, William, and Tavneet Suri. 2010. “The Economics of M-PESA.”
<http://www.mit.edu/~tavneet/M-PESA.pdf>

Jenkins, Beth. 2008. “Developing Mobile Money Ecosystems.” Washington, D.C.: IFC and the Harvard Kennedy School. http://www.hks.harvard.edu/m-rcbg/CSRI/publications/report_30_MOBILEMONEY.pdf.

Kenya School of Monetary Studies; United States Agency for International Development; and Booz, Allen, and Hamilton (KSMS, USAID, and BAH). July 2010. “Mobile Financial Services Risk Matrix.” <http://www.docstoc.com/docs/48358080/Mobile-Financial-Services-Risk-Matrix-100723>.

Mahmoud, Tarek M., Bahgat Abdel-latef, Awny A. Ahmed, and Ahmed M. Mahfouz. 2009. “Hybrid Compression Encryption Technique for Securing SMS.” *International Journal of Computer Science and Security* 3 (6): 473–81.
<http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume3/Issue6/IJCSS-169.pdf>.

Maurer, Bill. n.d. “Retail Electronic Payment Systems for Value Transfers in a Developing World.” Accessed Sept. 9, 2010, http://www.anthro.uci.edu/faculty_bios/maurer/Maurer-Electronic_payment_systems.pdf.

MMT Global Gateway. 2008. “MMT Explained, Part 2: Mobile Wallets.”
http://www.mobile-money-transfer.com/mmt_global/mmtex2.phpMyAdmin=513c4b9414a6t38cff6f1.

Pickens, Mark, and Brian Richardson. 2007. "Mobile Wallets and Virtual Currencies," in "Financial Services," *ICT Update* (36). <http://ictupdate.cta.int/en/Feature-Articles/Mobile-wallets-and-virtual-currencies>.

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

Robertson, Beth. 2010. "P2P Will Hit It Big in 2010," in *10 Trends that Will Shape Banking, Payments, and Security in 2010*. Javelin Strategy & Research.

Skoczowski, Lucas. 2008. "Mobile Money: Transforming the Wireless Paradigm." *International Billing OSS*.
http://www.billingoss.com/articles/mobile_money_a_global_opportunity_redknee.htm

U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs (INL). 2008. "Mobile Payments—A Growing Threat." *International Narcotics Control Strategy Report* (March). <http://www.state.gov/p/inl/rls/nrcrpt/2008/vol2/html/101346.htm>.