JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 4 (2012)

The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa

Vivienne Lawack-Davids
Faculty of Law, Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
vivienne@nmmu.ac.za

Abstract. *South Africa is a developing economy and has both a first and second economy. One of the problems that it faces is that of the "unbanked", that is, a large segment of the population does not have bank accounts and "banking" happens through informal means. It also appears from latest figures that more people in South Africa have mobile phones than bank accounts. The usage of mobile banking and in particular, payments by means of mobile phones, has increased in recent years, with consequent impacts viewed from a legal and regulatory point of view. This paper seeks to examine the legal and regulatory framework pertaining to mobile banking, and in particular, mobile payments in South Africa. Regulatory gaps and areas for improvement are highlighted. The author argues for a more flexible approach to regulation in South Africa.*

1. Introduction

Continuing technological innovation and competition among existing banks and new market entrants has allowed for a much wider array of banking products and services for retail and wholesale banking customers. These include traditional activities such as accessing financial information, obtaining loans and opening deposit accounts, as well as relatively new products and services such as electronic account payment services, personalised financial 'portals', account aggregation and business-to-business market exchanges. Mobile banking and consequently, mobile payments are the latest in a myriad of technological innovations in the banking industry. The dependence on technology for the provision of these services with the necessary security and the cross-border nature of transactions present additional risks for banks and new challenges for banking regulators.

The aim of this paper is to provide an overview of the legal and regulatory framework for mobile banking in South Africa and focuses specifically on mobile payments. The author highlights some of the regulatory challenges relating to the development of mobile banking and mobile payments in South Africa.

2. Definition of Mobile Banking and Mobile Payments

Mobile banking falls within the definition of "electronic banking". "Electronic banking", or "e-banking" includes the provision of retail and small value banking products and services through electronic banking channels as well as large value electronic payments, and other wholesale banking services delivered electronically.[1] In other words, e-banking is the use of electronic delivery channels for banking products and services. It is a subset of e-finance. The most important electronic delivery channels are the Internet, wireless communication networks, automated teller machines (ATMs), telephones and mobile phones. Whilst e-banking

[1] Bank for International Settlements. 2001. Risk Management Principles for e-Banking , p3. Hereinafter "BIS".

in the form of ATMs and telephone has been around for many years, the popularity of accessing banking services through the Internet and mobile phones is rising. The following services could be offered:

- account applications;
- account balance enquiries;
- account statements;
- electronic funds transfer (between the consumer's own accounts or third party transfers);
- withdrawals to a smart card or software 'wallet' or 'purse' on a mobile phone;
- third party scheduled payment, such as payment of rent;
- loan applications;
- credit card applications.

Other value-added services include:

- news services (such as financial news);
- stock and mutual fund quotations;
- portfolio management;
- investment alerts;
- expert advice (including graphing and analysis of investments); and
- exchange rates.

As a form of e-banking, "m-banking" is defined as:

> "...financial services delivered via mobile networks and performed on a mobile phone. These services may or may not be defined as banking services by the regulator, depending on the legislation of the country in question, as well as on which services are offered".[2]

"Mobile payments" refer to the provision of payment services through the use of mobile phones, mostly electronic funds transfer between a customer's own accounts, transfers to a third party (beneficiary) or would be mobile money. A mobile payment may also refer to the process of two parties exchanging financial value using a mobile device in return for goods and services.[3]

Mobile money or "m-money" is a form of electronic money and refers to "services that connect consumers financially through mobile phones. Mobile money allows for any mobile phone subscriber, - 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.[4] In this way, m-money can be used for both money transfers and mobile payments.

"Mobile money transfers" are international remittances using mobile phones.[5] These are not included in the definition of mobile payments for the purposes of this paper.

3. Mobile Payments in South Africa

Several initiatives have emerged for initiating payments from mobile phones by using short messaging services (SMS) or phone calls. Mobile payments can be made through voice access, text messaging knows as SMS (short messaging service) or WAP (wireless application protocol), which provides a gateway to the Internet. Two

[2] Bångens, L and Söderberg, B. Mobile Banking, Mobile Money and Telecommunication Regulations. 2008 , p5.
[3] Ramezani, E. Mobile Payment. June 2008, p4.
[4] GMSA. (2010). Mobile Money for the Unbanked Mobile - Money Definitions, p3. See also Bank for International Settlements CPSS - Survey of E-money and Internet and Mobile Payments, March 2004, p4.
[5] For more detail see Mbalekwa, S. (2011). The Legal and Regulatory Aspects of International Remittances within the SADC Region unpublished LLM dissertation NMMU.

business models are in use, namely paying from a prepaid balance or adding the payment to the mobile phone bill. Some products use the phone as an access channel through existing bank accounts or payment cards, whereas others allow customers to pay using the prepaid value stored on the mobile phone or pay afterwards, where payment for goods or services are additional items on the customer's phone bill.

Most m-payment initiatives follow a simple model where the customer (payer) first identifies him/herself to the merchant by providing his/her phone number or by calling the merchant. The merchant forwards the payment and customer information to the payment service provider (e.g., through the mobile phone network). The service provider then presents the payment information to the payer for confirmation and upon confirmation (e.g., with a PIN number or one-time password) records the transaction. The communication between the customer and the payment provider and/or merchant can take place through SMS. The paid amount is collected by direct debit from the payer's account and credited to the beneficiary's account. There are models where a second smart card is used for the payment application. However, the usage of these systems is still limited.

Mobile banking has been on the increase in South Africa. Recently the four major banks in South Africa have been given a "wake-up" call with the emergence of the new kid on the block, "Wizzit".[6] Wizzit was developed to operate even in older phones and is not confined to any mobile telecommunications network. It piggy-backs on the banking license of Bank of Athens, a registered branch of a foreign banking institution.

Mobile devices are well positioned for making payments, because the penetration level of digital mobile phones is higher in South Africa than that of PCs. Latest figures from Wide World Worx suggest that in 2009 South Africa had a mobile penetration level of about 10,8%, which amounted to 5,300,000 users out of a population of 49,052,489. [7] What is interesting though, is that even though the use of Internet services has exploded in South Africa, less than half of urban mobile phone users who have Internet-enabled phones use the Internet. As many as 9,500, 000 South Africans are able to browse on their phones. If they use the Internet, the figure of World Wide Worx would almost double to 9, 600,000.[8]

4. South African Legal and Regulatory Framework

Central banks worldwide are considering their positions with regards to these emerging technologies. The regulatory stance in South Africa has mostly been with reference to electronic money, a subset of e-banking. The legal and regulatory framework with regards to e-banking would apply to mobile banking. In South Africa the legal framework comprises of the following:

- South African Reserve Bank Act;[9]
- National Payment System Act;[10]
- Banks Act;[11]
- Exchange Control Regulations (if cross-border);
- Financial Intelligence Centre Act;[12] and

[6] Wizzit is the brain-child of Brian Richardson, one of its founders. It has a strategy of getting into South African townships using "whizzkids" to sign up users to open bank accounts. MTN Banking is another big player. MTN Banking, a joint venture between MTN and Standard Bank of South Africa. MTN simply requires a SMS it an ID number and make a follow-up call, to start an account opening procedure that includes voice recognition technology. FNB Mobile at one stage in 2005 signed up 130 000 customers in six months. See "Talking About a Revolution". November 2005. Maverick Magazine, p34-38.
[7] See South Africa Internet Usage, Population, Broadband and Market Report at http://www.internetworldstats.com/af/za.htm (8/10/2011).
[8] See Mansfield, I. "Mobile Internet Usage Booms in South Africa". Cellular-News, 27 May 2010 at http://www.cellular-news.com/story/43524 (8/10/2011).
[9] Act No. 90 of 1989.
[10] Act No. 78 of 1998.
[11] Act No. 94 of 1990.
[12] Act No. 38 of 2001.

- South African Reserve Bank Position Paper on Electronic Money.[13]

Since this paper focuses on mobile payments, the legal and regulatory framework for payment through the use of mobile phone would be restricted to the payment system.

4.1 The National Payment System (NPS)

Payment systems are critical to the effective functioning of financial systems in a country and globally. If a payment system is insufficiently protected against risks such as credit, liquidity and settlement risks, disruption within the system could trigger or transmit further disruptions among its participants, or generate systemic disruptions in the financial markets or more widely across the economy. This phenomenon is referred to as "systemic risk". A fundamental requirement for a stable and secure payment system is that it should operate in a well-defined legal environment, setting out the rights and obligations of each party involved in effecting a payment through the system. It is for this very reason that Core Principle I of the Bank for International Settlements' Core Principles for Systemically Important Payment Systems provides that the legal basis for payments should be well-defined.

The ambit of the National Payment System (NPS) or "payment system" (the terms "NPS" and "payment system" are used interchangeably to denote the wider payment system and not individual payment streams) is described in the South African Reserve Bank *National Payment System Framework and Strategy 2010*[14]

> "the entire process of making payment, in other words, it entails the process (including but not limited to) that enables the payer to make a payment, the payer to issue a payment instruction via a payment instrument or other infrastructure, the institution to receive the payment instruction via clearing or otherwise, the process of clearing and settlement (where applicable), the beneficiary to accept the payment instruction, the beneficiary to deliver the payment instruction to an institution for collection, the institution to receive and deliver the payment collection into clearing and settlement, and the beneficiary to receive the benefit of the payment. Within the described process, banks, third-person payment providers, system operators, PCH system operators (PCH refers to a 'payment clearing house') and agents of payers and/or beneficiaries are included".

4.2 Oversight of the NPS

The Reserve Bank, as neutral agent, is best suited to oversee and supervise the NPS. The powers conferred and duties imposed upon the Reserve Bank relating to its function of providing clearing and settlement facilities to banks are contained in section 10(1)(c) of the South African Reserve Bank Act.[15] This subsection enables the Reserve Bank to establish, operate, oversee and regulate payment, clearing and settlement systems.

The National Payment System Department of the Reserve Bank performs the oversight of payments in South Africa. In terms of section 3 of the Banks Act, the Registrar of Banks supervises the banking industry. The Registrar performs this function, in conjunction with the Bank Supervision Department of the Reserve Bank.

Depending on the type of banking product that a bank wishes to offer, oversight would fall into the domain of either of these departments, sometimes into both. For example, there is no provision in the Banks Act that prevents a bank from setting up mobile banking. Therefore, all the major banks in South Africa offer mobile banking as a value-added service to their customers. However, if mobile payments are offered, the matter would

[13]Position Paper No. 1of 2009.
[14] South African Reserve Bank. (2006). (hereinafter "*Vision 2010*" and "Reserve Bank").
[15] Act No. 90 of 1989.

fall within the ambit of the NPSD, because the provision of these services may pose systemic or other risks which may threaten the stability of and confidence in, the National Payment System.[16]

Besides the general powers of oversight in terms of section 10(1)(c) of the Reserve Bank Act as mentioned above, the Reserve Bank has the power to issue directives, in consultation with the payment system management body and other stakeholders.[17] To date, the Reserve Bank has not issued any directives dealing with m-money or m-payments.

4.3 Position Papers

The Reserve Bank sometimes issues "Position Papers" to clarify its regulatory stance. Although Position Papers do not have the same legal binding power as directives, they are usually followed because of the moral suasion powers of the Reserve Bank. In addition, if the Reserve Bank is so inclined, it may issue a special directive aligned with its stance in the Position Paper that must be complied with, otherwise the Reserve Bank may apply to the High Court for an order to direct such person to comply with the directive issued. The Reserve Bank initially issued a Position Paper on Electronic Money in 1999.18 This Position Paper was amended in 2006 and subsequently again in 2009.

Electronic money is defined in the 2009 Position Paper as:

> "monetary value represented by a claim on the issuer. This money is stored electronically and issued on receipt of funds, is generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand" (own emphasis).

There are five characteristics to this definition, namely:

- Monetary value represented by a claim on the issuer;
- Money is stored electronically;
- Money is issued on receipt of funds;
- Is generally accepted as a means of payment by persons other than the issuer; and
- Is redeemable for physical cash or a deposit into a bank account on demand.

Having "money" stored on a mobile phone could satisfy the definition of "electronic money" since it is monetary value represented by a claim on the issuer, it is stored electronically (on the mobile phone), is issued on receipt of funds (to the issuer) and may be redeemable for physical cash or a deposit into a bank account. One could argue that at this stage, mobile payments, while growing, would not be "generally accepted as a means of payment by persons other than the issuer.

The definition of e-money in the 2009 Position Paper is different from previous definitions of electronic money in various respects. Firstly, the underlined part of the definition denotes a significant departure from the definitions of "electronic money" in the previous NPSD Position Papers on electronic money. It is now a requirement that the monetary value be redeemable for physical cash or a deposit into a bank account on demand. In effect, it means that whilst the electronic value is not redeemed, it would not fit the definition of electronic money.

The second difference in the definition is the reference to electronic value having to be represented by a "claim on the issuer". From the Position Paper it seems that the reason for this change is to distinguish between

[16] For more detail on the South African NPS, see Lawack-Davids, V (2008). "The Legal and Regulatory Framework of the National Payment System - Peeling the Layers of the Onion". *Obiter* vol 29(3), p 453-471.
[17] Section 12 (1). It is an offence to fail, refuse or neglect to comply with directives and a person who is found guilty of such an offence is liable to a fine of R1 million or to imprisonment or to both a fine and imprisonment.
[18] Hereinafter "Position Paper".

payments to third parties when payment is "due "in terms of section 7 of the NPS Act and the situation when a payer sends electronic value to a beneficiary who is then able to encash that value.

Section 7 of the NPS Act allows a person, as a regular feature of that person's business, to accept money or payment instructions from any other person for purposes of making a payment on behalf of the first person, to a third person, to whom the payment is due.[19] The implication of this provision is that there is an obligation that must be settled, for example the payment of rates, taxes or electricity to a municipality. Payments to third persons may be provided subject to the provisions of the directive relating to payments to third persons.[20]

In terms of the Position Paper, with person-to-person payments, money is sent by the payer to a beneficiary in the form of electronic value and such money is normally not "due" to the beneficiary in terms of an obligation. This means that it would contravene section 7 of the NPS Act and be classified as "deposit-taking" in terms of the Banks Act.[21] The taking of deposits from the general public by an unregistered person (non-bank) is a criminal offence in terms of the provisions of the Banks Act. It is however, unclear when exactly or under which circumstances payments would be regarded as "being due".

The third and most significant departure is the fact that the Position Paper now states that only South African registered banks may issue electronic money, unlike the reference in the previous definitions of "making payments to undertakings other than the issuer, with or without involving bank accounts in the transaction".

With the emergence of a few non-banks such as Wizzit and provision of mobile banking services, the effect is that the normal sponsorship arrangements for clearing and settlement will prevail. In other words, Wizzit is not a settlement system participant and needs to be sponsored by a bank (in this case Bank of Athens, which is a registered branch of a foreign institution) to enable clearing and settlement.[22]

Viewed from the point of view of the Reserve Bank, it could be argued that emerging e-money products may require regulatory adjustment or intervention, which may arise from the need to:

(a) Maintain the integrity, confidence and limit the risk in the NPS;
(b) Assist other regulatory authorities in providing consumers with adequate protection from unfair practices, fraud and financial loss; and
(c) Assist law enforcement agencies in the prevention of criminal activity.[23]

It is evident from the above that the Reserve Bank initially adopted a wait-and-see approach but that the regulatory stance has changed to limit the issuance of e-money to banks. There is no formal prudential supervision of e-money, as is the case in the European Union.[24] This implies that there are no minimum capital reserve requirements pertaining to electronic money besides the normal prudential requirements pertaining to a bank.

Viewed from the perspective of non-banks wanting to enter this market, the Position Paper limits access to the payment system in that such non-bank would have to enter into a sponsoring arrangement with a bank, with consequent cost implications for such non-bank. Furthermore, the high growth and penetration rates of mobile telephony that is transforming cell phones into banks in pockets of Africa is providing opportunities for countries on the African continent to increase affordable and cost-effective means of bringing the "unbanked" into the formal financial system.

[19] See section 7 of the NPS Act.
[20] Directive No. 1 of 2007 (Directive for the Conduct within the National Payment System in Respect of Payments to Third persons.
[21] See the Position Paper. (2009), p5.
[22] See section 4 (2) (1) (d) and section 6 of the NPS Act on clearing and sponsorship arrangements.
[23] Position Paper. (2009), p4.
[24] See Directive 2000/46 EC on The Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions.

With the requirement in the Position Paper that an issuer of e-money has to be a bank registered in South Africa, one finds that multiple regulators are involved, namely the South African Reserve Bank for regulation of banking and oversight of payments and the telecommunications regulator for the regulation of the telecommunications service provider. In South Africa, telecommunications are regulated in terms of the Electronic Communications Act, 2005.[25] The main authority is the Independent Communications Authority of South Africa established by section 3 of the Independent Communications Authority of South Africa Act, 2000.[26] The problem with multiple regulators is that the possibility exists for regulatory arbitrage, that is, that players would take advantage of regulatory lacunae.

Whilst the above legal and regulatory environment seems for the most part sound, there are uncertainties as highlighted. It is submitted that instead of focussing on "e-money", the South African Reserve Bank may want to consider issuing a Position Paper dealing with all forms of emerging banking technology in which definitions can be stated clearly and any change in regulatory stance explained with reference to other regulatory instruments. For example, if the intention was to broaden access in the Vision 2010 by providing that non-banks "may also provide payment services to third parties", it is not clear why this statement has been limited through the requirement that payments must be "due" in the 2009 Position Paper. Mobile payments that do not arise to pay utilities are excluded and hence, the issuer(s) of such payments would have to be registered banks. The alternative is to be sponsored by a bank, which seems to be what non-banks select to do out of expediency. Klein and Mayer make a compelling argument that what mobile banking illustrates in a stark form is the way in which payment systems can be disaggregated into component services, namely exchange, storage, transfer and investment. In their words:

> "Regulation should mirror this and be structured by service rather than along traditional lines, like a bank. The question then is what type of regulation is appropriate for which type of service".[27]

This is a challenge which is not well researched at present in South Africa. It is submitted that with the increasing penetration level of mobile users in South Africa, research is needed into the impact on access to the unbanked given the change in regulatory stance of the South African Reserve Bank, lest a golden opportunity is missed to increase access to financial services to the poor in South Africa.

4.3 Regulatory Risks and Challenges

The challenges presented by e-banking involve the risks which they present, money laundering issues and consumer protection and education. However, this note does not deal with anti-money laundering related issues, but identifies the most important supervisory risks and challenges with regard to e-banking.

Despite the significant benefits of technological innovation, the rapid development of e-banking capabilities carries risks as well as benefits. The Basel Committee on Banking Supervision conducted a preliminary study of the risk management implications of e-banking in 1998.[28]

In terms of this early study it was evident that more work was needed in the area of e-banking risk management and the mission was entrusted to a working group, which consisted of bank supervisors of central banks. The Electronic Banking Group (EBG) was formed in November 1999. The Basel Committee released the EBG's Report on *Risk Management and Supervisory Issues arising from E-banking Developments* in October 2000.[29] In terms of the EBG Report, e-banking activities do not cause risks that were not already identified by

[25] Act No. 36 of 2005 replaced the former Telecommunications Act No. 103 of 1996. This Act aims to converge broadcasting and telecommunications under one regulator.
[26] Act No. 13 of 2000
[27] Mobile Banking and Financial Inclusion – The Regulatory Lessons. May 2011. World Bank Policy Research Working Paper 5664, p24-25.
[28](1998). Risk Management for Electronic Banking and Electronic Money Activities.
[29] See Electronic Banking Group Initiatives and White Papers October 2000, available at http://www.bis.org 2011-04-14 – hereinafter the "EBG Report".

previous work of the Basel Committee. However, it was noted that e-banking increases and modifies some of these traditional risks, thereby influencing the overall risk profile of banking. This report led to the *Risk Management Principles for Electronic Banking* report, published in May 2001. Although this report deals with 14 risk management principles which fall into three broad and often overlapping categories (board and management oversight, security controls and legal and reputational risk management), this note focuses on categories of risk most affected by the specific nature of e-banking activities. These are operational and reputational, which will be discussed in the context of the challenges that these create for regulators.

4.3.1 Regulatory challenges

The rapid innovation of emerging technologies presents a challenge, as the law inevitably trails these technologies and is playing 'catch-up'. In addition, m-banking has significant implications for the banking industry and regulatory authorities. There are several ways in which the expansion of this development generates potential challenges for regulatory policy.

Firstly, developing technology may change the structure and function of financial institutions. As new types of institutions evolve, the traditional lines of demarcation become less clear. For example, are mobile banks considered "virtual banks" or "branchless banks" if they are operated by technology companies, but considered an extension of traditional banking services if performed by a bank? Secondly, m-banking may raise either new concerns or, more likely, accentuate or lessen concern about current public policy issues. The most prominent example of a public policy concern accentuated by Internet banking has been the issue of privacy. Thirdly, developing technologies challenge traditional methods of safety and soundness of supervision by changing the nature and scope of existing risks and possibly creating new risks. Finally, the nature and scope of technological change may require regulators to re-balance their emphases on regulatory rules and industry discretion.

In terms of supervision of e-banking, there are at least two broad safety and soundness themes that will grow in importance as the supply and demand for m-banking services increase, namely system security and vendor management.

Firstly, as m-banking becomes more widespread and complex, the necessity for banks to assess and manage operational risks will become more crucial. Security is considered the central operational risk of e-banking. Threats can come from the inside and outside of the system. They include unauthorised access to the system through, for example, 'back doors', 'brute force', 'highjacking', 'sniffing' or 'spoofing' to retrieve and use confidential consumer information, add customer assets, subtract customer liabilities or interrupt operations. Similarly, 'denial of service' attacks and injecting a virus can disrupt services and affect the integrity of information.[30]

Security in mobile payment schemes is concerned with preventing misuse and eliminating fraud by unauthorised users. In the case of direct access to the bank account via the mobile phone, a high level of security is required. Basic internal security principles include the 'segregation of duties' and the 'access control' principle. Some of the principal security practices consist of properly configured firewalls, strong encryption technology and authentication techniques, sound password policies and standards, adequate back-up and recovery arrangements and updated virus scanning tools.[31]

The Position Paper states that information security is critical to the success of e-money services and their operational services. No information or funds transfer in the payment system should be vulnerable to

[30] 'Back doors' are pieces of programme code written into applications or operating systems which grant programmers access to programmes without the need to go through the normal security controls. 'Brute force attack' is a technique to capture encrypted messages and then use software to break the code and gain access to messages, user Ids or passwords. 'Highjacking' is an attack in which the connection is stolen after a victim has authenticated him or herself to the system. 'Sniffing' involves the use of a software programme that is illicitly inserted somewhere on a network to capture user passwords as they pass through the system (keystroke logging is an example of sniffing). 'Spoofing' refers to an attempt to gain access to a system by posing as an authorised user. See BIS. 2001. Risk Management Principles for E-banking, p13.

[31] BIS Committee on Payment and Settlement Systems. (2004) Survey of Developments in Electronic Money and Internet and Mobile Payments, p8.

interception by unauthorised users. Therefore, the technology used must be secure and ensure confidentiality, integrity, authenticity and non-repudiation. In addition, the security and operational services used for the e-money services must meet the requirements of international standard bodies. The same would apply for m-money or m-payments.

The second regulatory concern is that security failure at a particular institution could not only cause large losses for that institution, but could spawn a general lack of confidence in electronic banking and m-banking, leading to reputational risk. If a bank fails to deliver secure, accurate and timely services on a consistent basis, its reputation is at risk. In addition to system availability and integrity, breaches in data confidentiality and any other glitches to the security of operations can damage a bank's reputation.

The reputational risk may be higher for banks that rely entirely on electronic delivery channels ("so-called branchless or virtual banks") or banks that rely predominantly on electronic delivery channels, than for traditional "brick and mortar" banks. For the banking system as a whole, however, there seems to be no systemic risk from m-banking at this stage for as long as the share of virtual banks continues to be rather low and the value of m-payments remains low.

The development of newer electronic channels of delivery such as the Internet and mobile phones has made banks increasingly reliant on third party service providers. The greater the banks rely on outsourcing, the more dependent the safety and soundness of individual banks, and the banking system, become on third party service providers, many of which are not part of a regulated industry. This presents policy makers with the challenge of balancing access to, and oversight of, non-bank technology companies on the one hand, and avoiding excessive expansion of bank regulation and supervision to such banks, on the other hand. This is made more difficult when technology companies are regulated by a different regulator, as is the case in South Africa, as mentioned before.

Increasing reliance on outsourcing may add substantially to a bank's operational risk. Outsourcing not only introduces an additional security threat, it may also have a major impact on the data and system integrity and availability. Conducting due diligence, ensuring the adequacy of contracts governing e-banking, developing appropriate contingency plans, and monitoring the ongoing viability of third-party services must become part of banks' risk management.[32]

The only Banks Act Circular dealing with mobile banking issued to date by the Registrar of Banks in South Africa relates to anti-money laundering measures and how banks should treat these where mobile banking is concerned. Of note is the view expressed in the Circular that banks must continue exploring ways of enhancing the non face-to-face account opening procedure in order to ensure that the information received from a prospective client in any given case in fact pertains to that person. Furthermore, should banks wish to provide cell-phone banking type products, the Office of the Registrar has to be informed at least six weeks prior to the launch of such products.[33]

4.3.2 Interoperability

Several initiatives have been launched to promote interoperability between the different solutions. As stated above, mobile phones are already used to access financial services, via SMS or Wireless Application Protocol (WAP) services. Furthermore, newer technologies for mobile communication, such as General Packet Radio Service (GPRS), a packet-based technology that enables high-speed (115 kilobits per second), wireless Internet and data communications, are allowing wider access to Internet-based commercial services.

With regard to interoperability, the Electronic Money Position Paper[34] provides that if more than one settlement system participant issues e-money, an e-money Payment Clearing House (PCH) may be established by the Payment System Body (Payments Association of South Africa) to ensure interoperability and appropriate

[32] BIS Risk Management. (2001).
[33] Banks Act Circular 6/2006).
[34] P8.

rules for clearing and settlement of similar e-money transactions between these banks. The regulatory challenge here is how to encourage interoperability without letting players losing their competitive edge.

5. Conclusion

This note gives an overview of the legal and regulatory framework for mobile payments in South Africa. Whilst the legal and regulatory framework is for the most part sound, the author identifies risks and challenges and uncertainties which regulators may take into account. The note also examines the significance of the Position Paper on Electronic Money, the reasons for the change in regulatory stance and the effect that this may have on access to the payment system for non-bank mobile payment providers. The author argues that continued research in this area is needed to assess the impact of the change in regulatory stance on access to financial services for the poor, as a golden opportunity may be missed to increase access to the payment system if it is found that there is over-regulation of mobile payments in South Africa.

* * * *

Cite as: Lawack-Davids , Vivienne . The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa.. *Journal of International Commercial Law and Technology*, Vol.7 Issue 4 (October, 2012)