Washington Journal of Law, Technology & Arts

Volume 8
Issue 3 *Mobile Money Symposium*

Article 9

1-1-2013

Mobile Money, Financial Inclusion and Financial Integrity: The South African Case

Vivienne A. Lawack

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 3 MOBILE MONEY SYMPOSIUM 2013

MOBILE MONEY, FINANCIAL INCLUSION AND FINANCIAL INTEGRITY: THE SOUTH AFRICAN CASE

Vivienne A. Lawack [*]

Cite as: 8 WASH. J.L. TECH. & ARTS 317 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1202

ABSTRACT

The usage of mobile banking and in particular, payments by means of mobile phones, has increased in recent years in South Africa, with consequent impacts from a legal and regulatory point of view. South Africa is a developing economy with a large "unbanked" sector. That is, a large segment of the population does not have bank accounts and "banking" happens through informal means. This Article deals with the legal and regulatory framework pertaining to mobile money and examines issues relating to financial integrity and financial inclusion as they present themselves in South Africa. The author states that the regulatory framework in South Africa is not entirely conducive to greater financial inclusion and argues for a better balance between the regulation of risk and access to the payment system through an enhanced implementation of a risk-based approach.

---

[*] Vivienne A. Lawack, BJuris LLB LLM (UPE) LLD (Unisa) is Executive Dean: Faculty of Law, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa. My heartfelt thanks to Professor Jane K. Winn and Professor Louis de Koker for their invaluable support and guidance.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean's Innovation Fund.

TABLE OF CONTENTS

INTRODUCTION

Mobile banking, and consequently, mobile payments and mobile money are the latest in a myriad of emerging technological innovations in the banking industry. The usage of mobile banking and in particular, payments by means of mobile phones, have increased in recent years in South Africa, with consequent impacts from a legal and regulatory point of view.

South Africa is a developing economy with a large "unbanked" sector. 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 the penetration level of South Africans with mobile phones is increasing, yet the regulatory framework is not entirely conducive to greater financial inclusion. This Article seeks to examine the legal and regulatory framework pertaining to mobile money and examines issues relating to financial integrity and financial inclusion as they present themselves in South Africa. Regulatory gaps and areas for

improvement are highlighted. The author argues for a more flexible approach to regulation in South Africa to enhance financial inclusion through the use of mobile money there.

I. DEFINITION OF MOBILE MONEY

Before one could understand the term "mobile money," it is necessary to understand associated terms that may have bearing on the definition of mobile money. As a form of e-banking,[1] "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 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.[3] In this way, m-money can be used for both mobile money transfers[4] and mobile payments.[5] Mobile

---

[1] E-banking is the use of electronic delivery channels for banking products and services. *See* BANK FOR INT'L SETTLEMENTS [BIS], RISK MANAGEMENT PRINCIPLES FOR ELECTRONIC BANK 5 (2001), *available at* http://www.bis.org/publ/bcbs82.pdf.

[2] Lennart Bångens & Björn Söderberg, *Mobile Banking – Financial Services for the Unbanked?* 14 (Swedish Program for ICT in Dev. Regions, 2008), *available at* http://www.spidercenter.org/sites/default/files/Mobile%20banking%20-%20financial%20services%20for%20the%20unbanked.pdf. For the most recent publication, see PIERRE-LAURENT CHATAIN ET AL., PROTECTING MOBILE MONEY AGAINST FINANCIAL CRIMES: GLOBAL POLICY CHANGES AND SOLUTIONS (2011).

[3] COMM. ON PAYMENT AND SETTLEMENT SYS. [CPSS], BIS, SURVEY OF DEVELOPMENTS IN ELECTRONIC MONEY AND INTERNET AND MOBILE PAYMENTS 4 (2004), *available at* http://www.bis.org/publ/cpss62.pdf.

[4] "Mobile money transfers" are international remittances using mobile phones. For more detail, see CPSS & THE WORLD BANK, GENERAL PRINCIPLES FOR INTERNATIONAL REMITTANCE SERVICES 2 (2007), *available at* http://siteresources.worldbank.org/INTPAYMENTREMMITTANCE/Resources

money transfers are thus included in the definition of mobile money for the purposes of this Article.

II. MOBILE MONEY IN SOUTH AFRICA

Mobile banking has been increasing in South Africa. Several initiatives have emerged for initiating payments from mobile phones by using short messaging services (SMS) or phone calls. Some products use the phone as an access channel through existing bank accounts or payment cards. Meanwhile, other products allow customers to pay using prepaid value stored on their mobile phone or to pay afterwards, where payment for goods or services are additional items on the customer's phone bill or through the use of Near Field Communication (NFC) technology. However, this system was only piloted once within a closed system during a music festival called "Oppikoppi" and on a trial basis by ABSA employees.[6]

Initially the four major banks in South Africa were given a wake-up call with the emergence of then-new kid on the block, WIZZIT.[7] However, it is apparent that it is now the four biggest

---

/New_Remittance_Report.pdf. *See also* Simbarashe Mbalekwa, *The Legal and Regulatory Aspects of International Remittances Within the SADC Region* (Jan. 2011) (unpublished LL.M. dissertation, Nelson Mandela Metro. Univ.), *available at* http://www.nmmu.ac.za/documents/theses/SIMBARASHE%20MBALEKWA.pdf.

[5] "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. *See* Elham Ramezani, *Mobile Payment* 4 (June 17, 2008) (term paper, Hochschule Furtwangen Univ.), *available at* http://webuser.hs-furtwangen.de/~heindl/ebte-08-ss-mobile-payment-Ramezani.pdf.

[6] Jan Vermeulen, *Oppikoppi to go Cash Free in 2011*, MYBROADBAND (July 2, 2011), http://mybroadband.co.za/news/general/28051-oppikoppi-to-go-cash-free-in-2011.html; Media Release, ABSA Bank, Cellphones as Payment Devices (Dec. 6, 2011), *available at* http://www.absa.co.za/Absacoza/Media-Centre/Press-Statements/Cellphones-as-payment-devices.

[7] WIZZIT is the brain-child of Brian Richardson. It has a strategy of getting into South African townships using "whizz kids" to sign up users to open bank accounts. MTN Banking is a joint venture between MTN and Standard

commercial banks (Nedbank, First National Bank, Standard Bank, and ABSA) that are the providers of mobile banking services in South Africa through joint ventures with mobile technology companies and retailers. For example, Nedbank and mobile operator Vodacom teamed up to launch M-PESA, a solution that enables person-to-person money transfers via mobile phone, even between persons without bank accounts. This followed the Standard Bank's launch of a similar product, called "Instant Money," a joint venture between the bank and local retailer Spar. Standard Bank also has a joint venture company called "Oltio" between itself and pan-African mobile network operator MTN, which, through its "payD" platform enables customers to purchase products and services online and use their debit cards to pay for the purchase while making use of their mobile phones to enter their personal identification numbers (PINs). First National Bank also entered the fray, launching its "e-Wallet" mobile money transfer solution, which allows customers to send money to anyone in South Africa with a valid mobile phone number. Finally, as stated previously, ABSA Bank conducted South Africa's first live user trial of NFC technology on mobile phones, in a partnership with MasterCard, to embed the "Paypass Tap and Go" payment chip on mobile handsets for the trial. This enabled customers to load funds onto their phones through the ABSA website or ATMs and then to pay for goods or services by merely holding their phones in front of NFC-enabled pay points. The value of their transactions is then immediately debited from their stored value.[8]

Bank of South Africa. MTN simply requires a SMS that the user provides 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. WIZZIT was developed to operate even in older phones and is not confined to any mobile telecommunications network. It "piggybacks" on the banking license of Bank of Athens, a registered branch of a foreign banking institution. *See* Maya Fisher-French, *Talking 'Bout a Revolution*, MAVERICK MAGAZINE, Nov. 3, 2005, at 34, *available at* http://www.wizzit.co.za/media/revolution.pdf.

[8] For more detail, see the websites of the four commercial banks: FIRST NAT'L BANK, http://www.fnb.co.za; STANDARD BANK, http://www.standardbank.co.za; ABSA BANK, http://www.absa.co.za; and NEDBANK, www.nedbank.co.za (all websites last visited Aug. 16, 2012).

Mobile devices are well positioned for making payments because the penetration level of digital mobile phones is higher in South Africa than that of computers. Latest figures from Wide World Worx suggest that in 2009 South Africa had a mobile penetration level of about 10.8 percent, which amounted to 5,300,000 users out of a population of 49,052,489.[9]

It is interesting 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 the Internet on their phones.[10] If they use the Internet, the figure of World Wide Worx would almost double to 9,600,000.[11] The potential thus clearly exists for a higher penetration level with respect to Internet-enabled payments through the use of a mobile phone.

It is also interesting to note the inroads that have been made to increase the level of banked South Africans. Between 1993 and 2009, the number of banked South Africans increased remarkably, especially in the black ethnic group. This increase has largely been due to easier access to banking services being provided to people living in informal urban areas and to those earning less than ZAR2,000 a month. The driving force behind the substantial increase was the South African government policy on economic empowerment and the inclusion of targets in the Financial Sector Charter, which led to a proliferation of products and services offered, such as "Mzanzi accounts," ATM cards, debit/check cards, credit cards, savings and transaction accounts, as well as mobile banking.[12] Nonetheless, a significant portion of the black population is still unbanked.[13]

---

[9] *South Africa Internet Usage, Population, Broadband and Market Report*, INTERNET WORLD STATS, http://www.internetworldstats.co./af/za.htm (last visited Aug. 25, 2012).

[10] Ian Mansfield, *Mobile Internet Usage Booms in South Africa*, CELLULAR NEWS (May 27, 2010), http://www.cellular-news.com/story/43524.php.

[11] *Id.*

[12] For more detail, see GLOBAL P'SHIP FOR FIN. INCLUSION [GPFI], GLOBAL STANDARD SETTING BODIES AND FINANCIAL INCLUSION (2011), *available at* http://www.gpfi.org/sites/default/files/documents/Global%20Standard%20Setting%20Bodies%20and%20FI.pdf.

[13] For more detail, see FINMARK TRUST, FINSCOPE SOUTH AFRICA (2009),

III. FINANCIAL INCLUSION AND THE SOUTH AFRICAN LEGAL AND REGULATORY FRAMEWORK FOR MOBILE MONEY

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 is comprised of the following:

- South African Reserve Bank Act (Act 89 of 1990);
- National Payment System Act (Act 78 of 1998);
- Banks Act (Act 90 of 1994);
- Exchange Control Regulations (if cross-border);
- Financial Intelligence Centre Act (Act 38 of 2001); and
- South African Reserve Bank Position Paper on Electronic Money.[14]

A. The National Payment System (NPS)

Payment systems are critical to the effective functioning of financial systems in a country and globally.[15] If a payment system is insufficiently protected against risks such as credit, liquidity, and

---

available at http://www.finscope.co.za/documents/2009/Brochure_SA09.pdf. *See also* Press Release, FinMark Trust & TNS Research Surveys, South Africa in Black and White (Jan. 2009), *available at* http://www.tnsresearchsurveys.co.za/news-centre/pdf/2009/Fin08-FaceofSA.pdf.

[14] S. AFR. RESERVE BANK, POSITION PAPER ON ELECTRONIC MONEY (2009), *available at* http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf [hereinafter POSITION PAPER].

[15] The payment system can also be described as the "essential oil that lubricates the economy." Stefan Gannon, *Weaving Nets to Catch the Wind: The Legal and Regulatory Issues Concerning the Development of Robust and Efficient International Electronic Financial Infrastructure*, 33 COMM. L. WORLD REV. 352, 353 (2004).

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."[16]

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.[17] It is for this very reason that Core Principle I of the *Core Principles for Systemically Important Payment Systems* published by the Committee on Payment and Settlement Systems of the BIS provides that the legal basis for payments should be well defined.[18] The ambit of the South African NPS has been confirmed by the Reserve Bank in its recently released *National Payment System Framework and Strategy Vision 2015*.[19]

---

[16] The generally accepted terminology used to describe these risks are derived from CPSS, BIS, A GLOSSARY OF TERMS USED IN PAYMENTS AND SETTLEMENT SYSTEMS (2003), *available at* http://www.bis.org/publ/cpss00b.pdf.

[17] This is to guard against "legal risk." "Legal risk" is defined by the BIS as "the risk of loss because of the unexpected application of a law or regulation or because a contract cannot be enforced." *See id.* at 29.

[18] It states that "the system should have a well founded legal basis under all relevant jurisdictions." CPSS, BIS, CORE PRINCIPLES FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS 6 (2001), *available at* http://www.bis.org/publ/cpss43.pdf.

[19] S. AFR. RESERVE BANK, NATIONAL PAYMENT SYSTEM FRAMEWORK AND STRATEGY: VISION 2015 9 (2011), *available at* http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Documents/Overview/Vision2015.pdf. The ambit of the NPS or "payment system" is described in the S. AFR. RESERVE BANK, NATIONAL PAYMENT SYSTEM FRAMEWORK AND STRATEGY: VISION 2010 11 (2006), *available at* http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Documents/Overview/Vision2010.pdf:

> The oversight domain of the NPS entails 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

B. Oversight of the NPS

The Reserve Bank, as a neutral agent, is best suited to oversee and supervise the NPS. Section 10(1)(c) of the South African Reserve Bank Act enables the Reserve Bank to establish, operate, oversee, and regulate payment, clearing, and settlement systems. This power is reaffirmed in Section 2 of the National Payment System Act.[20]

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,[21] in consultation with the

---

> 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.

[20] Nat'l Payment Sys. Act 78 of 1998 (S. Afr.), *available at* http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/NPS%20Act.pdf [hereinafter NPS Act]. 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. However, if mobile payments are offered, the matter would fall within the ambit of the National Payment System Department (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. For more detail on the South African NPS, see Vivienne Lawack-Davids, *The Legal and Regulatory Framework of the National Payment System (NPS) – Peeling the Layers of the Onion*, 29 OBITER 453 (2008).

[21] Directives issued in consultation with the payment system management body terms of Subsection 1 are "general directives," as opposed to the "remedial directives" which the Reserve Bank may issue in terms of Subsection 3. Provision is made for the cancellation of previously issued directives and an offense in Subsection 3. *See* NPS Act §§ 12(3), (5), (6), (8).

payment system management body and other stakeholders (Section 12(1)).[22] The Reserve Bank has to date issued three directives, to wit, in respect of banks involved in the collection of payment instructions in the early debit order of Payment Clearing Houses (PCHs),[23] in respect of system operators,[24] and in respect of payments to third persons,[25] but no directives dealing with m-money or m-payments.

Furthermore, 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 Reserve Bank's moral persuasion powers. 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.

"Mobile money" is defined in the 2009 Position Paper as:

> [M]onetary 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.[26]

---

[22] It is an offense to fail, refuse, or neglect to comply with directives and a person who is found guilty of such an offense is liable to a fine of ZAR1 million or to imprisonment or to both a fine and imprisonment. No directives issued will have retroactive effect. Provision is also made for a grace period in respect of "general directives," as opposed to "remedial directives" which will become effective immediately. *See id.* at § 12(9).

[23] *See* NPS Act Directive 2 of 2006 (S. Afr).

[24] *See* NPS Act Directive 2 of 2007 (S. Afr.), *available at* http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Directives/D2_2007(SysOp).pdf.

[25] *See* NPS Act Directive 1 of 2007 (S. Afr.), *available at* http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Directives/D1_2007(ThirdParty).pdf.

[26] POSITION PAPER, *supra* note 14, at 3. The Reserve Bank initially issued a Position Paper on mobile money in 1999. This Position Paper was amended in 2006 and subsequently again in 2009.

Having "money" stored on a mobile phone could satisfy the definition of "mobile money" since it is monetary value represented by a claim on the issuer, it is stored electronically (on the mobile phone), it is issued on receipt of funds (to the issuer), and may be redeemed for physical cash or deposited into a bank account. However, 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 mobile money in various respects. Most notably for purposes of this Article is that the Position Paper now states that *only South African registered banks* may issue mobile 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 mobile banking services providers and retailers, the effect is that the normal sponsorship arrangements for clearing and settlement will prevail. In other words, the retailer or technology company is not a settlement system participant and needs to be sponsored by a bank to enable clearing and settlement.[27]

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

- Maintain the integrity, confidence and limit the risk in the NPS;
- Assist other regulatory authorities in providing consumers with adequate protection from unfair practices, fraud and financial loss; and
- Assist law enforcement agencies in the prevention of criminal activity.[28]

This view is affirmed by the new Reserve Bank Payment System Vision 2015, which explains that, in view of the global

---

[27] See NPS Act §§ 4(2)(d)(i), 6 on clearing and sponsorship arrangements. *See also* POSITION PAPER, *supra* note 14, at 4.

[28] POSITION PAPER, *supra* note 14, at 4.

crisis, a tightening of oversight is needed. Viewed from the perspective of non-banks wanting to enter this market, the Position Paper limits financial inclusion (access to the payment system) in that the 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.[29]

With the requirement in the Position Paper that an issuer of e-money has to be a bank registered in South Africa, 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.[30] 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 focusing on e-money, the South African Reserve Bank may want to consider issuing a Position Paper dealing with all forms of emerging payment technologies in which definitions can be stated clearly and any change in regulatory stance explained with reference to other regulatory instruments. It seems that due to the tightening of regulation, the trade-off is in favor of risk management over financial inclusion (access to the payment system). Klein and Mayer make a compelling argument that what mobile banking illustrates in a stark form is the way in

---

[29] See for example the success of M-PESA in Kenya. For more information, see Carmen Nobel, *Mobile Banking for the Unbanked*, HARVARD BUS. SCH. (June 13, 2011), http://hbswk.hbs.edu/item/6729.html.

[30] The Electronic Communications Act 36 of 2005 (S. Afr.) replaced the former Telecommunications Act 103 of 1996 (S. Afr.). This Act aims to converge broadcasting and telecommunications under one regulator. In South Africa, telecommunications are regulated in terms of the Electronic Communications Act. The main authority is the Independent Communications Authority of South Africa, established by Section 3 of the Independent Communications Authority of South Africa Act 13 of 2000 (S. Afr.).

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 institutional lines, like a bank. The question then is what type of regulation is appropriate for each type of service."[31]

Okeahalam examines the NPS from an economic point of view and argues that there may be a trade-off between widening of access in the payment system and systemic risk. Whilst it is difficult to be specific as to the exact cost of widening access, there are financial, microeconomic, and actuarial methods for estimation of risk and relating risk to the welfare benefits of the payment system.[32] It is submitted that Okeahalam is correct in his argument that different payment instruments present different sets of risk to the payment system. It is submitted that a "stratified" regulatory approach could be followed once an analysis has been done of the risk presented by individual instruments, as opposed to the individual institution, as is presently the case. This would mean that the regulatory approach would then be stratified based on the risks presented by the specific payment instrument. This is a challenge which is presently not well researched in South Africa, since the risks are determined based on the profile of the bank or institution. It is further 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 broaden access to financial services to the poor in South Africa.

---

[31] *See* Michael Klein & Colin Mayer, *Mobile Banking and Financial Inclusion: The Regulatory Lessons* 25 (The World Bank, Working Paper No. 5664, 2011), *available at* http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2011/05/18/000158349_20110518143113/Rendered/PDF/WPS5664.pdf.

[32] Charles C. Okeahalam, *Regulation of the Payments System of South Africa*, 4 J. INT'L BANKING REG. 338, 347-48 (2003).

IV. FINANCIAL INTEGRITY

This section deals with anti-money laundering (AML) and combatting financing of terrorist (CFT) concerns as regulated in South Africa. Other policy issues such as seigniorage, operation of monetary policy, and consumer protection concerns fall outside of the ambit of this Article.

A. South Africa

South Africa has criminalized money laundering in three separate provisions of the 1998 Prevention of Organised Crime Act (POCA),[33] which cover the conversion or transfer, concealment or disguise, possession, and acquisition of property in a manner that is largely consistent with the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 U.N. Convention against Transnational Organised Crime (Palermo Convention). POCA provides for both criminal and civil forfeiture. The former is based on conviction of the offender whereas the latter is not dependent on conviction.[34]

Terrorist financing is criminalized in South Africa in Section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA).[35] The POCDATARA is comprehensive and criminalizes the collection or provision of property with the intention that it be used for the purpose of committing a terrorist act, or by a terrorist organization or individual terrorist for any purpose.

Comprehensive AML/CFT preventative measures have been

---

[33] Prevention of Organised Crime Act 121 of 1998 (S. Afr.), *available at* http://www.dac.gov.za/acts/Prevention%20of%20Organised%20Crime%20Act.pdf.

[34] For a comprehensive overview of the applicable legislation, see Louis de Koker, *Money Laundering in South Africa*, *in* PROFILING MONEY LAUNDERING IN EASTERN AND SOUTHERN AFRICA 83 (Charles Goredema ed., 2003), *available at* http://www.issafrica.org/uploads/Mono90.pdf.

[35] Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 (S. Afr.), *available at* http://www.info.gov.za/view/DownloadFileAction?id=67972.

implemented in South Africa through the application of the 2001 Financial Intelligence Centre Act (FICA)[36] and the Money Laundering and Terrorist Financing Control Regulations (MLTFC Regulations), read with various exemptions in terms of the Financial Intelligence Centre Act (Exemptions). The FICA has since been amended in 2008 by the Financial Intelligence Centre Amendment Act, which addressed, *inter alia*, some of the supervisory concerns raised in the FATF mutual evaluation of South Africa undertaken in 2008.[37] While the POCA is the primary piece of legislation in terms of outlining activities that constitute money laundering offences, it does not outline the measures to be implemented to suppress and detect money laundering. Such is provided for in the FICA[38] which is the principle piece of legislation in terms of outlining AML measures.

What follows is a more detailed exposition of the specific issues pertinent to this Article.

B. Analysis

South African AML and CFT laws primarily affect mobile money via the customer due diligence (CDD) requirements that they place upon financial institutions. The CDD measures of the FICA and the POCDATARA are set out in the FICA, read with the MLTFC Regulations. The nature of these CDD requisites and their impact upon mobile money transactions are examined below.

1. Customer Identification and Verification

Section 21 of the FICA places an obligation upon "accountable institutions" to establish as well as verify the identity of their clients. The First Schedule of the Act outlines which institutions

---

[36] Financial Intelligence Centre Act 38 of 2001 (S. Afr.), *available at* http://www.info.gov.za/view/DownloadFileAction?id=68138 [hereinafter FICA].

[37] *See* FIN. ACTION TASK FORCE [FATF], MUTUAL EVALUATION REPORT: SOUTH AFRICA (2009), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20South%20Africa%20full.pdf.

[38] FICA, *supra* note 36.

are accountable institutions in terms of the Act and amongst those listed are banks as well as money remitters. The FICA prohibits these institutions from establishing a business relationship or concluding a single transaction with a person unless they have taken steps to:

- Establish as well and verify the identity of the client; and
- If the client is acting on behalf of another person, or alternatively, if the person acts on behalf of the client, the institution must establish and verify the identity of the other person and their authority to act on behalf of the client, or as the case may be, the client's authority to act on behalf of another person.

Should an accountable institution open an account or conclude a single transaction (once-off) transaction without duly identifying the client it commits an offence in terms of FICA.[39] The penalty for such an offence is imprisonment for a maximum period of 15 years or a fine of ZAR100 million (US$12 million).[40]

The MLTFC Regulations, which have to be read in conjunction with the FICA, give more intrinsic details in regard to how customer identification and verification of such is to be carried out (promulgated by GN No. R1595 in GG No. 24176). The Regulations state that, when establishing and verifying the identity of a client, the following information must be obtained:

- In the case of citizens, their full name, date of birth, identification number, residential address, and tax registration number.[41]
- In the case of foreigners, in addition to the ordinary information that a citizen must provide, they are required to give details in regard to their nationality as well as passport number.[42]

---

[39] *Id.* at § 46.

[40] *Id.* at § 68.

[41] Money Laundering and Terrorist Financing Regulations, Reg. 3, in Government Notice (GN) R1595/2002 4 (S. Afr.) [hereinafter MLTFC Regulations].

[42] *Id.* at 5 (Reg. 5).

The FICA, in contrast to the Exchange Control Act and its Regulations, does not put a duty on financial institutions to determine whether their clients are legally present in South Africa. Hence non-citizens are not required to provide details in regard to their residence or work permit in order for financial institutions to comply with the FICA provisions.[43]

A person's identity has to be verified by means of an identification document.[44] In the case of South African citizens and residents, an official national identity document would need to be presented whereas foreigners have to present a passport.[45] Residential addresses are to be verified using documents such as a utility bill.[46] Records in regard to, amongst other information, a client's identity, as well as transaction amounts, must be kept for a period of five years from the date that the business relationship is established or transaction is concluded.[47]

The regulator was mindful of the fact that the need to present an identity document could prevent individuals without such a document from accessing formal financial services and hence created room for exclusion. The MLTFC Regulations therefore allow financial institutions, in circumstances were it is deemed to be reasonably acceptable for a person to be unable to provide an identity document, to rely on another document issued to that person that bears the following:

- A photograph of the person;
- The person's full name or initials and surname;
- The person's date of birth; and

---

[43] Hennie Bester et al., *Reviewing the Policy Framework for Money Transfers* 18 (FinMark Trust & CENFRI, 2010), *available at* http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf.

[44] MLTFC Regulations, *supra* note 41, at 4-5 (Reg. 4), 6 (Reg. 6).

[45] An identity document is defined in Regulation 1. *Id.* at 3.

[46] Hennie Bester et al., *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines* 10-11 (World Bank First Initiative, Final Report, 2008), *available at* http://www.cenfri.org/documents/AML/AML_CFT%20and%20Financial%20Inclusion.pdf.

[47] FICA §§ 22-23.

- The person's identity number.[48]

Examples of documents that can be accepted as an alternative form of verification in exceptional circumstances are a valid South African driver's license or passport as well as a valid temporary identity document issued by the Department of Home Affairs.[49] The latter documents should be valid in the sense that they must be current and unexpired.

This exemption is, however, not applicable to individuals who are not South African citizens or residents, as no mention of such is made within the Regulations. If the Regulations are strictly implemented, migrants who have neither a passport nor valid travel document in their possession would be unable to access formal remittance services. It is submitted, however, that even if the exception were applicable to foreigners it would likely be of little effect taking into account that studies show that financial institutions such as banks have been hesitant to exercise the discretion bestowed upon them by Regulation 6.[50] The conservative approach has been attributed to the significant fines that are associated with money laundering offences.[51]

---

[48] MLTFC Regulations, *supra* note 41, at 4-5 (Reg. 4(a)(ii)).

[49] Fin. Intelligence Centre Guidance Note 3, Government Notice (GN) R715/2005 (S. Afr.), *available at* http://www.info.gov.za/view/DownloadFileAction?id=61267 [hereinafter FIC Guidance Note]; ABSA Bank, Establishing and Managing Business Relationships – Customer Identification and Verification, Compliance Document: FICA (Dec. 17, 2010), *available at* http://www.absa.co.za/deployedfiles/Absa.co.za/PDF%27s/About%20Absa/Absa%20Group/Compliance%20Documents/Financial%20Intelligence%20Centre%20Act.pdf.

[50] For more detail on financial inclusion, see Louis de Koker & John Symington, *Conservative Compliance Behaviour* (FinMark Trust, 2011), *available at* http://www.cenfri.org/k2/item/95-conservative-compliance-behaviour-2011. This study is the most recent study which also highlights trends in bank behaviour. *See also* CONSULTATIVE GRP. TO ASSIST THE POOR [CGAP] & THE WORLD BANK, FINANCIAL ACCESS 2010: THE STATE OF FINANCIAL INCLUSION THROUGH THE CRISIS (2010), *available at* http://www.cgap.org/gm/document-1.9.46570/FA_2010_Financial_Access_2010_Rev.pdf; GPFI & INT'L FIN. CORP., FINANCIAL INCLUSION DATA: ASSESSING THE LANDSCAPE AND COUNTRY-LEVEL TARGET APPROACHES (2011), *available at* http://www.gpfi.org/sites/default/files/documents/WORKINGDATA.pdf.

[51] Bester et al., *supra* note 46, at 144.

Ideally the information gathered in identifying a client should enable a financial institution to form a client profile. According to de Koker, many South African institutions are unable to form an individual comprehensive client profile for general financial service customers that would support effective AML/CFT monitoring for unusual activity.[52] This is due to the fact that under ordinary circumstances financial institutions are only obliged to obtain information that pertains to the personal identity of the client. Such particulars only play a small role in building a client profile and are insufficient to enable a financial institution to effectively detect suspicious financial activity by a client.

For a client profile to effectively be established, information such as the source of the client's income would be needed. Financial institutions are only obliged to obtain such information in the case of business relationships or transactions that present a high risk of facilitating money-laundering activities.[53]

In circumstances where a business relationship or once-off transaction presents a high risk of facilitating money laundering or where it is necessary for a financial institution to identify the proceeds of unlawful activity or money laundering, *inter alia*, the following must be ascertained:

- The source of the client's income; and
- The source of the funds which the client intends to use to conclude the transaction or series of transactions in the course of a business relationship.

Professor de Koker states that the procedure prescribed by the current Regulation 21 is essentially a "Know Your Customer" or CDD procedure, in contrast to the ordinary procedure of identifying clients which is merely a "Client Identification and Verification" procedure .[54]

---

[52] Louis de Koker, *Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001,* 4 J. OF S. AFR. L. 715, 723 (2004).

[53] MLTFC Regulations, *supra* note 41, at 15 (Reg. 21).

[54] de Koker, *supra* note 52, at 724.

2. The Provision and Verification of a Residential Address

The obligation to provide an address and the need for such to be verified appears to have been the chosen safeguard against identity fraud. The value of providing a residential address for purposes of identifying a customer has been questioned. It is argued that such a requirement may be more useful in developed countries without a system of national identity numbers, but with rich sources of data on their residents.[55] In such countries, addresses are helpful to distinguish between different people with similar names, but are less functional in countries with comprehensive national identification systems. Once an accountable institution obtains a client's name, date of birth, and unique national identity number, there is no need for it to obtain a residential address. Requiring address verification under these conditions does not add significant identification value, but causes undue hardship for customers who often lack formal addresses.

Professor de Koker argues that the negative impact of residential address verification increases as a result of the high level of internal migration in South Africa.[56] Such arguments become relevant when one considers the practical difficulties that have been experienced in South Africa in verifying the residential addresses of individuals.

In South Africa, the verification of a client's address has presented certain difficulties, particularly with low-income individuals.[57] The drafters of the FICA and its Regulations were aware of the fact that individuals who lived in informal settlements and rural areas could face problems in verifying their residential address in accordance with the regulatory requisites.[58] As a consequence, room for exception from the need to provide a residential address was created by means of "Exemption 17." The

[55] *Id.* at 742.
[56] *Id.*
[57] Bester et al., *supra* note 43, at 18.
[58] Louis de Koker, *The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa: Findings and Guidelines*, 12 J. MONEY LAUNDERING CONTROL 323, 325 (2009).

latter is contained within the Schedule to the MLTFC Regulations.[59]

3. Enhancing Financial Inclusion: Exemption 17 and Mobile Money

Exemption 17 relieves certain financial institutions from the general obligation placed upon them by Section 21 of the FICA, which requires them to attain as well as verify their customer's residential address. The exemption is only applicable if certain requirements are fulfilled. Exemption 17 was included in the original set of Exemptions, but it proved of little value in practice as the requirements were too rigid and could not be met by many unbanked persons. Exemption 17 was therefore revised in 2004.[60]

The amendments were informed by actual market research and take the needs of the financially excluded into account.[61] According to Isern and de Koker, this framework allows "financial institutions to verify a person's identity using the national ID document without having to verify the person's residential address if the financial product meets a certain balance limit (US$3,000) and transaction restrictions (US$600 per day)."[62]

The amended Exemption 17 facilitated the launch of the Mzansi account[63] that has reportedly brought over 6 million people into the formal financial sector.[64]

---

[59] Exemptions in Terms of the Financial Intelligence Centre Act of 2001, Exemption 17, Government Notice (GN) R1596/2002 9-10 (S. Afr.).

[60] Exemption in Terms of the Financial Intelligence Centre Act of 2001, Government Notice (GN) R1353/2004 (S. Afr.), *available at* https://www.fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/10.Revised%20exemption.pdf [hereinafter FICA Exemption 17].

[61] de Koker, *supra* note 52, at 729; Hennie Bester et al., *Legislative and Regulatory Obstacles to Mass Banking* 65-66 (Genesis Analytics, 2003), *available at* http://dro.deakin.edu.au/eserv/DU:30016861/dekoker-legislativeandregulatory-2003.pdf.

[62] Jennifer Isern & Louis de Koker, *AML/CFT: Strengthening Financial Inclusion and Integrity* 10-11 (CGAP, Focus Note No. 56, 2009), *available at* http://www.cgap.org/gm/document-1.9.37862/FN56.pdf.

[63] The Mzansi account is a savings account with basic transaction capability aimed at the low-income market.

[64] See the data in BANKABLE FRONTIER ASSOC., THE MZANSI BANK

The Financial Intelligence Centre (FIC) has, in addition, issued guidance notes as contemplated in Section 4(c) of the FICA, which provide guidance to banks in regard to which documents qualify as acceptable verification documentation. In establishing and verifying customer identity, banks are encouraged to undertake a "risk based approach" as opposed to following a "one size fits all approach."[65]

Exemption 17 also enabled the creation of a simplified CDD framework for mobile money. The Banks Act Guidance Note of 2008 issued by the Registrar of Banks brought mobile banking products within the framework of Exemption 17. The product is offered to clients via a non-face-to-face process, which must be followed only on the basis of the minimum set of criteria being met. Importantly, however, a lower daily transaction limit of ZAR1,000 (US$120) per day is set.[66] If a client wishes to exceed this limit, the normal verification procedures would have to be followed. Finally, the Guidance Note states that the "expansion of banking services should not happen to the detriment of control measures that are aimed at facilitating the detection and investigation, or even the prevention, of money laundering and terrorist financing through banks."[67]

It is submitted that the relief granted by Exemption 17, even in its amended form, is only partially effective in achieving the desired effect of increasing financial inclusion. This is taking into account that the exemption only provides room for exception in regard to the ascertainment of a client's residential address; it does not absolve individuals from presenting an identity document. In addition to the latter, the exemption does not apply to cross-border

---

ACCOUNT INITIATIVE IN SOUTH AFRICA 3 (2009), *available at* http://www.gatewaytosavings.org/cmsdocuments/MzansiProject-FINAL_REPORT_March202009.pdf.

[65] FIC Guidance Note, *supra* note 49. For more detail on the risk-based approach, see also de Koker, *supra* note 58.

[66] Banks Act Guidance Note 6/2008 from E.M. Kruger, Office of the Registrar of Banks, to All Banks, Controlling Companies and Branches of Foreign Banks, at 2 (May 7, 2008), *available at* http://www.cgap.org/gm/document-1.1.6005/SARB%20Guidance%20Note%206%20of%20on%202008%20Cell-Phone%20Banking.pdf.

[67] *Id.*

transactions that go beyond the Common Monetary Area (CMA), comprised of South Africa, Lesotho, Namibia, and Swaziland.[68] Transactions that go beyond the CMA are still subject to the stringent CDD requisites imposed by FICA. Furthermore, the exemption only applies to certain accountable institutions and not all of them. Mobile money transfer businesses, unlike banking institutions, have not been included within the scope of the exemption.

Asylum seekers have been dealt a major blow by the May 2010 FIC advisory issued to banks that banks are not allowed to transact with asylum seekers based on the official certificates and permits issued by the South African government. This means that an asylum seeker is barred from opening a bank account and conducting transactions until the application for asylum is processed, asylum was granted and the refugee was issued with a more formal maroon South African refugee document. Before the issuing of the interpretation, they were allowed to rely on the permits and licenses to open accounts. Since the interpretation was issued, asylum seekers have reported that banks have also refused them permission to withdraw their funds from the accounts that they have previously opened, causing severe personal hardship.[69] Not only was the FIC advisory ineffective communication, it was also confrontational and upset a practice which banks have adopted as early as 2003.

A compromise has since been reached following litigation challenging the position of the FIC allowing banks to accept asylum documentation to verify identify only after verifying the authenticity of the document with the South African Department of Home Affairs.[70]

---

[68] FICA Exemption 17, *supra* note 60, at 6.

[69] *See* FATF, FATF GUIDANCE ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION (2011), *available at* http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf.

[70] For more information on the debacle, see Tatenda Gumbo, *S. African Court Restores Access to Bank Accounts by Refugees and Asylum Seekers*, VOICE OF AMERICA ZIMBABWE (June 8, 2012), http://www.voazimbabwe.com/content/south-acrican-court-restores-bank-access-for-refugees-107057558/1459047.html.

Despite the compromise, the hardship for undocumented migrants deepened when they lost their access to mobile communication in South Africa. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)[71] of 2002 introduced customer identification and verification measures that are very similar to the FICA CDD requirements. Users have to verify their identities using official documentation to access mobile communication services. Foreigners without passports are generally not able to legally gain normal access to South African-issued mobile phones. They are therefore faced with mobile money access barriers created by RICA as well as FICA. A recent report stated:

> Refugees are vulnerable to the high levels of random crime that afflict South Africa, as well as sexual and gender-based violence, exploitation in the workplace and detention due to lack of proper documentation. Poor socio-economic conditions among host communities provide a breeding ground for xenophobia. Documents of limited validity compromise refugees' efforts to become self-reliant by making it hard for them to hold long-term jobs, while at the same time a law allowing refugees and asylum-seekers to have bank accounts is not being fully implemented.[72]

The fact that a passport must be presented effectively bars undocumented migrants who do not have valid travel documents from accessing formal remittance services. Migrants who live in informal settlements[73] are also barred from accessing formal remittance channels as they are unable to fulfill the address

---

[71] Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (S. Afr.), *available at* http://www.internet.org.za/ricpci.html.

[72] *See South Africa*, THE UN REFUGEE AGENCY, http://www.unhcr.org/pages/49e485aa6.html (last visited Aug. 27, 2012).

[73] HUMAN SCIENCES RESEARCH COUNCIL, CITIZENSHIP, VIOLENCE AND XENOPHOBIA IN SOUTH AFRICA: PERCEPTIONS FROM SOUTH AFRICAN COMMUNITIES 16 (2008); Glenn Ashton, *Xenophobia Redux*, S. AFR. CIVIL SOCIETY INFO. SERV. (July 7, 2010), http://sacsis.org.za/site/article/510.1.

verification requisite imposed by FICA. In view of the above, it is submitted that regulators should give more thought in making policy that would align AML/CFT, financial inclusion, the regulation of telecommunications service providers who offer mobile money services, as well as South Africa's international obligations to alleviate the plight of refugees.

In his Article on the 2012 FATF Standards, de Koker notes that the risk-based approach is now mandatory for countries and institutions and that the cornerstone of the risk-based approach is risk assessment. It is interesting to note that South Africa has to some extent followed a risk-based approach, but to date no formal risk assessment has taken place. The current CDD requirements, for example, were based on the previous FATF Recommendations. Regulation 21, for example, was based on the predecessor of 2003 Recommendation 5, which has now, in turn, been replaced by Recommendation 10. In effect this would mean that South Africa would have to conduct a formal risk assessment and in a sense conduct a "gap analysis" of the current CDD requirements as contained in the FICA and regulations thereto and match this against the new 2012 FATF Standards. Furthermore, lower-risk and higher-risk scenarios would have to be determined. Should the risk assessment show that mobile money is considered a "lower risk" product, the effect would be that the limits imposed would have to be commensurate with the risk identified, i.e. the lower the risk, the more simplified the measures should be. It would be interesting to see how this would be done in South Africa, where, as stated earlier, even though a "risk-based approach" was followed in the past, a formal risk assessment would now have to take place. It is hoped that in the formal risk assessment, a more equitable system would be employed as far as migrant workers who come from outside the CMA are concerned.[74] This would

[74] For example, mobile money could be regarded as "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes." FATF, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS 64 (2012), *available at* http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20Februar

mean that regulators would have to show more faith in refugees and asylum seekers in amending Exemption 17, which remains to be seen.[75]

Even if the AML barriers are removed, refugees and asylum seekers are still faced with the barriers imposed by RICA.[76] In effect this would mean that if a risk assessment is made for South Africa and a distinction is made between low-risk and high-risk scenarios, RICA would likewise have to be amended to allow for greater financial inclusion in line with the risk-based approach to be followed and formalised through the formal risk assessment.

4. Cross-Border Networking

If one is to take a look at the effects of AML measures upon the remittance industry from a wider perspective the FATF Standards become relevant. The 2012 FATF Standards deal with correspondent banking relationships in Regulation 13. Financial institutions that are involved in correspondent banking relationships must gather information about their counterparty's business, which includes their AML and CFT supervision, investigation and regulatory action, and their AML/CFT controls. Furthermore, these financial institutions should obtain approvals from senior management before establishing new correspondent banking relationships; they must clearly understand the respective responsibilities of each institution and be satisfied that the respondent bank has conducted CDD on its customers who have direct access to accounts of the correspondent bank.

New Recommendation 14 provides that countries should take measures to ensure that natural or legal persons who provide

---

y%202012)%20reprint%20May%202012%20web%20version.pdf. For more detail, see Louis de Koker, *The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework*, 8 WASH. J.L. TECH. & ARTS 165, 175 (2013).

[75] For more detail see de Koker, *supra* note 58, at 328.

[76] *See* Louis de Koker, *Will RICA's Customer Identification Data Meet Anti-Money Laundering Requirements and Facilitate the Development of Transformational Mobile Banking in South Africa?* (FinMark Trust, Exploratory Note, 2010), *available at* http://www.cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf.

money or money value transfer services are licensed or registered and subject to effective systems for monitoring and compliance with the relevant measures called for in the FATF Recommendations. South Africa would need to ensure that this is accommodated for in its legal framework.

V. RECOMMENDATIONS

Policy makers may need to consider some potentially new challenges posed by technological innovation and other changes in the payment system more generally as well as how these impact regulatory approaches with respect to AML/CFT. For instance, mobile money products in some countries may be offered by entities other than institutions subject to banking supervision, although many countries apply anti-money laundering laws to all institutions.

The extent of CFT/AML regulation should depend on the relative attractiveness for money launderers and risk posed by such a scheme. In other words, if a risk-based approached is followed, the level of regulation would be relative to the risk introduced by such system. It is recommended that a stratified approach to regulation of m-money be followed, viewed from a risk-based AML/CFT perspective.

The following factors could be taken into consideration to arrive at such a stratified approach based on the service rather than the institution:

- Semi-open systems – A limited form of regulation could be applicable. Issuers could be licensed as M-Money Issuers similar to the EU or U.K. position or Authorized Institutions similar to the Hong Kong position. One of the conditions could be to place a limit on the value on the card similar to the U.K. position.

- Open loop systems – In consultation with the SARB on oversight and supervisory issues, open loop systems would be regulated by the SARB in terms of its E-money Position Paper which restricts such systems to banks. However, from an AML/CFT perspective, the FIC could add provisions in the Regulations which would state that reporting on m-money products have to be done as part of

> such bank's obligations as an accountable institution in terms of FICA and the Regulations.

The relief granted by Exemption 17, as mentioned previously, is only partially effective in facilitating greater financial inclusion. The view is taken bearing into account that Exemption 17 is not applicable to certain mobile money transfers, namely remittance transactions that go beyond the CMA,[77] nor does it apply to financial institutions that provide mobile money transfers (remittance services) as their only business.[78] Hence, migrant laborers who live in informal settlements face a significant barrier in accessing formal remittance services as they are likely to face significant difficulty in verifying their residential address. An amendment of Exemption 17 is thus needed if the trade-off has to be in favor of financial inclusion. It is always difficult to balance financial integrity on one hand and the concern of financial inclusion on the other. South Africa would have to conduct a formal risk assessment in accordance with the mandatory risk-based approach advocated in the 2012 FATF Standards. This means that there is an opportunity to align the South African legal framework with the 2012 FATF Standards and hopefully, also amend Exemption 17 to be more inclusive, depending of course on the outcome of the formal risk assessment of course. This would also mean that the obstacles imposed by RICA be revisited in light of the formal risk assessment mandated by the 2012 FATF Recommendations.

CONCLUSION

This Article gives an overview of the legal and regulatory framework for mobile payments in South Africa. While the legal and regulatory framework is, for the most part, sound, the Article identifies risks, challenges, and uncertainties that regulators may take into account. The analysis also examines the significance of the South African Reserve Bank's 2009 Position Paper on Electronic Money, the reasons for the change in regulatory stance,

---

[77] FICA Exemption 17, *supra* note 60, at 6.
[78] FICA Exemption 17, *supra* note 60.

and the effect that this may have on financial inclusion (access to the payment system) for non-bank mobile payment providers. 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 financial inclusion to the payment system if it is found that there is over-regulation of mobile payments in South Africa. What may be needed is a stratified regulatory approach, that is, that regulation be structured by service rather than along traditional lines and that the focus should be on what type of regulation would be appropriate for which type of payment. The opportunity now arises to address this through a formal risk assessment, as mandated by the 2012 FATF Standards, as well as an amendment to RICA to remove the obstacles for refugees and asylum seekers. If this is not done properly, the clear benefits of mobile money as shown in Kenya may not be realized in South Africa.