

Country Policy Note
International Experiences of Mobile Banking Regulation

Catia Batista, Felix Simone, and Pedro C. Vicente
IGC Mozambique

January 2012

Introduction

The introduction of mobile banking (m-banking) services in both high and low-income countries has revolutionized traditional notions of ‘banking’. In low-income countries in particular, m-banking is regarded as an opportunity to bring financial services to the unbanked poor who are not a profitable target for commercial banks.

The promise of m-banking lies in the fact that access to these services requires no more than access to a widely available and inexpensive technology such as mobile telephony, even for poor uneducated individuals who are typically marginalized by traditional banking providers. This promise has been materialized most successfully in Kenya, where Safaricom’s M-PESA started in March 2007 and, by September of 2009, over 8.5 million Kenyans had registered to use the service and US\$3.7 billion (10 percent of Kenya’s GDP) had been transferred over the system.

The success of Kenya’s M-PESA has raised the question of how most effectively to regulate mobile money services. As pointed by Ivatury and Mas (2008), mobile network operators (MNOs) like Safaricom are well-placed to reach customers with affordable financial services due to their existing customer base, marketing capabilities, physical distribution infrastructure, and experience with high-volume, low-value transactions (e.g., the sale of airtime). However, regardless of this potential to bring financial services to low-income populations, regulators are often reluctant to permit MNOs to directly contract with customers for the provision of financial services.

As pointed by Tarazi and Breloff (2010), taking redeemable money from the public is very close to accepting public deposits - an activity almost always reserved for prudentially regulated financial institutions, such as commercial banks. Funds kept with such banks are protected by strict prudential requirements (and related supervision) to ensure systemic stability and deposit security, and these same requirements would typically apply to electronic value issued by banks in exchange for deposited funds. In contrast, nonbanks are rarely subject to the kind of prudential regulation that

applies to banks, so when nonbanks issue e-money, regulators are understandably concerned about ensuring adequate protection for customer funds.

Nevertheless, as policy makers around the world recognize the potential for nonbank e-money issuers to significantly promote financial services among low-income populations, a number of regulations have been approved, permitting nonbanks to contract directly with customers for the issuance of e-money. For instance, in Cambodia and Kenya the approach has been to act on an ad hoc basis through “no objection” letters and conditional approvals of m-banking services. From Afghanistan to the Philippines, West Africa to the European Union, jurisdictions around the world have adopted regulation that enables a leading role for nonbanks - while mitigating the risks presented by the involvement of a service provider that is not subject to full prudential regulation.

In this note, we will present a typology of m-banking implied risks and corresponding regulation, followed by a broad description of the international experiences of m-banking regulation in countries such as Afghanistan, Brazil, Cambodia, India, Indonesia, Kenya, Malaysia, Philippines, South Africa, and UEMOA¹, based mainly on the work by Lyman et al. (2008) and Tarazi and Breloff (2010). We will not address issues related to the telecommunication side of m-banking regulation, which Alampay (2010) reviews in detail.

What is m-banking?

According to Alampay (2010), m-banking is a form of electronic banking (e-banking) delivered via mobile networks and performed on a mobile phone. E-banking itself is defined in Basel (1998) as ‘the provision of retail and small value banking products and services through electronic channels; these include deposit taking, lending, account management, the provision of financial advice, electronic bill payment and the provision of other electronic payment products and services, such as electronic money.’

Following Tarazi and Breloff (2010), our working definition of electronic money (e-money) refers to electronically recorded value issued against the receipt of equivalent value. Once issued, this electronic value may be redeemed for cash, transferred between customers, or used by a customer to make payments to merchants, utility companies, and other parties. E-money may be issued by banks or nonbanks, where ‘bank’ refers to any supervised and prudentially regulated financial services institution.

¹ UEMOA is the acronym in French for West African Economic and Monetary Union. It includes Benin, Burkina Faso, Côte d’Ivoire, Guinea-Bissau, Mali, Niger, Senegal, and Togo.

Finally mobile money (m-money) is described as a form of e-money that ‘allows for mobile phone subscribers – whether banked or unbanked – to deposit value into their mobile account, send value via a simple handset to another mobile subscriber, and allow the recipient to turn that value back into cash easily and cheaply’ (GSMA, 2009).

How to regulate m-banking? Risks and regulation

Banking regulation aims at preventing known asymmetric information problems, such as moral hazard created by the existence of a lender of last resort or adverse selection of borrowers. In this way, it is hoped that risks to the financial system and to the overall economy are mitigated. An additional function of banking regulation is to control the creation of money by credit providers.

The regulation of m-banking pursues the same broad objectives as the regulation of traditional banking, regardless of whether the m-banking providers are ‘banks’ or not. Klein and Mayer (2011) provide a typology aimed at isolating the fraction of risks associated to m-banking activities out of all risks associated with a traditional financial organization. We next summarize the Klein and Mayer (2011) risk and implied regulation² typology adding some considerations by other authors, as indicated.

Exchanging forms of money

When m-money is exchanged for cash, the parties to the exchange begin by getting confirmation of the transfer by SMS and, once that information has been received, the exchange can proceed. The exchange functions of m-banking can be handled through normal commercial law dictating the contractual relationship between customer and cash merchant, between the merchant and the wholesaler and between the merchants, wholesalers and MNO. Beyond this, the pure element of exchange does not raise financial risks requiring the imposition of prudential regulation.

Monetary concerns arise when competing currencies are issued by different parties, the key concern being whether the monetary authorities lose control over the money supply. When exchanging cash

² Note our working definition of the different types of regulation, following Klein and Mayer (2011): ‘Business conduct regulation’ encompasses such fields as consumer protection and anti-money laundering measures. The most basic question is whether to rely purely on normal commercial law and the means for redress it provides, in which case buyers of services are at risk and, if hurt, they need to seek redress via normal dispute resolution procedures. ‘Prudential regulation’ may require more substantial discretion. Core tools are capital adequacy and liquidity requirements, but also rules governing risk-taking on the asset side. For example, regulators may limit credit growth or require certain loan-to-value ratios. It is a mantra of prudential regulation that it should be rule-based as far as possible but in practice substantial discretion may be required particularly when assessing system-wide risks, namely macro-prudential regulation.

for m-money, money is not being created; one form of money (cash) is simply being exchanged for another. Nevertheless, by facilitating the exchange and allowing transactions to occur at distance through mobile connections, it may affect the velocity of circulation and therefore the relation between the money supply and nominal output and income. Monetary authorities need to be aware of this and the likely impact of mobile banking on transactions. However, by making transactions more transparent and the determination of aggregate levels of expenditure more readily measurable, mobile banking may make it simpler for monetary authorities to observe and measure changes in the velocity of circulation.

The monetary authorities may thus require the account provider to provide regular information about volume and structure of payment transactions.

Keeping money safe

A record needs to be created that establishes who owns the account and how access is gained to the account. In addition, an account requires rules on how the records are maintained and how the owner is informed about transactions and the balance on the account. The key to any safe-keeping function is regulation that assures the integrity of the system and requires procedures to be subject to audit (Makin, 2009). Back-up systems are needed to ensure that account information can be recovered in case of physical destruction or theft.

An additional requirement related to safe-keeping is the registration of m-banking accounts. Know-your-customer (KYC) procedures are a key element in the fight against money laundering and terrorism financing. KYC procedures typically require customers to present valid identification and providers to verify the documents and store copies. They establish the identity of the owner, process the request for account opening and perform checks required by Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulation.

These requirements can present obstacles to financial inclusion in several ways. First, it may constitute an obstacle to poor people who do not have ready access to documents, especially in countries with no national ID scheme. Second, extra operational requirements may impose a higher account opening cost for banks, to the point of making low-balance accounts economically unprofitable. Finally, it may present logistical problems to rural retail outlets which do not have access to copy machines or lack stable electricity supply.

The notion of proportionate or risk-based KYC procedures is well established within the Financial Action Task Force (FATF)³ principles and it should enable an easy, cheap entry proposition for previously unbanked people. As customer balances and transactions volumes grow, the KYC and security arrangements can be tightened progressively.

Transferring money

Poor people often transport their money themselves or give it to friends or to a bus driver to take to their relatives. Safer and cheaper means of transport are hugely in demand. The issue is reliability and integrity of the transport mechanism. The telecommunications provider may be subject to special regulations arising from consumer protection and competition policy concerns, but specific financial regulation is not obviously required for the movement of money across physical distance.

A special case arises when m-money is moved across national borders. This may be of concern where monetary authorities seek to implement some form of control on the movement of capital. The reason for concern is not that the physical transport risks require prudential regulation but that local currency may be exchanged into foreign currency. Currency control regulations may thus be an issue and restrict the transfer of m-money across borders - although in practice the amounts being transferred in m-transfer systems tend to be below the limits imposed on the transfer of cash or other assets for capital control purposes.

The account owners involved need to be informed about whether the instructions have been carried out and they need to receive verification. Systems are thus required to insure the integrity of this process including identification of the parties involved and, depending on the degree of integrity sought, special passwords and other identifiers may be required. To protect information 'in transit' varying degrees of encryption may be required and measures to prevent and detect attempts to steal information, for example, via hacking.

Over and above normal contractual relations, the form of regulation that is required in relation to transportation is therefore conduct of business. Prudential regulation is not required.

Investing money

The exchange of money, safe-keeping and transfer can all happen without involving lending or other investment. In this case, the money of depositors is not invested and not subject to any investment

³ The FATF sets international AML/CFT standards and oversees compliance monitoring.

risk. Prudential banking regulation only applies to ‘deposit-investing’ institutions, not to purely ‘deposit-taking’ ones.

Compared to a model where the account provider keeps deposits in a safe-deposit box, an MNO that holds deposits in an amount equivalent to the m-money value it provides is performing a rudimentary lending function as banks are free to on-lend these deposits. The risk of such an investment is thus equivalent to the risk of a deposit in banks that are subject to supervision by the relevant regulator.

Hence, where deposit in banks is allowed or required, regulation may limit deposit options to the safest of instruments and insist on some level of diversification among invested banks.

In summary, as stated by Alexandre et al (2011), ‘a deposit-taking institution that does not on-lend funds and instead commits to place 100% of deposits raised in one or more pooled accounts in supervised banks does not give rise to prudential or liquidity risks; indeed, it is not that they are prudentially unregulated, as in fact they are subject to the highest level of prudential regulation imaginable: a 100% reserve requirement; in this manner, regulatory and supervisory concerns can be circumscribed to operational and technology risks’.

A final note is deserved by a couple of emerging regulatory questions raised by Tarazi and Breloff (2010). According to these authors, regulators are currently confronting questions about whether e-money accounts should enjoy the same benefits and protections as bank accounts. In particular:

Should e-money issuers be permitted to pay interest on e-money accounts?

Most regulatory authorities consider the payment of interest a feature of a bank deposit. However, this distinction between payments and banking activity is of questionable legal merit. Collecting repayable funds from the general public is arguably a ‘deposit’ regardless of whether it is collected by a bank or payment services provider (Tarazi, 2009). As e-money is increasingly used as a savings vehicle, and as customers naturally desire to earn interest, regulators may be forced to re-evaluate perceived risks and reconsider permitting nonbank e-money issuers to pay interest earned on pooled accounts.

Should the funds backing the e-float be covered by deposit insurance schemes?

In most developing country frameworks, e-money is not considered a deposit and, thus, is not covered by deposit insurance. However, as discussed, to the extent underlying customer funds are kept in bank accounts, such funds are exposed to the risk of bank failure. Even in circumstances where deposit insurance exists, the value of pooled accounts is often much higher than the applicable deposit insurance coverage limits. As electronic value offerings grow in volume and popularity, and as evidence mounts that e-money schemes are increasingly being used as savings vehicles, regulators

may want to consider extending deposit insurance protection at the level of individual customer e-money balances or alternatively raise the ceiling for pooled accounts. Many developed countries already provide such deposit protection. The United States, for example, expressly characterizes the funds underlying stored-value cards as ‘deposits’ covered by deposit insurance as long as such funds are placed in an insured institution (FDIC, 2008).

Specific m-banking regulation issues and experiences

We now turn to providing a broad description of m-banking regulation efforts in a variety of different countries and contexts. This discussion closely follows the work of Lyman et al. (2008) and Tarazi and Breloff (2010).

Fund safeguarding

Fund safeguarding measures are aimed at ensuring that funds are available to meet customer demand for the cashing out of electronic value. In countries that have permitted MNO issuance of e-money, regulators have typically addressed fund safeguarding concerns by requiring that such issuers maintain liquid assets equivalent to the total value of the customer funds collected (i.e., the total value of electronic value issued and outstanding, also known as the ‘e-float’). Liquid assets are most often required to be maintained as accounts with a prudentially regulated bank but sometimes they may be maintained as other safe assets, such as government securities, although such securities may not always be as liquid as bank accounts. Note that this is a more stringent requirement than imposed on deposit-taking financial institutions, which are typically subject to reserve requirements mandating only some small portion of overall deposits to be kept in liquid form (typically cash) to satisfy potential depositor claims. Liquidity requirements exist in Indonesia, Afghanistan, the Philippines, Cambodia, Malaysia, India (in connection with prepaid payment instruments), and others. In Kenya, Safaricom maintains fund liquidity by placing collected cash in prudentially regulated banks pursuant to a prior agreement with the Central Bank of Kenya (CGAP, 2010).

Liquidity requirements are sometimes reinforced by restrictions on the use of customer funds by the nonbank issuer — for example, by prohibiting issuers from using the funds to finance operating expenses. In Malaysia, for example, issuers are expressly prohibited from using such funds for any purpose other than cashing out against electronic value or executing funds transfers to third parties pursuant to customer request. Other limitations on the use of customer funds are more indirect. The Philippines expressly prohibits nonbank issuers from engaging in the extension of credit, effectively ensuring customer funds are not endangered through intermediation by an entity that is not fully prudentially regulated.

Diversification of e-float fund holdings

Funds held in prudentially regulated banks are not risk-free. When banks fail, they cannot always pay their depositors, often leaving small value depositors to pursue recovery through deposit insurance schemes. In countries with weak banking sectors there is an even greater risk of bank failure coupled with the possibility that no deposit insurance exists. However, even where deposit insurance exists, the value of pooled accounts held by nonbank e-money issuers is typically much larger than deposit insurance coverage limits, leaving the issuer and customers more exposed in the case of bank failure. Afghan regulators sought to minimize the risk of bank failure by requiring that when any e-money issuer's e-float exceeds a specified amount, no more than 25 percent of the cash funds backing such float may be held in a single financial institution. No regulations outside of Afghanistan expressly require such diversification as protection against bank failure, though the trustee of the M-PESA trust account in Kenya independently chose to minimize risk by dividing the cash backing M-PESA's e-float among more than one bank.

Fund isolation

Liquidity requirements, coupled with other restrictions on use, may prove to be effective mechanisms for fund safeguarding. However, funds may still be at risk if the customer's ownership of the funds is unclear. While funds can be safeguarded in accounts of prudentially regulated institutions, such funds are often pooled and held in the name of the issuer — not in the name of the customers. Therefore, the nonbank issuer is often the legal owner of the accounts, thereby making the underlying funds vulnerable to claims by the issuer's creditors if the issuer goes bankrupt or if accounts have been used as collateral to secure specific debts of the issuer.

In Kenya, M-PESA customers are isolated from creditor claims and other ownership threats by the use of a trust account that is administered by a third-party trustee and held for the benefit of M-PESA customers. However, other jurisdictions, particularly those jurisdictions where trust accounts do not exist, do not provide the same protections. Indonesia, for example, mandates certain fund safeguarding measures, but the bank accounts holding the funds are in the name of the nonbank issuer. This is also the case in practice in Cambodia, although Cambodian regulators are reportedly considering regulation to replicate the protections afforded by the trust account structure in Kenya. Malaysia, Indonesia, and Cambodia require that customer funds be deposited and managed separately from the issuer's working capital funds. However, while such separate management facilitates supervision of an issuer's compliance with fund safeguarding requirements, it does not isolate customer funds from claims by the issuer's creditors.

Agents

Brazil, India, and Kenya provide illustrative examples of the range of current regulatory practice with respect to the use of agents. In Brazil, nearly any retail establishment with a cash drawer can act as a banking correspondent. But the central bank notes some restricting conditions, namely that a bank is liable for the actions of its agents. By contrast, the Reserve Bank of India's 'Business Correspondent and Facilitator Circular,' issued in early 2006, permits only a narrow range of cooperatives, non-profit entities, and the postal system to be used by banks as agents. In Kenya, the mobile phone-based M-PESA stored-value accounts are carefully structured so as not to constitute a 'banking activity' under the Kenyan Banking Act. This leaves M-PESA's provider, Safaricom free to choose its agents based on its business judgment alone. Both Safaricom and Vodafone have their own reasons to choose and manage agents carefully, given the potential reputation risk to their core telecommunications business. However, they do not stand behind their agents in the way Brazilian banks are required to do by regulation.

Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)

In many countries, a critical regulatory prerequisite for launching m-banking is adopting a risk-based approach for combating money laundering and terrorist financing. Unless the rules are adapted to the realities of low-income clients who may have limited access to formal documentation and remote transactions conducted through relatively unsophisticated retail agents, they risk preventing m-banking from getting off the ground. The FATF sets international AML/CFT standards and oversees compliance monitoring. It calls for national-level regulatory regimes to require that adequate Customer Due Diligence (CDD, also known as KYC rules) be undertaken on all new accounts and on one-off cash transactions over designated thresholds. FATF-compliant CDD/KYC rules require 'identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information' (FATF Recommendation 5).

In addition to CDD/KYC, FATF standards require financial service providers to keep detailed transaction records (including documentation collected in identifying and verifying the identity of customers) for at least five years (FATF Recommendation 10) and that they report suspicious transactions promptly to the AML/CFT authority (FATF Recommendation 13). FATF standards also mandate special attention to 'threats that may arise from new or developing technologies that might favor anonymity', and require policies and procedures be in place 'to address any specific risks associated with non-face to face business relationships or transactions' (FATF Recommendation 8).

Inadequate national AML/CFT regimes without space for non-face-to-face account opening, including CDD/KYC entrusted to staff of nonbank retail agents, or remote account opening may stop branchless banking before it starts. However, the experience of South Africa and the Philippines offers some encouragement to policy makers and regulators who want both a FATF-compliant AML/CFT regulatory regime and working m-banking services.

In the Philippines, policy makers managed to tighten AML/CFT regulation and enforcement sufficiently to get the country removed from FATF's blacklist of noncompliant countries and regions. At the same time, they arrived at regulatory accommodations that permitted the launch of both the bank-based (Smart) and nonbank-based (Globe) models of branchless banking. This includes mechanisms that enable CDD/KYC to be conducted by agents, a key characteristic of both Smart's and Globe's mobile banking models. They also allow a multiplicity of formal identity documents to be presented for verification purposes.

In South Africa, a carefully tailored exemption to otherwise applicable CDD/KYC measures and a special allowance for remote account opening permitted the launch of two different mobile phone-based branchless banking ventures (MTN Banking and WIZZIT). At roughly the same time, South Africa was meeting the stringent standards necessary to gain admission as a full member of FATF in 2003 (even holding the FATF presidency for 2005–2006). The exemption eliminated the otherwise applicable requirement under South African regulation to verify a customer's physical address for accounts subject to a maximum balance cap and a daily transaction limit (South African Ministry of Finance, 2004). One-third of South Africans, particularly low-income individuals, have difficulties securing documents to prove their physical address, mostly because they live in informal housing (Truen et al, 2005). The allowance extended the exemption to mobile-based services, permitting non-face-to-face account opening under certain circumstances. Clients can open mobile banking accounts by submitting data remotely via mobile phone. These data must then be verified against a third-party source, such as credit bureaus or databases containing information from the Department of Home Affairs. To limit risk, the functionality of accounts opened in this manner is more restricted than under the exemption, namely in terms of transaction limits (South African Reserve Bank, 2006). Reliable third-party databases in South Africa help satisfy the requirement of FATF Recommendation 5 to verify customer identity 'using reliable, independent source documents, data or information.'

E-money and other stored-value instruments

A growing number of countries have already moved beyond pure payment services to offer a virtual transaction account where customers can 'park' repayable stored value in electronic form for an indeterminate period and make payments and other money transfers when they choose to. These

models, to the extent that they facilitate payments via mobile phones, offer great potential for ‘transformational branchless banking’ because they effectively constitute a retail payments network far beyond the current banking and POS networks. Where the electronic stored value is issued by a bank, the funds, or float, backing the stored value will be monitored as a component of the overall prudential supervision of the bank, even if it is not considered a normal bank deposit.

The regulatory treatment of nonbank-issued e-money and other stored-value instruments in Russia and the Philippines illustrates two ends of the spectrum of the countries where nonbanks are not prohibited entirely from offering electronic stored value accounts. In Russia, WebMoney offers stored value accounts in unlimited amounts that can be topped up, among other means, via electronic cash acceptance terminals or through the purchase of scratch cards. WebMoney faces no prudential oversight, and customers’ funds are not protected from the firm’s other creditors. In the Philippines, the central bank used its broad regulatory powers to bring Globe Telecom’s GCash subsidiary GXI under its supervision. The central bank limited the risk of GCash by requiring, among other things, daily and monthly transaction caps, as well as a low cap on the amount customers may leave in their virtual account. Moreover, GXI submits monthly reports on its activities to the central bank.

Consumer protection

Furthermore, many of the countries studied started out with consumer protection-related challenges not directly related to branchless banking. In Russia, for example, consumer protection for all matters, from consumer product safety complaints to credit card fraud, falls within the jurisdiction of a single, centralized, and lightly staffed body. On the other hand, in India, primary legislative jurisdiction for consumer protection lies at the state level, meaning providers face a patchwork of different requirements depending on the location of their agents. In all countries studied, to a greater or lesser extent, poorer and more remote clients may not know about or understand their rights even if adequate regulatory protections are in place.

Payment system regulation

Russia, the Philippines, and Kenya, none of which has comprehensive national payment system legislation, are nonetheless the leaders among the countries studied in the development of alternative, nonbank, technology-based payment services platforms. They prove that national payment system legislation is not necessarily a prerequisite for launching m-banking.

Concluding remarks

This note describes the current international experience regulating the provision of m-banking services. There is a great potential for nonbanks such as MNOs to improve the reach and range of financial services for the unbanked, but the challenge lies in creating regulation that mitigate the risks without harming the dynamism of these new providers of financial services.

One of the lessons to be learned from the international experience is that m-banking regulation is just a subset of traditional banking regulation focusing only on the fraction of risks associated to m-banking activities out of all risks associated with a traditional financial organization. Going over each potential risk associated with m-banking, we conclude that, whenever the m-banking provider does not on-lend funds and instead is obliged to place 100% of deposits raised in one or more pooled accounts in supervised banks, m-banking activities do not give rise to prudential or liquidity risks. Indeed, in this manner, regulatory and supervisory concerns can be circumscribed to operational and technological risks.

Perhaps the most interesting international example is that of Kenya, the country where the most notable m-banking experience has taken place, bringing financial services to populations previously outside of the financial system and where m-banking providers have actually been able to make profits with the operation. The regulatory experience of Kenya has been one of not issuing e-money regulations and yet permitting MNOs to provide financial services through ‘no objection’ letters and conditional approvals. This has consequences on the practice of m-banking in the country. For instance, Safaricom maintains fund liquidity by placing its deposits in prudentially regulated banks following a prior agreement with the Central Bank of Kenya (CGAP, 2010), thereby minimizing prudential risks. In addition, the mobile phone-based M-PESA stored-value accounts are carefully structured so as not to constitute a ‘banking activity’ under the Kenyan Banking Act. This leaves M-PESA’s provider, Safaricom free to choose its agents based on its business judgment alone.

The future of m-banking services can also already be guessed when looking at Kenya: M-KESHO was recently launched in Kenya as a partnership between Safaricom and Kenya-based Equity Bank. This new product uses M-PESA’s platform and agent network to provide an expanded set of banking services, namely interest-earning savings accounts, micro-credit, and micro-insurance products. Such partnerships are likely to feature in the next phase of m-banking, when MNOs are likely to deliver a full array of financial services to those currently underserved by traditional banking models.

References

- Alampay, E. (2010), *Mobile Banking, Mobile Money and Telecommunication Regulations*. LIRNEasia and UPNCPAG.
- Alexandre, C., I. Mas and D. Radcliffe (2011), *Regulating New Banking Models that Can Bring Financial Services to All*, Challenge, forthcoming.
- Basel (1998), *Risk Management for Electronic Banking and Electronic Money Activities*, BIS.
- CGAP (2010), *Research Note on Regulating Branchless Banking in Kenya, 2010 Update*.
http://www.cgap.org/gm/document-1.9.42400/Updated_Notes_On_Regulating_Branchless_Banking_Kenya.pdf
- FDIC Financial Institutions Letters, 2008, *Insurability of Funds Underlying Stored Value Cards and Other Nontraditional Access Mechanisms*, *New General Counsel's Opinion No. 8*. Washington, D.C.: FDIC, 13 November.
- GSM Association [GSMA] (2009), *Mobile Money for the Unbanked*, Annual Report 2009.
http://www.gsmworld.com/documents/mmu_2009_annual_report.pdf
- Klein, M. and C. Mayer (2011), *Mobile Banking and Financial Inclusion: The Regulatory Lessons*, Frankfurt School of Finance and Management – Working Paper Series No. 166.
- Lyman, T., M. Pickens and D. Porteous (2008), *Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance*, CGAP Focus Note 43.
- Ivatury, G. and I. Mas (2008), *The Early Experience with Branchless Banking*, CGAP Focus Note 46.
- Makin, P. (2009), *Regulatory Issues Around Mobile Banking*, OECD, Paris, mimeo.
- Porteous, D. (2009). *Mobilizing Money through Enabling Regulation*. *Innovations*, Vol. 4, No. 1, Pages 75-90.
- Tarazi, M. and P. Breloff (2010), *Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds*, CGAP Focus Note 63.