# Know-Your-Customer measures: Mitigating money-laundering risks in mobile banking transactions

**H NEL**

**10968660**

Dissertation submitted in fulfilment of the requirements for the degree *Master of Law* in Trade and Business Law at the Potchefstroom Campus of the North-West University

Supervisor: Prof SF du Toit

March 2017

**Summary**

The backbone of a modern, developed, strong economy and a stable, transparent financial market is the ability to effect payments securely, efficiently and unambiguously through sound payment systems. Conversely, the reality we face is that banks do not find it economically viable to establish banking infrastructure in economically disadvantaged communities.[1] This approach contributes to and exaggerates the disparities of those individuals living in low-income areas and as such this business model requires transformation. The emergence of new financial ecosystems known as mobile network operators (hereinafter MNOs),[2] with products such as mobile money, has the ability to fuel economic growth and yield major social benefits by improving financial inclusion for the poor; however, at the same time such innovations create numerous opportunities for criminals who have identified weaknesses within the financial system.

This dissertation seeks to highlight the growth and financial inclusion potential of mobile money, whilst examining whether this presumably low-risk product and the exemption provided to low-income individuals, in the spirit of financial inclusion, still appropriately mitigates potential money laundering and terrorist financing risks.

South Africa's anti-money laundering and countering the financing of terrorism approach, which is found in the *Financial Intelligence Centre Act* 38 of 2001, has forced banks to assess and understand who their clients are, to reshape their value proposition to risks and to engender a compliance culture. The ultimate purpose of the application of client due diligence (i.e. know-your-client principles) is to provide a foundation for banks to understand their clients' potential exposure to money laundering and terrorist financing risks.

1 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

2 Mobile Network Operators operate the uses of mobile airtime currency which is prefunded electronic stores of value which is housed in stored value accounts on a mobile phone, subject to s 1 of the *Banks Act* 94 of 1990.

The application of an effective anti-money laundering and countering the financing of terrorism compliance culture is not without challenges. It may be noted that the regulatory framework is not entirely conducive to the principle of financial inclusion for low-income individuals, who are often not able to produce verifiable residential address documentation. This has forced central banks globally to review their regulatory and supervisory policy responses to the evolution of new payment technologies and the application of a risk-based approach. The application of a risk-based approach to products, client and/or transactions permit banks to focus their time and resources on the areas which requires more attention, due to the perceived money laundering and terrorist financing risks it poses to the business.[3] The redrafted Exemption 17 *Financial Intelligence Centre Act* 38 of 2001 and *Bank Act* 94 of 1990 Circular 6 of 2008 (hereinafter the *Banks Act* Circular) was specifically designed to overcome the obstacles of producing verifiable residential address documentation by applying simplified due diligence procedures to confirmed low-risk products or clients.

Although electronic or e-banking has reduced the inherent risks of a cash-based system, the elusiveness, anonymity, low risk rating, high marketability, global access to bank networks and poor supervision are all vulnerabilities which money launderers will use to their advantage.[4] Within this space launderers benefit the most from having various juridical personalities, non-face-to-face business relationships, creating a network of artificial trading, false identities and the absence of credit risks due to the prepaid system.[5]

Mobile banking transactions are perceived to be low risk based on the low transactional threshold limit and the type of client target market. In pursuit of financial inclusion and a cashless environment, payment transfer via mobile banking has risk elements of elusiveness, anonymity, high marketability, global access to bank networks, low risk rating and poor supervision. Although low risk products, clients and/or transaction are crucial to the increase of financial inclusion, it is often

---

3 De Koker 2004 *TSAR* 720 and Financial Intelligence Centre unknown date https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf.

4 World Bank 2008 http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf .

5 Souto 2013 *Journal of Money Laundering Control* 267.

disregarded for ML/TF risks, as more attention are allocated to high risk money laundering and terrorist financing risk areas.[6] It is within this space that launderers and terrorist financiers identify the gaps and opportunities of possible abuse.

**Key terms:** anti-money laundering, client identification and verification, countering the financing of terrorism, electronic banking, enhanced due diligence, Exemption 17 of the *Financial Intelligence Centre Act* 38 of 2001, mobile banking transactions, money laundering, simplified due diligence and terrorist financing.

[6] De Koker 2009 *Journal of Financial Crime* 338-340.

**Acknowledgement**

Firstly, I wish to express my sincere gratitude towards my study supervisor, **Prof Sarel Du Toit** for his inputs and continued support during my study.

A special word of thanks goes to my colleagues, **Abi-gail Marshman** and **Maarten Fouché**, who were always willing to be my sound-board for exchanging insights, ideas and interpretive approaches to the relevant legislation.

Furthermore, I wish to use this opportunity to express my gratitude towards **Diana Coetzee** and **Herco Steyn**, my language editors, who have done this task with such commitment and professionalism. Their inspiring guidance and invaluable constructive criticism assisted in producing this dissertation.

For the last few years my family has been the solid foundation in my journey to complete my studies. In this regard special thanks go to my mother, **Lasya Nel**, sisters, **Rachel Botha** and **Lasya Nel**, and my great friend **Marilie Swarts** for providing me with your unfailing support and continuous encouragement. This accomplishment would not have been possible without them.

My late father, **Johan Nel**, warrants a special mention as it was due to his exemplified character, motivation and support that it was possible for me to have accomplished this. He was one of the most humble persons I know. His support and interest in my studies always encouraged me.

I would also like to express my deepest appreciation towards the **South African Reserve Bank** for their financial support towards the binding costs of my dissertation.

Lastly, this dissertation would not have been possible without the grace of **God** and the sacrifices and dedication of my family.

HETTIE-ANNETTE NEL

January 2017

**Contents**

# CHAPTER 1

## SCOPE, STRUCTURE AND RESEARCH METHODOLOGY

*If power corrupts, then automatic power corrupts automatically.*[7]

## 1 Introduction

The current age of globalisation is characterised by a need for rapid mobility of funds through the introduction of faster and innovative payment systems. The use of new payment technologies such as electronic banking (hereinafter e-banking) and more particularly mobile banking (hereinafter m-banking) transactions have not only enhanced accessibility to the financial market for the unbanked, but coincidently also contributed to money-laundering and/or terrorist financing (hereinafter ML/TF), being regarded as a globalised crime.[8] It follows therefore that the proliferation of technology has potentially shifted conventional m-banking transactions to invisible and faceless carriers.[9]

The 2004 redrafted Exemption 17 *Financial Intelligence Centre Act* 38 of 2001 (hereinafter *FICA*) and *Banks Act* Circular 6 of 2008 was specifically designed to overcome the obstacles of producing verifiable residential address documentation by applying simplified due diligence (hereinafter SDD). Thus, in the spirit of promoting financial inclusion, Exemption 17 of *FICA* allows banks to reduce the client identification and verification (hereinafter CIV) obligations[10] and to apply SDD to confirmed low risk clients and products (i.e. m-banking), subject to the discharge of certain requirements. It is believed that Exemption 17 of *FICA* provides a good example of the balance between risk management and financial inclusion.

Although m-banking has reduced the inherent risks of a cash-based system the elusiveness, anonymity, low risk rating, high marketability, global access to bank networks and poor supervision are all vulnerabilities which money launderers will use

---

7 Grimmelamann 2014 http://ssrn.com/abstract=2358627.
8 Souto 2013 *Journal of Money Laundering Control* 266.
9 Vlcek 2011 *Development Policy Review* 424.
10 Section 21 of *FICA* 38 of 2001.

to their advantage.[11] It is accordingly within this space that launderers and terrorist financiers benefit the most as m-banking provides a platform for various juridical personalities, non-face-to-face business relationships, creating a network of artificial trading, false identities, including the absence of credit risks due to the prepaid system.[12]

Stemming from the above, this dissertation seeks to highlight, through qualitative research, the growth and financial inclusion potential of mobile money, whilst at the same time examining whether this presumably low-risk product and the application of an exemption to the CIV requirements for low-income individuals, in the spirit of financial inclusion, does mitigate potential ML/TF risks.

## 2 Background to problem statement

M-banking has forever altered financial services in the most profound way for the unbanked[13], underbanked[14] and the world's poorest people. Triggered by technological development, m-banking transactions have in recent years become more prevalent than any other financial market instrument.[15] What used to fit inside an entire building now fits inside your pocket.

The accessibility to money is no longer constrained to the ambit of the traditional banking sector. The proliferation of technology has shifted conventional m-banking transactions to invisible and faceless carriers.[16] According to the 2016 Ericsson Mobility Report,[17] the mobile subscription growth rate is 3 per cent year-on-year (i.e. 7.4 billion mobile subscriptions). Ericsson estimated that the global mobile broadband subscription will grow to 7.7 billion by 2021, which will have a ripple effect on the

---

11 World Bank 2008 http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf.

12 Souto 2013 *Journal of Money Laundering Control* 267.

13 "Unbanked" is used as a slang term and refers to those individuals who generally pays for thing in cash and do not use or have access to bank accounts/facilities, as described and defined in Investopedia 2015 http://investopedia.com/terms/u/unbanked.asp.

14 "Underbanked individual" refers to individuals who has an account, but who also has availed of at least one alternative financial service in the past 12 months, as defined in Gross *et al* 2012 http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf.

15 European Central Bank 2012 http://ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

16 Vlcek 2011 *Development Policy Review* 424.

17 Ericsson 2016 https://ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf.

emergence of mobile transactions applications and growing risks with regard to financial crime, ML/TF, regulation and information technology access. In its April 2015 press release, the World Bank confirmed that the number of unbanked people globally has decreased by 20 per cent to 2 billion adults.[18] In view of the above, the application of effective and financially inclusive anti-money-laundering and countering the financing of terrorism (hereinafter AML/CFT) measures is vital in protecting the safety and soundness of banks, and the integrity of international financial systems.[19]

In terms of Exemption 17 of *FICA* and subject to certain conditions being met, banks are exempted from obtaining and verifying the addresses of clients. Thus, simplified know-your-client (hereinafter KYC) measures could be applied to those individuals living in informal or rural settlements, where providing proof of residential address may be difficult.[20] Lawack,[21] however, believes that South Africa's legal and regulatory framework for m-money is not fully inclusive due to the challenges around undocumented migrants.

Stemming from the assessment conducted of Exemption 17 (i.e. m-banking) transactions in terms of *FICA*, it has been noted that although the low prescribed threshold limit applied to m-banking transactions (i.e. not exceeding R5 000.00 per day and not exceed R25 000.00 in a monthly cycle)[22] appears to be small in value, but the volume of transactions effected through South African commercial banks is vast. Based on the fact that this type of product would be regarded as low risk, very little (indeed if any) transaction monitoring would be applied to assist banks in identifying possible abuse of the product.

While automated payment systems, such as m-money, make financial services accessible to the unbanked, at the same time it creates a funnel of opportunities for criminals who have identified weaknesses within the financial system. It has been noted that m-banking facilitates the transfer of value through electronic

---

18 World Bank 2015 http://worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report.

19 Basel Committee on Banking Supervision 2014 *Sound management of risks related to money laundering and financing of terrorism* http://bis.org/press/p140115.htm.

20 De Koker 2009 *Journal of Money Laundering Control* 330.

21 Lawack 2013 *Washington Journal of Law, Technology and Arts* 317.

22 Section 21 read with Exemption 17 of *FICA* 38 of 2001.

payment systems, without any reference being made to the identity of the beneficiary thereof.[23] From the number of fraud and ML cases cited since the inception of Mzansi accounts,[24] it is evident that e-banking and specifically m-banking products are not resistant to criminal manipulation.[25]

## 3 Structure of dissertation and outline of chapters

This study aims to provide an economic, commercial, technical, legal and regulatory overview of m-banking transactions and present evidence of the development of possible ML/TF risks link to the application of SDD to low-risk products. It follows therefore that this study comprises five chapters, including this one. As such the main focus points of each chapter are set out below and will generally cover the problem statement as articulated in the next section.

*Chapter 1*: Serves as the introductory chapter to the dissertation topic, which includes the problem statement discussion.

*Chapter 2:* Focuses on the literature review and introduces concepts such as money, legal tender, unbanked, branchless banking, e-banking, m-banking, mobile money, ML and TF.

*Chapter 3:* Provides an extensive overview of the various types of e-payments available. The pros and cons of electronic money vs paper money are considered. The concepts of financial inclusion, financial integrity, risk-based approach (hereinafter RBA) and financial crime are discussed. The chapter also highlights and provides another vantage point for the new and various types of illicit uses of digital money such as mobile money (e.g. digital smurfing, fraud, drugs etc.).

---

23 Popa 2012 *Metalurgia International* 219.

24 Mzansi account refers to "an entry-level bank account, based on a magnetic stripe debit card platform, developed by the South African banking industry and launched collaboratively by the four largest commercial banks together with the state-owned Postbank in October 2004" as described and defined FinMark Trust 2009 http://bankablefrontier.com.

25 De Koker 2009 *Journal of Money Laundering Control* 324; *USA v Liberty Reserve S.A. and 7 others* [2013] CRIM 368 (United States District Court, Southern District of New York) and Reuters 2016 http://reuters.com/article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB. During the end of May 2016 criminals managed to counterfeit Standard Bank credit card and withdraw 1.4 billion yen (approximately USD 3 million) via effecting in 14 000 transactions using ATM machines.

*Chapter 4*: Provides an overview of the international standards on AML/CFT measures, which include the Financial Action Task Force (hereinafter the FATF), the Wolfsburg Group and the Basel Committee on Effective Banking Supervision (hereinafter the Basel) standards on managing AML/CFT risks within new technologies. The concept of the application of *lex lata, lex ferenda* and the application of the proportionality principle are also explored.

*Chapter 5:* Looks at the national regulatory framework applied to m-banking transactions and investigates the regulatory challenges posed by mobile innovation. This chapter also looks at the application of KYC, SDD, the RBA vs rule-based approach, and provides an analysis of the challenges in the application of Exemption 17 of *FICA, Banks Act* Circular 6 of 2008, *Banks Act* Guidance Note 6 of 2008 (hereinafter GN 6) and Financial Surveillance Department's (hereinafter the FinSurv) cross-border remittance exemption.

*Chapter 6:* Provides a summary of the dissertation and recommendations.

In order to commence with the investigation of whether this presumably low-risk product (i.e. m-banking transactions), an exemption from the CIV requirements, and in the spirit of financial inclusion, do in fact mitigate potential ML/TF risks, it is important to have a meaningful discussion of CIV requirements, the RBA, SDD, challenges in the application of Exemption 17 of *FICA*, *Banks Act* Circular 6 of 2008, GN6 and new digital crimes, which will be covered in chapters 2 and 3.

## 4 Problem statement

From the above the following problem statement can be formulated:

| **Problem statement** |
| --- |
| To what extent, if any, does the application of the Know-Your-Client measures in mobile banking transactions mitigate money-laundering risks? |

## 5 Aim of study

The aim of this study is to determine to what extent, if any, presumably low-risk product such as m-banking transaction and the application of an exemption to the CIV requirements, in the spirit of financial inclusion, could make it susceptible to ML and TF risks. Firstly an analysis of the current concepts of "money" is conducted, followed by an overview of the application of m-banking models and how international standards (e.g. FATF Recommendations) and domestic regulation (e.g. *FICA*) are applied. Like many banking products, m-banking transactions are not immune to criminal abuse and as such the focus on new trends of criminal abuse in m-banking transactions will be highlighted to identify possible regulatory gaps. These gaps will provide the reader with a better understanding of the actual and perceived ML and TF risks. This will determine whether and how domestic regulation can improve its current approach to perceived low-risk products such as m-banking transactions.

## 6 Research methodology

ML refers to any act or attempt to conceal the identity of illegally obtained proceeds derived from predicate activities such as the shadow economy (e.g. tax evasion) and white-collar cross-border crime (e.g. capital flight, and under- and over-invoicing).[26] The employment of research methods such as case studies, proxy variables or models have proven to under- or overvalue ML.[27] The nature of predicate activities commands a different approach, as a number of academics[28] have realised that it is not possible to assess the quality and/or effect of ML, as not all predicate offences are linked to ML. It is thus not immediately apparent how best to measure something this is unobservable.[29]

---

[26] Popa 2012 *Metalurgia International* 219 and Unger "The Gravity Model for Measuring Money Laundering and Tax Evasion" 1-4

[27] Unger "The Gravity Model for Measuring Money Laundering and Tax Evasion" 1-4.

[28] Unger "The Gravity Model for Measuring Money Laundering and Tax Evasion" 1-4; Chong and López-de-Silanes *Money Laundering and its Regulations* 11-12 and Masciandaro 1998 *Journal of Money Laundering Control* 49-51.

[29] Unger "The Gravity Model for Measuring Money Laundering and Tax Evasion" 1-4; Chong and López-de-Silanes *Money Laundering and its Regulations* 11-12 and Masciandaro 1998 *Journal of Money Laundering Control* 49-51.

Stemming from the above, a large portion of this study will be based on an analytical review of the literature, an analysis of international AML/CFT standards, legislation, academic articles, case law, various textbooks, academics' opinions and electronic sources, which will specifically focus on the CIV obligations placed on the banking industry, in terms of section 21 of *FICA*, read with Exemption 17, the 2012 FATF Recommendations and the developments on the regulatory aspects in m-banking.

All the resources used in the literature reviews were drawn from open sources which are accessible on websites and from the subscription databases of the South African Reserve Bank and North West University Library available to authorised employees and registered students.

## 7 Delimitation, limitation and assumptions of scope

The analysis and investigation in this dissertation will be limited to South African regulatory challenges in the application of exemptions to the CIV obligations, as set out in section 21 of *FICA*, and the rapid evolution of faceless predicate activities linked to ML/TF through the use of m-banking transactions. Due to the faceless nature of m-banking transactions, and the limited number of confirmed and documented cases of TF, the analysis linked to the financing of terrorism will be relatively limited. Furthermore, the analysis of m-banking transactions will be a constraint to the use of m-banking services and not mobile securities accounts. Also, digital currencies such as virtual currency (e.g. BitCoin) will not form part of the scope of discussions linked to mobile money or mobile money transactions. This study is limited to the banking industry and its provision of m-banking transactions to its clients.

Stemming from the above the following assumptions can be made:

a. the development of new payment technologies such as m-banking will require the enhancement of policies and regulatory legislation relating to AML and CFT;

b. financial service providers, such as banks, telecommunications providers and money remitters, play a key role in realising the CIV obligations contained in section 21 of *FICA*; and

c. regulators may overlook the possibility of ML and TF abuse in lower-value transactions, such as those involving m-banking.

## 8 Concluding remarks

The advancements in information technology have revolutionized the way in which banks operate and conduct business.[30] M-banking has proven itself to be the most successful business-to-customer product.[31] These innovative payment technologies has cause banks to alter their strategies to attack new clients, retain existing clients for business growth and simultaneously required banks to identify, understand and manage possible ML and TF risks. From my research on the dissertation topic, I was unable to find any quantitative research which confirms that the application of SDD to presumably low risk products or clients, such as m-banking product, does mitigate ML/TF abuse.

[30] Al-Jabir 2012 *Journal of Electronic commerce Research* 379 -380.

[31] Pousttchi and Schuring 2004 http://doi.ieeecomputersociety.org/10.1109/HICSS.2004.1265440.

## CHAPTER 2

## THE CONCEPT OF MOBILE MONEY AND MONEY LAUNDERING

*Next to language, money is the most important medium through which modern societies communicate.*[32]

### 1 Money

Similar to the way in which language functions as "currency" to unlock meaning and facilitate communication, money itself may analogously be regarded as the fuel that powers the engine of economic and social development. It creates, transforms, transports and possesses meaning by virtue of how it is used.[33]

The relatively new and technologically developing concept of mobile money has forever altered the ease and speed to which money is transformed and transported. Stemming from above, it is necessary to understand the associated terms that may have a bearing on the definition of "mobile money", in order the grasp the concept of mobile money payments.

### 2 Money as legal concept

One might be tempted to think that the term "money" is relatively easy to define. However, depending on the economic and legal context, and taking due cognisance of the universality of money, its various forms and numerous functions, and the multitude of monetary systems used to facilitate trade, the term "money" can have various definitions.[34] For most monetary theorists assigning a satisfactory definition to money is a vexing problem. For instance, economists use the functions of money to describe it as both a means of exchange and a measure of value in relation to contractual obligations.[35] Nussbaum[36] believed that money represented a dominant concept of law and a nexus exist between the economic and legal theories of money.

---

32 Grotius *De Jures Belli* ac Pric*,* ii12.17*.*

33 Carruthers and Espeland 1998 *American Behaviour Scientist* 1374.

34 Organisation for Economic Co-operative and Development (OECD) 2002 http://oecd.org/futures/35391062.pdf.

35 Frederic *The Economics of Money, Banking and Financial Markets* 8.

36 Nussbaum 1937 *Michigan Law Review* 875 and Nussbaum *Money in the Law: National and International* 19.

In practice, Mann[37] noted that lawyers readily accept that the economic theory of money has expanded. This matter was debated as early as 1827 in the case of *Spratt v Hobhouse* [38], and which resulted in the notion that everything that can readily be turned into money may be treated as money. A broader definition of the term "money" was attributed in the case of *Moss v Hancock* [39] (hereinafter the *Moss case*), where money was defined as:

> …that which passes freely from hand to hand throughout the community in final discharge of debts and full payment of commodities, being accepted equally without reference to the character or the credit of the person who offers it and without the intention of the person who receive it to consume it or apply it to any other use than in turn to tender it to other in distance of debts or payments for commodities.[40]

The criteria in *Moss case* for a physical thing ("all chattels"[41]) for money were also supported by Mann, which resulted in the adoption of the economic definition of money. It would appear that *Moss case* follows a quantitative, functional approach to money, which also denotes a requirement of a corporeal, tangible form of money to enable it to "…pass freely from hand to hand…".[42]

To find a statutory definition of money is rare. At a very basic level most authors[43] agree that, from an economic perspective, money has three functions, namely it is regarded as (a) a unit of account, (b) a medium of exchange and (c) a store of value.[44] Blackstone[45] believes that money can be defined as the universal medium of commerce which sets a standard by which the value of all commodities can be

---

37 Mann *The Legal Aspect of Money 5th ed* 23-24.

38 1827 4 Bing 179.

39 1899 2 QB 111 116.

40 Du Toit 2013 http://dspace.nwu.ac.za/bitstream/handle/10394/10197/Du_Toit_SF.pdf?sequence=1.

41 Mann *The Legal Aspect of Money: With Special Reference to comparative Private and Public International Law* 4th ed 8.

42 Mann *The Legal Aspect of Money: With Special Reference to comparative Private and Public International Law* 4th ed 8.

43 Law *Money and Trade Considered* 6-8; Scott 2013 http://research.stlouisfed.org/pageone-economics/uploads/newsletter/2013/PageOne0313_Money_Trade_Barter_Inflation.pdf and Aglietta 2002 http://goo.gl/RTOse.

44 Scott 2013 http://research.stlouisfed.org/pageone-economics/uploads/newsletter/2013/PageOne0313_Money_Trade_Barter_Inflation.pdf.

45 Blackstone 1765 – 1769 http://press-pubs.uchicago.edu/founders/documents/a1_8_5s1.html.

determined. In contrast, Ernst[46] argues that fiat money[47] cannot be regarded as a measure against which all things are valued. He believes that the price of all things provides the measure of the value of money. Mehrling[48], however, differentiates between "fiat" money, which is regarded as a nonconvertible, so-called "money-thing" issued by government, and "credit", which appears to mean the same as "fiat money", but which is only issued by private entities. This suggest a disaggregation at a legal and economic level of the traditional nexus to the Orthodox School approach. With this definition Mehrling, however, fails to recognise the sovereignty of the state because he conflates "money-things" with money.[49] According to Khanna,[50] money can be defined as legal tender (i.e. the coins and currency declared by government as the accepted medium of exchange) or anything that serves the functions of money and excludes all others.

Du Toit[51], however, believes that property law guides the way we think about money. He has noted that the courts and writers refer to account holders as the owner of money, even if there is now reference to money in a property law.[52] It is thus important to distinguish between the concepts of money and payment methods. Goode[53] maintains that any transfer of value, whether or not in cash, will constitute a payment. It is generally agued by lawyers that a payment represents the existence of money.[54] The court held in *Miller v Race* [55] that due to the attribute of money, also referred to as currency, the normal application of property law in claims by even *bona fide* recipients for tangible items, cannot be applied. Thus, money as a currency is an exemption to common law rules of property in that a seller cannot assign a better title than what was received. What is interesting to note when we

---

46 Von Hagen and Welker *Money as God? The Monetization of the Market and it Impact on Religion, Policy, Law and Ethics* 3-4.

47 The term "fiat money" is derived from the Latin word "fiat" and means "let it be done". It is described as a currency which value is only recognised through government legislation. Investopedia 2014 http://investopedia.com/terms/f/fiatmoney.asp.

48 Mehrling 2000 *Journal of Post Keynesian Economics* 402.

49 Wray 2010 http://e1.newcastle.edu.au/coffee/pubs/workshops/12_2001/carlson.pdf.

50 Khanna *Advanced Study in Mona and Banking: Theory and Policy Relevance in the Indian Economy* 16.

51 Du Toit 2009 *TSAR* 1-2.

52 Du Toit 2009 *TSAR* 1-2.

53 Goode and McKendrik *Goode on Commercial Law* 488.

54 Goode *Commercial Law* 2nd ed 491-492.

55 (1758) 1 Burr 452.

look at the idea of "money as a currency", legislators have, for the purpose of prevention and punishment of offences of counterfeiting, acceded to the provision contained in the *International Convention for the Suppression of Counterfeiting Currency* of 1929[56] (hereinafter the Convention), which resulted in the promulgation of the *Prevention of Counterfeiting of Currency Act* 16 of 1965 (hereinafter the *PCC Act*). Conversely to the *PCC Act*, article 2 of the Convention defined "currency" as paper money[57] and metallic money which is legally authorised. Notwithstanding the above, the *PCC Act* gives effect to the Convention and thus it can be argued that the definition would also be applicable to the *PCC Act*.

Money, as a fiat currency has no intrinsic value[58] because it is solely used as a means of payment and can only derive value through government decree.[59] In South Africa, the definition of the term "money" can be found in section 1 of the *National Payment Systems Act* 78 of 1998 (hereinafter the *NPS Act*), which defines it as a banknote or coin issued in terms of section 10(1)(a)(iii) read with section 14 of *The South African Reserve Bank Act* 90 of 1989 (hereinafter the *SARB Act*), by the South African Reserve Bank (hereinafter the SARB). In terms of section 9 of the *Currency and Exchanges Act* 9 of 1933 read with regulation 1 of the *Exchange Control Regulations* 1961, the term "money" also consist of foreign currency or bill of exchange or other negotiable instruments. The governance and the management of currency, as well as the right to issue banknotes and coins, fall within the sole power of the SARB.[60] In terms of sections 14 and 15 of the *SARB Act*, money is described as coins and notes as well as deposits in deposit-taking institutions such as banks.

---

56 Unknown 1929 International Convention for the Suppression of Counterfeiting Currency of 1929 http*://*paclii.org/pits/en/treaty_database/1929/3.rtf*.*

57 Section 1 of the *Prevention of Counterfeiting of Currency Act* 16 of 1965 defines bank notes to include paper money which is regarded as legal tender in the jurisdiction where it is issued, but exclude bank notes issued under s 14 of the *South African Reserve Bank Act* 90 of 1989.

58 "Intrinsic value" can be defined as the actual value of an asset (tangible or intangible) based on the believe that it has value, which might not be the same as the current market value due to the determination of supply and demand. WebFinance Inc., Investor Words 2015 http://investorwords.com/2587/intrinsic_value.html.

59 Mankiw *Macroeconomics* 81.

60 Section 14 of the *SARB Act* 90 of 1989.

Based on the assumption that some tangible thing can provide the basis for "money" to be regarded valuable to other, it can be argued that "money" in law follows both a common law and an Aristotelian-derived[61] Orthodox[62] economic theory. [63]

According to Kocherlakota,[64] a lack of commitment and recordkeeping will cause the use of money as a payment medium to become essential as it improves efficiently relative to an economy without money. However, in a decentralised economy the use of money can lead to resource misallocation. Characterised by the anonymity and decentralisation of trade, the use of money allows unrestricted access to receive and transfer money and goods without any restriction on who can use money or how money can be used.[65]

## 3 Legal tender

During the early Middle Ages, most countries' sovereigns protected their sole right to issue money within their jurisdiction and prohibited all others issuers from minting coinage.[66] To date, monetary sovereignty[67] has not changed much, except that worldwide states have delegated this function to central banks.[68]

In terms of section 10(1)(c) of the *SARB Act*, the SARB is required to perform such functions, implement such rules and procedures and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment,

---

61 Schumper *History of Economic Analysis* 62-63 and Meikle 1994 *A Journal for Ancient Philosophy* 27-33 - The commodity-based monetary theory proclaims that the value of money is based on its relationship with commodity.

62 Law *Money and Trade Considered* 6-8. The Orthodox School economist define money as anything which can be expressed as a standard unit to which store value (a price or debt can be measured) and is widely accepted in payment of goods. Geva and Kianieff 2005 http:// goo.gl/QfR4y – Although did not agree with Mann's inclusion of a tangible thing, for instance a chattle, in the definition of money, they agreed with the appropriation of an economic definition to money by law, however failed to analyse the what is meant by "tangible".

63 Mann *The Legal Aspect of Money: With Special Reference to comparative Private and Public International Law* 4th ed 8.

64 Kocherlakota 1998 *Journal of Economic Theory* 232-233.

65 Chiu and Wong 2014 http://bostonfed.org/payments2014/papers/Chiu_Wong.pdf.

66 Innes 1913 http://community-exchange.org/docs/what%20is%20money.htm.

67 Mann stated that monetary sovereignty consists of three exclusive rights namely, the right to issue currency (e.g. banknotes and coins as legal tender); the right to determine and change the value of that currency and the right to regulate the use of currency within a specific jurisdiction. Mann *The Legal Aspects of Money* 460-462.

68 Gianviti 2004 http://imf.org/external/np/leg/sem/2004/cdmfl/eng/gianvi.pdf.

clearing or settlement systems. Section 2 of the *NPS Act* 78 of 1998 reaffirms this authority entrusted to the SARB. Stemming from the above and in accordance with section 15(1) the *Currency and Exchanges Act* 9 of 1933 and section 14 of the *SARB Act*, the exclusive right to issue or cause to be issued banknotes and coins in the Republic of South Africa vests with the SARB.

Section 11 of *The Banks Act* 94 of 1990 (hereinafter the *Banks Act*), furthermore states that no person may conduct the "business of a bank" unless such a person is a public company and registered as a bank. Subject to certain exclusions, the "business of a bank" is defined to include the acceptance of deposits form the general public as a regular feature of the business in question and soliciting of or advising for deposits.[69] Thus, "deposit taking" becomes the key element of the concept of "business of a bank". Section 1 of the *Banks Act,* in general, describe a "deposit" as an amount of money paid by one person to another person subject to an agreement in terms of which an equal amount or any part thereof will be repaid on demand, on a specified or unspecified date or in circumstances agreed upon.[70] The taking of deposits, which also includes soliciting a deposit, from the general public by an unregistered person (non-bank) is regarded as a criminal offence in terms of section 91(8) of the *Banks Act*.

According to section 17 of the *SARB Act*, legal tender is defined as the banknotes or coins that are legally offered as payment of a debt and for which a creditor is required to accept. Legal tender of the payment of money can be described as a tender by the SARB of:

- a note of the SARB or of an outstanding note of another bank for which the SARB has assumed liability in terms of section 15(3)(c) of the *Currency and Banking Act* 31 of 1920 or in terms of any agreement entered into with another bank before or after commencement of the *SARB Act*; and

- an undefaced and unmitigated coin which is lawfully in circulation in the Republic of South Africa and of current mass.

---

69 Section 1 of the *Banks Act* 94 of 1990.

70 A more comprehensive definition is contained in terms of s 1 of the *Banks Act* 94 of 1990.

It follows therefore that it can be argued that money consist of mainly two financial elements namely, deposit-taking and payments. As a legal tender, it guarantees payment by the SARB to any holder of a sum of legitimate money (i.e. notes and coins).[71]

## 4 Unbanked and underbanked

"Money is the root of most progress."[72] According to Furguson[73], poverty is reflective of a lack of access to financial services and not inevitably a consequence of financial exploitation. Innovative financial services technologies, such as emerging m-banking technologies, have the potential to foster financial access and inclusion for the unbanked and underbanked. The key finding identified in McKinsey Quarterly report[74] indicated that half (2.5 billion) of the world's adults do not use formal banks or semiformal microfinance services to save or borrow money, of which 62% (2.2 billion) are situated in Africa, Asia, Middle East and Latin America. Refer to annexure 2.1. attached hereto which depicts the percentage of unbanked adults on a global scale.[75] The 2013 Federal Deposits Insurance Corporation's[76] national survey of unbanked and underbanked households highlighted the follow as reasons for individuals being unbanked: these individuals do not earn enough to justify having an account; high bank charges, distrust of the banking system, inconvenient business hours and difficulties with identification documents or bad credit records.

---

71 South African Reserve Bank National Payment System Department 2014 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf.

72 Ferguson *The Ascent of Money: A Financial History of the World* 2.

73 Ferguson *The Ascent of Money: A Financial History of the World* 12-13.

74 Chaia, Goland and Schiff 2010 http://mckinsey.com/insights/financial_services/counting_the_worlds_unbanked - The report represents a data set compiled from existing cross-country data sourced on financial access and socio-economic and demographic characteristics for the purpose of highlighting the size and nature of the global population not utilising formal/semiformal financial services.

75 Chaia, Goland and Schiff 2010 http://mckinseyonsociety.com/downloads/reports/Economic-Development/Half_the_world_is_unbanked.pdf

76 Federal Deposits Insurance Corporation 2014 https://www.fdic.gov/householdsurvey/2013report.pdf.

Gross *et al*[77] noted that unbanked and underbanked individuals are in most instances young, female, unmarried, unemployed, from the minority low-to-moderate income group, who is reluctant to partake in financial risk. Stemming from the above one can argue that most unbanked and underbanked individuals are more inclined to use an informal system (i.e. cash) and/or alternative financial service providers such as pawn lenders and *stockvel* services.

The term "unbanked" is used as a slang term and refers to those individuals who generally pays for thing in cash and do not use or have access to bank accounts/facilities.[78] An "underbanked" individual refers to individuals who has an account, but who also has availed of at least one alternative financial service in the past 12 months. A "fully banked" individual, however, is viewed as someone with a bank account but does not avail of any alternative financial services.[79] Furthermore, according to the Federal Reserve Board's 2012 survey of consumers and mobile financial services (SCMFS), unbanked households are most likely to resolute in the low income bracket (i.e. less than USD 25 000), whilst the underbanked households will have moderate incomes (i.e. approximately USD 25 000 to USD 39 999).[80] The Federal Reserve Bank's SCMFS advocate that m-banking technologies provide an enhanced integration mechanism for the unbanked and underbanked into the conventional financial system.[81]

From the above it should be noted that traditional banking channels cannot realize the needs of the unbanked and underbanked segment population and requires mobility and an innovative approach.

---

[77] Gross *et al* 2012 http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf.

[78] Investopedia 2015 http://investopedia.com/terms/u/unbanked.asp.

[79] Gross *et al* 2012 http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf.

[80] Gross *et al* 2012 http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf.

[81] Gross *et al* 2012 http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf.

## 5 Electronic-banking and mobile-banking

Due to the need to trade independently from where clients are located, client mobility has become ingrained in modern financial markets.[82] Most financial institutions have recognised this opportunity to significantly change their client target market through the implementation of new payment systems,[83] such as electronic and m-banking. While the introduction of e-banking enabled individuals to transact at any time, m-banking offers individuals even greater flexibility to transact anywhere.[84]

E-banking can be defined as the "provision of retail and smaller value banking products and services through electronic channels".[85] The difference between e-banking and m-banking is that e-banking is regarded as the overarching system of which m-banking is a subdivision thereof.[86]

Triggered by technological development, m-banking has become more prevalent than any other financial market instrument.[87] M-banking as a transformative model of mobile financial service[88] consists of m-banking and mobile transactions.[89] This model is aimed at the unbanked population[90] and largely low-income individuals. M-banking can be defined as financial services that are received via the use of a mobile network and accessed on a mobile phone.[91] For the purpose of prudential supervision and oversight, m-banking activities are regarded as falling within the ambit of banking

---

82 Webb 2010 *Journal of Banking Regulations* 129.

83 Section 1 of the *NPS Act* 78 of 1998 defines 'payment systems' as a system that facilitates the transfer of money or permits payment to be effected and includes any instrument and procedures linked to the system.

84 Tiwari and Buse *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector* 26.

85 Basel Committee on Banking Supervision 1998 http://bis.org/publ/bcbx35.pdf .

86 Chatain *et al Protecting Mobile Money against Financial Crime* 1.

87 Consultative Group to Assist the Poor (CGAP) 2008 http://cgap.org/sites/default/files/CGAP-Focus-Note-Regulating-Transformational-Branchless-Banking-Mobile-Phones-and-Other-Technology-to-Increase-Access-to-Finance-Jan-2008.pdf .

88 Mobile financial services refers to finance-related services which are provided by using mobile telecommunications technology - Tiwari and Buse *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector* 69.

89 Webb 2010 *Journal of Banking Regulations* 129.

90 The term "unbanked population" is used as a slang term and refers to those individuals who generally pays for thing in cash and do not use or have access to bank accounts or banking facilities - Investopedia 2015 Definition of Unbanked http://investopedia.com/terms/u/unbanked.asp.

91 Lawack 2013 *Washington Journal of Law, Technology and Arts* 319.

business activities.[92] This view is also supported in the SARB's 2009 position paper[93] which states "only South African registered banks may issue mobile money". M-banking also refers to the financial services that are available to individuals through the use of mobile phones, and includes both transfers and payments.[94] M-banking has the ability to transform traditional retail banking from a physical and face-to-face transaction to a branchless and non-face-to-face activity.[95] It has the means and potential to reach the very large population of unbanked individuals in developing countries where there are significantly more mobile phones than branches available.[96]

## 6 Electronic money and digital money

The evolution of new payments systems such as digital money, electronic money (hereinafter e-money) and mobile money has significantly altered the performance of payment instruments in terms of convenience, transactional speed and anonymity.[97] These new forms of money emerge in the monetary hierarchies in an attempt to overcome the said challenges pertaining to access, transactional speed and anonymity.[98]

E-money or currency is defined as an electronic record that stores money.[99] This description also includes digital currency, computer money and e-cash, which are found in two basic forms, namely smart cards and network money.[100] In contrast, the

---

92 Webb 2010 *Journal of Banking Regulations* 129.

93 South African Reserve Bank National Payment System Department 2009 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf.

94 Bångers and Söderberg 2008 http://spidercenter.org/polopoly_fs/1.163645.1390316332!/menu/standard/file/Spider%20ICT4D%20Series%202%20Mobile%20banking%20-%20financial%20services%20for%20the%20unbanked.pdf.

95 Greenacre 2014 http://clmr.unsw.ed.au/article/risk/material-risk/fure-mobile-banking-part-one.

96 Villasenor 2013 http://brookings.edu/research/papers/2013/09/16-smartphones-mobile-money-developing-countries-villasenor .

97 Chiu and Wong 2014 http://bostonfed.org/payments2014/papers/Chiu_Wong.pdf .

98 Organisation for Economic Co-operative and Development 2002 http://oecd.org/futures/35391062.pdf .

99 Ely 1996 http://cato.org/moneyconf/14mc-2.html .

100 Benjamin *The Future of Global Currency: The Euro versus the Dollar* 31.

Electronic Money Directive[101] considered e-money to be an electronic representation of fiat currency (e.g. banknotes and coins). Like many other forms of fiat currency[102] (e.g. credit and debit cards) e-money is regarded as one of the mechanisms through which value denominated in fiat currency can be transferred while retaining legal tender status.[103]

The European Payment Council (hereinafter the EPC) recognised that the diverse definitions of "e-money" have a substantial regulatory impact. On 16 September 2009 the EPC attempted to resolve this issue by formulating a uniformed definition. In terms of section 2(2) of the *Directive 2009/110/EC,* e-money can be defined as:

> Monetary value represented by a claim on the issuer which is stored in an electronic device and accepted as a means of payment by undertaking other than the issuer.[104]

This view is shared in the SARB's above-mentioned 2009 position paper, in that the SARB[105] defined e-money as "electronically stored monetary value issued on receipt of funds and represented by a claim on the issuer". Therefore e-money can only be issued on receipt of funds that are not lower in value than the monetary value issued and it must be prepaid.[106] E-money is not viewed as a separate currency and is regulated by the central bank.[107] It is accepted as a payment instrument by persons other than the issuer and can be exchanged for physical cash or a deposit into a bank account on demand thereof.[108] The position paper confirmed that only

---

101 The European Commission 2006 http://ec.europa.eu/internal_market/bank/docs/e-money/evaluation_en.pdf.

102 Financial Action Task Force Report 2014 http://fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf - Fiat currency is also known as real currency or real money or national currency and refers to banknotes and coins of a country which is accepted and issued as legal tender.

103 Financial Action Task Force Report 2014 http://fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

104 The Bank of International Settlements 2009 http://http://legislation.gov.uk/uksi/2011/99/schedule/4/part/2/made.

105 South African Reserve Bank National Payment System Department 2009 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf.

106 Webb 2010 *Journal of Banking Regulations* 135.

107 Central Bank of Ireland 2013 http://centralbank.ie/regulation/industry-secrors/electronic .

108 South African Reserve Bank National Payment System Department 2014 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Docume

authorised registered South African banks are allowed to issue e-money as defined in the *Banks Act.*[109]

The basic properties that e-money shares with "real" or physical money are that both are durable, transportable, divisible, allow for anonymity and cannot be easily counterfeited. Although an e-money-based payment system requires the payers and payees to obtain specific payment devices (e.g. cards, electronic devices or software downloads) from the e-money issuer before transacting, it allows for greater access, transactional speed and anonymity compared to a money-based payment system.[110] Chatain believes that e-money products can be subdivided into mobile money, electronic wallets and network money.[111]

Ali[112] *et al* believe that digital currency is archetypal of both a leading-edged payment system and possible inventive currency. The economist theory requires that for digital currency to be considered as a new form of currency, it will have to be capable of storing value, regarded as a medium of exchange and function as a unit of account.[113] In contrast to e-money, digital currency refers to a digital representation of either money (fiat money) or virtual currency[114] (non-fiat). It does not represent a claim on anybody and some authors believe it is a type of commodity.[115] The proliferation in digital currencies has caused it to be used interchangeably with the term "virtual currency".[116] Virtual currency is regarded as an unregulated, digital money, which is

---

nts/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf.

109 South African Reserve Bank National Payment System Department 2009 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf.

110 Chiu and Wong 2014 http://bostonfed.org/payments2014/papers/Chiu_Wong.pdf.

111 Chatain *et al Protecting Mobile Money against Financial Crime* 1.

112 Ali *et al* 2014 http://bankofengland.co.uk/publications/Documents/quaterlybulitin/2014/qp14q301.pdf

113 Ali *et al* 2014 http://bankofengland.co.uk/publications/Documents/quaterlybulitin/2014/qp14q301.pdf

114 "Virtual currency" is defined, in the Financial Action Task Force Report on Virtual Currencies: Key Definitions and Potential AML/CFT Risks, as a math-based, decentralised, digital representation of value that can be digitally traded and functions as a medium of exchange and/or unit of account and/or a store of value, but does not enjoy any legal tender status. 4.

115 Ali *et al* 2014 http://bankofengland.co.uk/publications/Documents/quaterlybulitin/2014/qp14q301.pdf

116 Financial Action Task Force 2014 http://fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf and the SARB's Position Paper on Virtual Currency defines virtual currency as a decentralised digital representation of value

issued and controlled by its developer and accepted amongst member of the virtual community.[117] It operates as a currency in certain environments, but does not have the attributes of real currency.[118] Designed to be decentralised[119] and has no legal tender status in South Africa.[120] This is viewed as a form of peer-to-peer transfer, where electronic value is transferred from one person to another, without any intervention by financial institutions.[121]

Stemming from above and for the purpose of this paper, digital currency such as virtual currency does not form part of the scope discussions liked to mobile money or mobile money transactions.

## 7 What is mobile money?

The evolution of mobile phone data communication capability has prompted banks to partner with communication companies to leverage on the existing communications infrastructure in a bit to launch mobile financial services[122] such as mobile payments for the unbanked.[123] The use of mobile phones has far outnumbered bank accounts.[124] This growth has lead to a multifaceted "mobile

---

that can be digitally traded and functions as a medium of exchange, a unit of account and/or a store of value, but is not regarded as legal tender. http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf.

117 Parker 2014 http://cgap.org/publications/bitcoin-vs-electronic-money.

118 FinCen 2013 https://fincen.gov/news_room/testimony/html/20131119.html.

119 "Decentralised" means that there is no central entity in charge of issuing the currency and processing transactions – South African Reserve Bank: National Payment Systems 2014 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem%28NPS%29/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf.

120 South African Reserve Bank: National Payment Systems 2014 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem%28NPS%29/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf.

121 Nakamoto 2008 http://cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf.

122 Webb 2010 *Journal of Banking Regulations* 131 – Mobile service providers are generally referred to as financial services providers, acting as intermediaries between buyers and sellers aimed at facilitating a transaction via the use of a mobile phone.

123 Lawack 2013 *Washington Journal of Law, Technology and Arts* 317 – 318 - Unbanked refers to the population sector which does not have any bank accounts and payments are effected though informal means.

124 Villasenor 2013 http://brookings.edu/research/papers/2013/09/16-smartphones-mobile-money-developing-countries-villasenor .

money" ecosystem where billions of dollars are transferred amongst mobile phone users every month.[125]

Mobile money (hereinafter m-money) is a form of e-money, where the actual value of the transaction and personal account data are stored on the mobile phone, which is in turn used to effect financial transactions.[126] According to Winn[127] m-money refers to "the use of mobile phones to deposit, withdraw or transfer funds". In addition, Chatain *et al.* [128] define m-money as a type of financial service that enables clients to send and receive funds through the use of a mobile phone. Thus m-money can be used for both money transfers and payments.[129] In the SARB's aforementioned 2009 position paper[130], m-money is defined as:

> Monetary value represented by a claim on the issuer. The 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.

In essence mobile phones are used to provide a platform for offering and accessing financial services. The prerequisite for its successful implementation necessitates a network of "agents" and its ability to convert data to cash.[131] Stemming from the above, m-money offers a means to provide financial access for a very large population of unbanked individuals[132] who do not have access to traditional branch banking.[133]

---

125 Global Mobile Money Adoption (GMSA) 2012 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/03/MMU_Results-from-the-2012-Global-Mobile-Money-Adoption-Survey.pdf.

126 Popa 2012 *Metalurgia International* 219 –220.

127 Winn and de Koker 2013 *Washington Journal of Law, Technology and Arts* 156.

128 Chatain *et al Protecting Mobile Money against Financial Crime* xxix.

129 Lawack 2013 *Washington Journal of Law, Technology and Arts* 319.

130 The South African Reserve Bank National Payment System Department 2009 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf .

131 Kumar and Dutta 2015 *Economic and Political Weekly* 40.

132 Buckley *et al* 2014 http://clmr.unsw.edu.au/taxonomy/term/77. According to Burkley *et al* the World Bank Predicted that mobile money could by the year 2020 impact the lives of 2 billion people in developing countries.

133 Buckley *et al* 2014 http://clmr.usw.edu.au/taxonomy/team/77.

## 8 Branchless banking

The concept of branchless banking is not new,[134] although it bears little resemblance to what it looked liked 10 years ago.[135] Currently, any mobile phone and any store can, with the correct technology platform, potentially become a client interface, providing access to funds.[136] The rapid expansion of innovative payment technologies such as m-banking to large numbers of unbanked individuals has rekindled new interest in branchless banking model.[137]

Branchless banking can be defined as providing financial services outside the ambit of traditional bank branches through the implementation of information and communication technologies and use of non-bank retail agents.[138] It is a strategy of distribution channel which aim to expand the concept of a traditional bank branch. The implementation of branchless banking through the use of m-money will not only speak to the issue of financial exclusion but also provides an affordable and accessible medium to the poor.[139] The term "branchless banking" can be misleading. It implies that bank branches will become absolute and irrelevant. Stemming from this Alexander[140] *et al* rather advocate the use of the term "banking beyond bank branches" as it is believed that banking in the future will remain rooted in local branches with specialised banking channels.

Branchless banking consists of two basic models namely, a bank-base model and a non-bank base model which can also function in combination.[141] A bank-base model

---

134 Basel Committee on Banking Supervision has since 1998 issued guidance on electronic banking, see http://bis.org/publ/bcbs35.pdf.

135 Pikens, Poreous and Rotman October 2009 http://cgap.org/sites/default/files/CGAP-Focus-Note-Scenarios-for-Branchless-Banking-in-2020-Oct-2009.pdf.

136 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

137 Dias and McKee 2010 http://cgap.org/publications/protecting-branchless-banking-consumers.

138 Pikens, Poreous and Rotman October 2009 http://cgap.org/sites/default/files/CGAP-Focus-Note-Scenarios-for-Branchless-Banking-in-2020-Oct-2009.pdf.

139 Alexandre 2001 http:/microcreditsummit.org/uploads/resource/document/alexandrec_branchless_banking_52485.pdf.

140 Alexander, Mas and Radcliffe August 2010 http://financialaccess.org/sites/default/files/publications/regulating-new-banking-models-that-can-bring-financial-services-to-all_0.pdf.

141 Pikens, Poreous and Rotman October 2009 http://cgap.org/sites/default/files/CGAP-Focus-Note-Scenarios-for-Branchless-Banking-in-2020-Oct-2009.pdf.

refers to a direct client contractual relationship with a prudentially licensed and supervised financial institution. In contrast, a nonbank-based model refers to a client relationship with no contractual relationship with a fully prudentially licensed and supervised financial institution.[142] In this relationship cash is exchanged at a retail agent for an electronic record of value which is stored on a server such as a mobile network operator's server.[143] This is also referred to as a closed loop system, limited to a specific vendor.[144] It should be noted that non-banks[145] are not subject to the same level of prudential regulation which applies to banks, for the purpose of protecting client funds from illicit activities such as ML and TF. Section 4(2)(d)(i) of the *NPS Act*, however, requires that non-banks, such as m-banking retailers, must be sponsored by banks to enable the clearance and settlement transactions.[146] The main risk of branchless banking, from a regulatory and supervisory point of view, can be derived from extensive use of outsourcing to agents[147] coupled with ineffective regulatory oversight.[148]

## 9 Financial abuse and financial crime

The terms financial abuse and financial crime are often used interchangeably. According to the International Monetary Fund[149], financial abuse does not only encompass illegal activities but also include poor supervisory and regulatory

142 Pikens, Poreous and Rotman October 2009 http://cgap.org/sites/default/files/CGAP-Focus-Note-Scenarios-for-Branchless-Banking-in-2020-Oct-2009.pdf.

143 Pikens, oreous and Rotman October 2009 http://cgap.org/sites/default/files/CGAP-Focus-Note-Scenarios-for-Branchless-Banking-in-2020-Oct-2009.pdf.

144 Guardian Data Systems 2014 http://guardiandatasystems.com/open-vs-closed-loop-payment-processing/.

145 The term non-bank can be defined as the non-prudentially regulated institution – Chriten, Lyman and Rosenberg 2003 http://info.worldbank.org/etools/docs/library/83619/cgap_paper.pdf.

146 Lawack *Washington Journal of Law, Technology and Arts* 327.

147 Dias and McKee 2010 https://cgap.org/sites/default/files/CGAP-Focus-Note-Protecting-Branchless-Banking-Consumers-Policy-Objectives-and-Regulatory-Options-Sep-2010.pdf.

148 Dias and McKee 2010 http://cgap.org/publications/protecting-branchless-banking-consumers.

149 Plays a role in protecting the integrity of the international financial system form abuse, by promoting the implementation of sound financial systems and good governance – Assessing the Implementation of Standards: A review of Experience (SM/01/11, January 2001).

frameworks, which have the potential to harm financial systems.[150] See attached hereto as annexure 2.2. which illustrate the concept of financial abuse.

There is no internationally accepted definition of financial crime. In this regard, financial crime, refer to any non-violent crime which results in financial loss (i.e. financial fraud, ML etc.).[151] Financial crime can be purported by financial institution in three ways[152], namely as a victim (i.e. subject to e.g. misrepresentation), a perpetrator (i.e. commit different types of fraud on others) or an instrument (i.e. to keep or transfer funds).[153]

## 10 Money laundering

It is clear from the aftermath of 9-11 that, the financial services sectors are not immune to ML and the TF activities. Predicate offences[154] such as drug smuggling, fraud etc. are crimes that underpin ML and TF activities. Interpol defines "money laundering" as:

> …any act or attempt to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legal sources.[155]

In essence, it describes the process of changing "dirty" money into "clean" money.[156] Generally, ML activities involve a series of multiple transactions used to mask the source of the financial assets so those assets may be used without compromising the

---

150 International Monetary Fund 2001 https://imf.org/external/np/ml/2001/eng/021201.pdf.

151 International Monetary Fund 2001 https:// imf.org/external/np/ml/2001/eng/021201.pdf.

152 International Monetary Fund 2001 https://imf.org/external/np/ml/2001/eng/021201.pdf.

153 During June 2013 the Lebanese Canadian Bank agreed to pay USD 102 million settlement of civil forfeiture for the role it played in the money laundering and terrorist financing network which resulted in approximately USD 329-million being transferred – Raymond 2013 http://reuters.com/article/2013/06/25/us-lebanesebank-settlement-idUSBRE95O17P20130625.

154 United Nations Office on Drugs and Crime 2008 https://unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf, 119 and Financial Action Task Force Recommendation 3 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

155 Interpol 2015 http://interpol.int/Crime-areas/Financial-crime/Money-laundering.

156 Saksenber, Spitz and Meyer *FICA Training Manual* 36-38 described the general steps which criminals will follow to launder money to consist of: (1) placement (introduction of illegal activities into the financial system), (2) layering (the separation of the proceeds through layering of complex transactions to make it untraceable) and (3) integration (effecting additional transactions to create the illusion of legality into the financial system).

criminals who are seeking to use them.[157] In terms of the section 1 of *FICA*, "money laundering" or "money laundering activity" can be defined as an activity which is aimed at obscuring or masking the nature, origin, location, character or movement of the proceeds derived from illegal activities and any interest which any person has in such proceeds, as well as any activities which signify a transgression of section 64 of *FICA* or sections 4, 5, or 6 of *the Prevention of Organised Crime Act* 121 of 1998 (hereinafter the *POCA*).

The *Prevention and Combating of Corrupt Activities Act* 12 of 2004, specifically prohibits any act of bribery and corruption and furthermore imposes very strict reporting obligations of persons of authority.[158] In terms of sections 4, 5 and 6 of the *POCA*, single specific offences are identified, which involves that a person shall be alleged to being guilty of an offence if he or she "knows or ought reasonably to have known" that the proceeds are linked to an unauthorised activity,[159] which, *inter alia*, result in the making of any type of arrangement in connection with the money or property (i.e. conceal the nature, source, location and/or get rid of it and/or assist somebody to avoid prosecution); or a person entering into any agreement whereby the retention or control of the proceeds is facilitated or are used. The test for "ought reasonably to have known" is based on the person's general knowledge, skill, educations, experience and understanding, having regard to the situation.

Money launderers facilitate and expose the financial services sectors to the crime of ML with the objective to gain access to the use of different banking products,[160] which is then employed to disguise the origin and nature of their illicit funds.[161] ML and TF within the financial sector raise significant issue regarding the prevention, detection,

---

157 Popa 2012 *Metalurgia International* 219 -220.

158 Chapter 2 of *Preventions and Combating of Corrupt Activities Act* 12 of 2004.

159 Section 1(xv) of the POCA describes "proceeds of unlawful activities" as any "property or part thereof or any service, advantage, benefit or rewards which was derived, received or retained directly or indirectly, in connection with or as a result of any unlawful activity carries on by any person, whether in the Republic or elsewhere…"

160 Examples of bank products: Mortgage bonds, loans, hedge funds, mobile money and savings accounts.

161 PwC 2014 http://pwc.co.za/en_ZA/za/assets/pdf/global-economic-crime-survey-2014.pdf.

monitoring and prosecution.[162] As such it is believed that these abusive activities can be more effectively managed through the understanding of what potential ML risks are associated with clients, transactions and the implementation of new payments systems.

It can be argued that without proper and effective monitory, the implementation of new payment systems such as m-money transactions can become an ideal funnel for money laundering activities.

## 11 Terrorist financing

The term "terrorism" was the first time used to describe the Jacbin "Reign of Terror" which followed the French Revolution in 1789.[163] It is instantly evocative and emotive and is mostly associated with inducing extreme fear, intense terrorisation superimposed with centuries of political connotations.[164] Terrorism seriously threatens and demolishes basic human rights and freedoms, particularly life, liberty and security including economic, social and cultural rights. Although "terrorism" remains a political term, describing various acts and methods of political brutality, the United Nations (hereinafter the UN) advocates that a cumulative definition[165] for the word "terrorist" is applicable to international criminal law.

The 9-11 terror attack[166] and the recent wave[167] of international terrorist attacks have lead to an increased focus on ML, the TF and its regulation. FATF viewed TF as a

---

162 The International Bank for Reconstruction and Development, The World Bank and The International Monetary Fund *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* I1-I2.

163 Golder and Williams 2004 https://corrigan.austlii.edu.agu.

164 Saul 2008 https://ssrn.com.

165 United Nations Security Council resolution 1516 (2003) and 1530 (2004). Since 2003 the United Nations Council has condoned "any act", "all acts" and "all forms" of terrorism.

166 *United States of America Act* 2001 http://uspatriotact.org - commonly known as the "The Patriot Act" 2001 was proclaimed following the attacks on the twin towers of the World Trade Centre in New York in September 2001. This provided the US government with the appropriate tools required to intercept and obstruct terrorist acts.

167 Gardner Paris 2014 http://bbc.com/news/world-europe-30789123 and Howden 2014 http://theguardian.com/world/interactive/2013/oct/04/westgate-mall-attacks-kenya-terror.

global problem which requires a concentrated global solution.[168] The World Bank defines "terrorist financing" as:

> …the financial support, in any form, of terrorism or of those who encourage, plan or engage in terrorism.[169]

The very broad South African definition of "terrorist activity" can be found in section 1(xxv)(a) of *The Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004 (hereinafter the *POCDATARA*). The main functions of the *POCDATARA* is to provide a detailed description of terrorist-related offences[170], give extra investigative and arrest power to the South African Police Service and authorise the attachment of financing of terrorist organisation.[171] According to section 2 of the *POCDATARA* if a person knowingly engages in an act or ought to have reasonably known or suspected that the act will result in supporting a terrorist activity[172], that person will be found guilty of the offence of terrorism.[173] The objective of the *POCDATARA* is to align South Africa's anti-terrorism law with international standard and to ensure compliance with the United Nations 1999 International Convention for Suppression of the Financing of Terrorism.

Similar to the objectives and techniques applied by money launders, terrorist also apply different techniques to evade detection. However, the main objective for TF is to protect the identities of their sponsors and/or ultimate beneficiaries. Another key defining element that differentiates the TF activities from ML activities is that the

---

168 Financial Action Task Force 2013 http://fatf-gafi.org/documents/news/fatf-action-on-terrorist-finance.html.

169 The International Bank for Reconstruction and Development, The World Bank and The International Monetary Fund *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* I1 –I6.

170 Section 1 of the *Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004.

171 Golder and Williams 2004 https://corrigan.austlii.edu.agu.

172 Section 25 of the *Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004 requires the President of South Africa to issue a notification of any specific entity and individual who had been listed by the Security Council of the United Nations as having been identified of attempting to commit and/or having committed any terrorist related activity.

173 Sections 2 and 3 of the *Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004.

source of the funds does not require an illicit element.[174] The funds acquired for the TF can be sourced from legitimate activities such as donations and profit from businesses.[175] Terrorists would use formal banking systems and informal value-transfer systems such as Hawalas to transfer funds to beneficiaries. It has been noted that the transactions linked to terrorist activities tends to be small,[176] which makes the use of new payment systems such as m-money transactions an ideal instrument for evading detections and concealing the identities of beneficiaries. For instance, the ISIS terrorist organisation has highlighted the emergence of a new funding stream, which requires FATF and the UN Security Council Resolution 2199 to review of TF methods.[177]

## 12 Concluding remark

The transformation from money to electronic value has forever altered the fuel that powers the engine of economics and society development. New payment systems have managed to adapt and transform to the needs of societies to participate in a modern economy without the limitations associated with traditional banking.

Only thought the understanding of the fundamental terms associated with the concept of m-money transactions, it becomes clear why m-banking activities are regarded to fall within the prudential supervision, including the oversight of banking business activities.[178]

While m-money transactions has reduced the inherent risks of a cash-based system, the elusiveness, anonymity, low-risk rating, high marketability, global access to bank networks and poor supervision are all vulnerabilities that money launderers will use to

---

174 The International Bank for Reconstruction and Development, The World Bank and The International Monetary Fund *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* I6.

175 Financial Transaction and Report Analysis Centre of Canada http://fintrac-canafe.gc.ca/fintrac-canafe/definitions/terrorist-terroriste-eng.asp.

176 Financial Transaction and Report Analysis Centre of Canada http://fintrac-canafe.gc.ca/fintrac-canafe/definitions/terrorist-terroriste-eng.asp.

177 Financial Action Task Force 2013 http://fatf-gafi.org/documents/news/fatf-action-on-terrorist-finance.html.

178 Webb 2010 *Journal of Banking Regulations* 129.

their advantage.[179] The application of effective and financially inclusive anti-money-laundering and countering the finance of terrorism measures are vital in protecting the safety and soundness of banks, and the integrity of international financial systems.[180]

[179] Solin and Zerzan 2010 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/amlfinal35.pdf.

[180] Basel Committee on Banking Supervision 2014 http://bis.org/press/p140115.htm.

# CHAPTER 3

# MOBILE MONEY, FINANCIAL INCLUSION AND FINANCIAL CRIME

*We need banking but we don't need banks anymore.*[181]

## 1 Mobile money

The mobile and digital revolution has both transformed and redefined access to banks for the economically deprived.[182] It is not a question of expensive banking costs, but rather the fact that banks are simply inaccessible to many poor communities.[183] Accordingly, banks do not find it economically viable to even establish banking infrastructure such as automated teller machines (hereinafter ATMs) in an economically disadvantaged community, thus often depriving individuals of basic banking services.[184] Klein[185] is, however, of the opinion that the fundamental pillars to sustainable development rest upon expanding access to financial services. Fundamentally, this business model requires change and mobile innovations, such as m-money, to have the ability to fuel economic growth and yield major social benefits by improving education and financial inclusion for the poor; however, at the same time such innovations are open to ML and TF abuse.[186]

This chapter seeks to highlight the growth and financial inclusion potential of m-money, while at the same time investigating whether this presumably low-risk product is susceptible to ML and TF risks. To the best of my knowledge, most experts[187] believe that due to very low transaction threshold limit of R5 000 per day, but not exceeding R25 000 per month,[188] mobile payments should be regarded as low risk. Although this may encourage access to banking services, most studies on m-

---

181 Gates 2015 http://social.yourstory.com/2015/01/quotes-bill-gates-mobile-banking.

182 Demombynes and Thegeya 2012 http://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5988.

183 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

184 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

185 Klein in Chatain *et al* 2008 http://.siteresources.worldbank.org/INTAML/Resources/WP146_web.pdg.

186 GSM Association 2015 http://gsmamobileeconomy.com/.

187 De Koker 2009 *Journal of Money Laundering Control* 323-339; Luo, Zhang and Shim 2010 http://unm.edu/~xinluo/papers/DSS2010_MB.pdf; Alexandre and Eisenhart 2013 *Washington Journal of Law, Technology and Art* 258.

188 Section 21 read with exemption 17 of *FICA* 38 of 2001.

banking have been theoretical and qualitative in nature,[189] with the result being that nobody is looking at the real risks and potential abuse of m-money products for ML and TF purposes.

## 2 Mobile money potential

It is estimated by the World Bank that global remittances[190] exceed one quarter of a trillion dollars annually.[191] The 2015 *Groupe Speciale* Mobile Association (hereinafter GSMA) Mobile Economy report noted that a larger portion of the population has access to mobile services than to basic electrical, sanitation and financial services.[192] By 2020 smartphone usage globally would have more than doubled, reaching 6.1 billion,[193] of which mobile payments will be the most prevalent form of banking within Africa, Asia and Latin America.[194] This means that an anticipated 70% of the world population will be using smartphones by the year 2020.[195] In the past six years the use of m-banking systems has been predominantly strong in the Philippines (SMART Padala had by 2006 a monthly average of 1.5 million users remitting USD 15 million);[196] Kenya (two million users registered with Safaricom M-PESA system within a year of its nationwide rollout)[197] and South Africa (where 450,000 people use Wizzit).[198] Mobile phones are no longer a symbol of luxury but of necessity in Africa.[199]

---

189 Jonathan and Camilo 2008 *Asian Journal of Communication* 318-322; Merritt *Mobile Money Transfer Services: The next phase in Evolution in Person-to-Person payments*, Federal Reserve Bank of Atlanta, Retail Payments Risk Forum White Paper http://frbatlanta.org/-/media/documents/rprf/rprf.../wp0810.pdf and Thacker and Wright 2012 http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/bn_116_building_business_models_for_mobile_money.pdf .

190 "Global remittances" can be defined as the non-reciprocal transfer of cash through a payment system, from one person to another, usually across boarder (generally over a long distance) in relatively low value – The World Bank 2013 http://worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank.

191 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

192 GSMA 2015 http://gsmamobileeconomy.com/.

193 Ericsson 2015 http://ericsson.com/ericsson-mobility-report.

194 The Statistics Portal 2015 http://.statista.com/statistics/234659/number-of-mobile-payment-users-in-africa/ .

195 Ericsson 2015 http://ericsson.com/ericsson-mobility-report.

196 GSMA 2006 http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/Philippines-Case-Study-v-X21-21.pdf .

197 Vaughan 2007 in Coyle (Ed.) *The transformational potential of m-transactions* 6-9.

198 Ivatury and Pickens 2006 https://cgap.org/sites/default/files/CGAP-Mobile-Phone-Banking-and-Low-Income-Clients-Evidence-from-South-Africa-Jan-2006.pdf - Consultative group to assist the poor (CGAP) and the United Nations Foundation.

With this surge in connectivity banks can unlock the potential for mass-scale transformation. It is thus not surprising that m-money is increasingly adapting to provide access to even migrant workers who wish to transfer funds to their families abroad.[200] Such account holders can pay bills, receive funds, check balances and even receive their salaries by phone. M-money services offer a "virtual ATM" to every holder of a mobile phone.[201] Jenkins[202] believes that the success of m-money is based on three fundamental pillars, namely utility (use of m-money by clients), capacity (ability of a provider to make available an effective and comprehensive service) and enabling setting (client trust and the establishment of an appropriate regulatory framework).[203]

## 3 Electronic money vs paper money

In recent years the m-banking[204] and m-money[205] market has faced unprecedented growth as one of the emerging technological innovations in the banking sector.[206] Such technological innovations have caused these mobile products to become an extension of peoples' lifestyles and have created access to banking services for the unbanked. It can be a powerful instrument to reduce reliance on cash, which is regarded as a major ML/TF risk.[207]

M-money and mobile currency are both highly representative of modernity as these products provide the user with a sense of being fashionable, trendy, important and

---

199 Aker and Mbiti 2010 *Journal of Economic Perspectives* 208 and The Economists 2008 http://economist.com/node/11465558?story_id=11465558.

200 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

201 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

202 Jenkins 2008 http://hks.harvard.edu/m-rcbg/CSRI/publications/report_30_MOBILEMONEY.pdf.

203 Kumar and Dutta 2015 *Economic and Political Weekly* 41.

204 Mobile banking refers to the financial services that are received via the use of a mobile network and accessed on a mobile phone - Lawack 2013 *Washington Journal of Law, Technology and Arts* 319.

205 "Mobile money payments" refers to provision of a payment service through the use of a mobile phone, where money is stored electronically and issued on receipt of funds. These electronic funds is generally accepted as a means of payment between the client's own account and the beneficiary, for physical cash or a deposit into a bank account on demand. - The South African Reserve Bank National Payment System Department 2009 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf .

206 Lawack 2013 *Washington Journal of Law, Technology and Arts* 318.

207 Chatain *et al Protecting Mobile Money against Financial Crime* xxx.

connected to the modern world.[208] The reality of the modern world is that the majority of the economically deprived individuals residing in Africa and Asia mostly, if not exclusively, depend on cash-based storage, transactions and savings instruments.[209] Even in a developing economy such as South Africa a large segment of the population does not have bank accounts or access to banks,[210] thus allowing banking to take place through informal means.[211]

Although the holding physical cash provides a sense of assurance to some, it is not without risks. The lack of physical evidence linking currency to a chain of owners or the ability to provide an audit trail of transactions becomes problematic when trying to reconstruct transactions illicitly performed.[212] As such cash is characterised by anonymity and subject to wear-and-tear and degradation. The universality of cash is based on the fact that it is government issued[213] and thus requires the construction of infrastructure to operate and be regulated, which ultimately adds to the transaction costs.

M-money transactions represent the transfer of value via a mobile phone[214] and compared to cash, are traceable and can lend itself to account monitoring and restrictions.[215] According to Goode[216] any transfer of value, whether or not sounding in money, will constitute a payment and lawyers generally argue that a payment represents the existence of money.[217] Relying on the mobile operating networks and an existing system of retail outlets, m-money does not involve the construction of costly infrastructures to operate.[218] By leveraging existing communications infrastructure, which connects billions of clients worldwide, m-money facilitates the transfer of money. The development of personal, faster, simplified and secure transactional banking products, such as m-money, has significantly changed the way

208 Maurer 2012 *Banking and Finance Law Review* 308.
209 Kumar and Dutta 2015 *Economic and Political Weekly* 41
210 Fouriesburg a small town located in the Free State Province do not have any banks in the town.
211 Lawack 2013 *Washington Journal of Law, Technology and Arts* 318.
212 Maurer 2012 *Banking and Finance Law Review* 303-304.
213 Phillips 2014 *Western New England Law Review* 221.
214 Popa 2012 *Metalurgia International* 219 –220.
215 Chatain *et al Protecting Mobile Money against Financial Crime* xxx.
216 Goode and McKendrik *Goode on Commercial Law* 488.
217 Goode *Commercial Law* 2nd ed 491-492.
218 Maurer 2012 *Banking and Finance Law Review* 305-306.

in which clients interact with banks.[219] M-banking offers individuals (banked or unbanked) greater flexibility to transact anywhere.[220] Stemming from the above, it stands to reason that m-money has the ability to provide greater access, security, convenience and is more cost effective than traditional banking channels while simultaneously minimising the inherent risks and costs associated with cash.[221]

Notwithstanding the above, m-money is not impervious to risk. In this regard, Chatain *et al*[222] confirmed that, from an ML and TF point of view, vulnerabilities such as anonymity, rapidity, vagueness and poor oversight in m-money transactions remain highly relevant. Although the risk of financial crime abuse in m-money has been relatively low, cases of fraud[223] and ML[224] in e-banking have been identified. However, to date no cases of TF abuse within the realm of m-money have been reported.[225]

## 4 How does mobile money work?

At the turn of the century m-money services were non-existent. The reality is that in developing economies more people have access to mobile phones than to traditional bank accounts.[226] The ability to transfer funds through the use of mobile phones has remedied this inequality to some extent and the growth of an increasingly complex m-money ecosystem.[227]

---

219 Fonte 2013 *Washington Journal of Law, Technology and Arts* 421.

220 Tiwari and Buse *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector* 26 -27.

221 Jenkins 2008 http://hks.harvard.edu/m-rcbg/CSRI/publications/report_30_MOBILEMONEY.pdf.

222 Chatain et al 2008 http://siteresources.worldbank.org/INTAML/Resources/WP146_web.pdg.

223 *Uganda v Sserunkuma and 8 others* [2015] UGHCACD 5 (High Court of Uganda Holden, case no. HCT-00-CR.SC 15/2013) and also see Morawczvnski 2015 http://cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion - The Kampala's Anti-Corruption Court is still continuing residing on a major mobile money fraud case where six ex-employees of MTN were charged with defrauding the company of approximately USD 3.4 million.

224 Samani, Paget and Hart 2014 http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf - Liberty Reserve's digital currency service was used to launder US$6 billion.

225 Chatain *et al Protecting Mobile Money against Financial Crime* xxx.

226 Villasenor 2013 http://brookings.edu/research/papers/2013/09/16-smartphones-mobile-money-developing-countries-villasenor.

227 Pénicaud 2013 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/03/MMU_Results-from-the-2012-Global-Mobile-Money-Adoption-Survey.pdf.

### *4.1 Types of mobile money transactions*

In respect of deposit-taking and in terms of section 1 of *the Banks Act*, MNOs are prohibited to offer any cash-out or mobile wallet facilities unless they are authorised to operate the "business as a bank" as defined in the *Banks Act*. Banks can, however, appoint trusted third parties/agents as a branchless bank for the purpose of leveraging of the ubiquitous cellular networks and minimizing the barriers to financial services to the poor. The role of a branchless bank dealing in m-money is to be the interface between a bank and its clients where traditional banking is not accessible.[228] In developing countries, most m-money transactions can be divided into three categories:[229]

a. Store value (currency): Where a client already has a bank account, the funds can be accessed via mobile phone by linking the mobile phone to the account. In the absence of an account, a bank account can still be created online; however, CIV[230] will first have to take place before the account is activated;

b. Cash-in or cash-out stored value: Where the account is linked to a bank account, a client can visit the bank and, in most cases, also the third-party agent of the bank, to cash in or cash out the stored value; and

c. Transfer stored value between accounts: By using a set of SMS messages or PIN codes, funds can be transferred between accounts linked to two mobile phones.

Banks who want to position themselves in a more competitive and innovative market will take advantage of building their own m-money agent networks. Depending on the integration, different types of contrast amongst the partnering bank and the mobile service provider can exist.[231] In the case of a partially integrated partnership, the role of the bank is clearly defined and distinguished from that of the mobile service provider.[232] The bank will provide and own the banking services, whilst the

228 Kumar and Dutta 2015 *Economic and Political weekly* 28.
229 Jonathan and Camilo 2008 *Asian Journal of Communication* 318-322.
230 Section 21 read with exemption 17 of *FICA* 38 of 2001.
231 Jonathan and Camilo 2008*Asian Journal of Communication* 318-322.
232 Jonathan and Camilo 2008 *Asian Journal of Communication* 318-322.

mobile service provider will proved mobile communication infrastructure and control the agent network.[233] The bank will compensate the mobile service provider for access to the network and the bank will benefit from having a greater competitive footprint in the market.

### *4.2 Mobile money models*

Prior to 2008, the m-money models consisted of bank-led and MNOs; however, technology proliferation has created a variety of new, complex emerging models. This evolution has in turn resulted in the fragmentation of services and different players, each playing a key role in m-money transactions.[234] For the purpose of this dissertation only the mobile-network operator-centric and bank-centric mobile payment models will be reviewed.

M-money products are often linked to the prepaid accounts market, where non-bank entities such as telecommunication providers have been successful m-money issuers, subject to regulation or licensing.[235] MNOs can be regarded as playing a crucial role in any of the old and new m-money models.[236] MNOs do not only provide mobile communication services, but also have an ubiquitous immediate communication network that permits transactions to be authorised and settled in real time.[237] In a MNO-centric mobile payment model, mobile payment services are offered as an extension to the core communications services and client funds are held in a prepaid account by the MNO.[238] MNOs also operate a fully encrypted smartcard-based authentication system which is rooted in the client's SIM card.[239] SIM cards enable MNOs to authenticate client and transaction information securely and have the potential for account monitoring. In this regard, Alexandre[240] *et al* believe that except for the regulatory requirements, prepaid cards (SIM cards) and e-money are in

---

233 Demombynes and Thegeya 2012 *World Bank Policy Research Working Paper*, No. 5988.
234 Chatain *et al Protecting Mobile Money against Financial Crime* xxxi.
235 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf
236 Chatain *et al Protecting Mobile Money against Financial Crime* xxxi.
237 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.
238 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.
239 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.
240 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

principle very similar to what banks offer (i.e. saving accounts). In addition, due to their large base of clients, MNOs have a higher level of branch awareness amongst their clients and can at a high degree of reliability and accessibility operate high-volume, real-time pre-paid systems.[241] However, MNOs have no experience in developing financial products beyond basic transactional services.

Stemming from above, both MNOs and banks have realised the mutual benefits of partnering to provide an m-money platform to the poor and unbanked: The MNOs provide the telecommunication network and the banks the electronic payment infrastructure where alternative payment systems (e.g. ATMs) do not exist.[242] Thus, any mobile phone or store can become a client's transactional point where they could access and manage their bank account.[243] Banks and accountable institutions[244] (hereinafter the account providers (APs)) have a long tradition of endorsing product diversity in rendering financial services and are responsible for the delivery and management of m-money services (e.g. account opening, transaction processing and record keeping). This is referred to as a bank-centric mobile payment model.[245] APs are regarded as being the main role players in the provision of mobile payment services.[246] Although retail outlets will manage the bulk of cash transactions on behalf of the AP's clients, APs will still be the cash distribution hub for the non-bank retail outlets.[247] In this regard, regulators and/or supervisors of AML/CTF programmes will look to APs to take all reasonable steps to ensure compliance with AML/CFT international standards and local legislation.[248] Reasonable steps[249] would

---

241 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

242 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

243 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

244 Schedule 1 of *FICA* 38 of 2001 – Provides a list of accountable institutions which *inter alia* includes a person who carries on "business of a banks" as defined in the Banks Act 94 of 1990.

245 Chaix and Torre "Which economic model for mobile payments?" 2-4 and 9-10; and Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf – the clients are account holders of the bank which offers mobile payment services.

246 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

247 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.

248 Chatain *et al Protecting Mobile Money against Financial Crime* xxxi.

249 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

include to know-your-client (KYC), know your agent, monitoring, transaction reporting and training. Retail outlets can also become an agent of AP.

Currently there are no international best practice guidance relating to retail outlets and FATF Recommendations do not require retail outlets to be licensed or regulated.[250] Each country has the authority to decide how they will deal with this.[251] The licensing of the role players would require significant capacity, which will increase the transactional cost of this initiative and thus make m-money products undesirable for the unbanked.

## 5 Financial inclusion and financial integrity

Isern[252] believes that international anti-money laundering (AML) and combating the financing of terrorism (CFT) standards underpin financial integrity and support the fight against crime. The inappropriate application of these standards can cause financial exclusion for millions of economically deprived and unbanked individuals. If this happens, the goals of AML and CFT cannot be achieved. However, it need not be this way as financial inclusion and financial integrity are regarded as complementary and cross-reinforcing policy objectives.[253]

Endorsed by the FATF, the G20 issued the Principles for Innovative Financial Inclusion.[254] This concept was reinforced by the Basel's revised 2012 Basel Core Principles for Effective Banking Supervision.[255] The proportionality principle aims to encourage banks to find the right balance between risk and benefits by tailoring policies and regulatory frameworks in such a way to mitigate risks without imposing

250 Financial Action Task Force 2013 http:/.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

251 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

252 Isern and de Koker 2009 http://cgap.org/publications/amlcft-strengthening-financial-inclusion-and-integrity.

253 Chatain *et al Protecting Mobile Money against Financial Crime* xxx.

254 Principles and Report on Innovative Financial Inclusion 2010 http://gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf.

255 Global Partnership for Financial Inclusion 2014 https://g20.org/wp-content/uploads/2014/12/2014_g20_financial_inclusion_action_plan.pdf.

excessive regulatory limitations on innovation.[256] The criteria for proportionality underpin the application of a RBA,[257] which includes the implementation of reduced client due diligence[258] (hereinafter CDD) for low-risk[259] products, such as m-money.[260]

### *5.1 Financial integrity*

The FATF seeks to effectively address financial integrity risks (i.e. risk of ML, terrorist or proliferation financing risks), in an effort to entice the unbanked[261] into the formal financial service, subject to the application of effective controls.[262] For the purpose of financial integrity, regulators are divided as to how best to regulate m-money.[263] In this regard, Winn *et al*[264] are if the view that balancing regulatory initiatives and market expectation can be problematic. Striving to attain financial inclusion objectives can also lead to non-compliance with international AML and CFT standards, which then could lead to financial exclusion.[265] Furthermore, the application of integrity principles such as KYC and CDD in m-money becomes a perplexing aspect of financial integrity controls, where different business models and role payers exists. The question as to who would be responsible executing the said integrity principles also has to be decided beforehand. For this reason, integration

256 Principle 8 of Proportionality: Proportionality refers to the drafting of a policy and regulatory framework that is proportionate with the risks and benefits involved in such innovative products and services and is based on an understanding of the gaps and barriers in existing regulation - Global Partnership for Financial Inclusion September 2014 "2014 Financial Inclusion Action Plan." https://g20.org/wp-content/uploads/2014/12/2014_g20_financial_inclusion_action_plan.pdf.

257 Recommendation 1 of the 2012 Financial Action Task Force Recommendations htpp://.fatf-gafi.org.

258 Financial Action Task Force Recommendation 10 (required to identify and verify clients) read with Recommendation 15 (assess risk of new payment system prior to implementation). htpp://fatf-gafi.org.

259 "Low risk" refers to cases that may qualify for an exemption from the Financial Action Task Force Recommendations and/or governing legislation to be applied - Financial Action Task Force June 2013 http:/fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

260 Interpretive notes of Financial Action Task Force Recommendation 1: "… Provided … there is a proven low risk of money laundering or terrorist financing;…and relates to a particular type of financial institution or activity…". htpp://.fatf-gafi.org.

261 "Unbanked" refers to individuals who do not have a bank account or access to banking services.

262 Winn and de Koker 2013 *Washington Journal of Law, Technologies and Art* 156.

263 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

264 Winn and de Koker 2013 *Washington Journal of Law, Technologies and Art* 158.

265 "Financial exclusion" refers to inadequate access to financial services on a temporary or long-term basis. – de Koker 2006 *Journal of financial crime* 26-50.

between the regulatory framework and retail outlets becomes fundamental to integrity risk management and business development.[266] Such integration will cause retail outlets to become the client interface for the unbanked, providing both meaningful communications and transaction functionality.

### *5.2. Financial inclusion*

Financial inclusion provides opportunities to enhance financial stability. Not only is financial inclusion one of the core objectives of the World Bank Group, but it is also a key development goal for many developing and emerging countries.[267] Lack of access to banking services forces people to rely on a cash-based economy, which falls outside the ambit of the AML and CFT objectives. M-money is regarded as a cost-effective service that enlarges banking services' footprint to the unbanked.[268] The growth in m-money is, however, reliant on the application of anti-financial crime standards such as the FATF Recommendations (i.e. money laundering/ financing of terrorism risk assessment, KYC, record keeping, reporting etc.), coupled with local legislation.[269] The SARB's Payment System Vision 2015[270] explains that in a global financial crisis, the objective of financial integrity and stability requires a shift in the form of tighter oversight and regulation.[271] In such situations prudent risk management is invariably favoured, but at the expense of financial inclusion. When examining the *NPS Act*, Okeahalam[272] correctly observes that different payment instruments would mitigate against different sets of risks. The trade-off between financial inclusion and risk management must be judged against this background of specific risks. It can be argued that exemption 17 of *FICA* provides a good example of the balance between risk management and financial inclusion, especially in the South African. In the spirit of promoting financial inclusion, exemption 17 reduced

266 Chatain *et al Protecting Mobile Money against Financial Crime* xxxi.
267 Chatain *et al Protecting Mobile Money against Financial Crime* xiii.
268 Winn and de Koker 2013 *Washington Journal of Law, Technologies and Art* 155 – 156.
269 Chatain *et al Protecting Mobile Money against Financial Crime* xxx.
270 South African Reserve Bank 2015 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem%28NPS%29/Documents/Overview/Vision2015.pdf.
271 Lawack 2013 *Washington Journal of Law, Technology and Arts* 327-329.
272 Okeahalam 2003 *Journal of Banking Regulation* 338.

the CIV obligation[273] placed upon financial institutions, subject to the discharge of certain requirements. Lawacks,[274] however, believes that South Africa's legal and regulatory framework for m-money is not fully inclusive due to the challenges around undocumented migrants. It follows therefore that it is important that policymakers should try to eliminate barriers not conducive to financial inclusion and integrity objectives by finding the right balance between risks and benefit.[275]

Alexandre and Eisenhart[276] advocate the exclusion of regulatory limitations from m-money products, which are able to attain the objectives of financial inclusion and financial integrity. Their rationale is based on the belief that there are synergies between financial inclusion and financial integrity as m-money reduces dependence on a cash-based system, accelerates the development of bank accounts and generates data pivotal for financial inclusion and financial integrity.[277]

M-money can facilitate access to financial services for sustainable development, but will require close monitoring with regard to TF and ML risks. By finding the perfect balance between financial inclusion and financial integrity objectives, m-money has the capability to drive digital inclusion in developing countries, far beyond the current reach of traditional branch banking services.[278] This requires a fine balancing act between access to payment systems and regulation of AML/CFT risks.[279]

## 6 Risk-based approach

The application of a RBA has become one of the overarching principles of international standard-setting bodies such as the FATF, Basel[280] and the European Union (EU).[281] Having echoed the importance of identifying and assessing ML and TF risks linked with emerging payment systems (i.e. m-money), the applications of an

273 Section 21 of *FICA* 38 of 2001.
274 Lawack 2013 *Washington Journal of Law, Technology and Arts* 317.
275 Demirgüç-Kunt, Beck and Honohan 2008. http://go.worldbank.org/HNKL9ZHO50.
276 Alexandre and Eisenhart 2013 *Washington Journal of Law, Technology and Art* 258.
277 Winn and de Koker 2013 *Washington Journal of Law, Technologies and Art* 159.
278 Villasenor 2013 http://brookings.edu/research/papers/2013/09/16-smartphones-mobile-money-developing-countries-villasenor.
279 Lawack 2013 *Washington Journal of Law, Technology and Arts* 318 – 344.
280 Basel Committee on Banking Supervision 2014 http://bis.org/publ/bcbs275.pdf.
281 Stokes 2012 *Information and Communications Technology Law 224* – 227.

RBA has become mandatory for all financial institutions.[282] Basel regards the implementation of sound RBA and risk management programme[283] to all types of risk as part of banks' general obligations.[284] It follows therefore that the absence thereof would expose banks to costly reputation, operational, compliance, systemic and concentration risks, which would undoubtedly have an impact on financial stability.

The application of simplified CDD to low-risk[285] products and services are based on FATF Recommendation 1 (i.e. application of an RBA). Recommendation 15 of the FATF Recommendations reinforces the application of a fundamentally sound RBA obligation prior to the implementation of new payment systems, such as mobile payment services.[286]

Stemming from the above, a prerequisite for the implementation of a sound RBA and effective ML and TF risk management (i.e. monitoring of client profile, business relationship and detection of suspicious activity) requires accurate mapping of ML/TF risks.[287] Depending on the relevant bank's business model and risk appetite, mapping of ML/TF risks can start at a risk assessment and rating of a product/service, client, sector or jurisdiction. The ML/TF risk assessment should be informed by an understanding of the client's profile and the pertinent risks associated with that client. Moreover, the allocated risk rating must be commensurate with the identified risk.[288] Based upon the application of an adequate risk assessment, banks have the

---

282 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

283 In terms of principle 15 of the Basel Core Principles, sound risk management requires the analysis and identification of money laundering and terror financing risks, which would inform the design and effective implementation of policies and procedures that are commensurate with the identified risk - Basel Committee on Banking Supervision 2012 http://bis.org/publ/bcbs213.pdf.

284 Basel Committee on Banking Supervision 2014 http://bis.org/publ/bcbs275.pdf.

285 "Low risk" refers to cases that may qualify for an exemption from the Financial Action Task Force Recommendations and/or governing legislation to be applied - Financial Action Task Force 2013 http://atf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

286 Financial Action Task Force 2012 http:// fatf-gafi.org/publications/fatfrecommendations/#?hf=10&b=0&s=desc(fatf_releasedate).

287 Chatain *et al Protecting Mobile Money against Financial Crime* xxxii.

288 Basel Committee on Banking Supervision 2014 http://bis.org/publ/bcbs275.pdf.

discretion to apply simplified CDD[289] measures to low-risk products and services.[290] The absence of adequate controls and monitoring can lead to an abuse of the application of simplified CDD. It was noted in Australia's FATF Mutual Evaluation Report of 2015, that FATF raised serious concerns on the excessive use of exemptions (i.e. simplified CDD), which can diminish the application of CDD.[291]

Within m-money the risk profiles may differ from model-to-model and the various roles can be carried out either by a single entity or via an agent. This in itself creates regulatory challenges in establishing where to place the responsibility for implementing sound AML/CFT controls and oversight.[292] This simply highlights the need to establish appropriate and proportionate regulations to ensure the sustainability of m-money services.[293]

The FATF has in numerous reports[294] highlighted the potential for financial abuse of any financial product which has the capability to mask ownership and identity, whether intentionally through product design or operational use. Both the FATF and the 3rd EU Directive[295] echo the recognition of greater risks of non-face-to-face transactions and recommend the application of enhanced due diligence (hereinafter EDD).[296] The lack of transactional record keeping becomes a problem when trying to reconstruct the illicitly performed transactions, especially with prepaid mobile phone handsets, were no account statements are available. Telecommunications entities

---

289 "Simplified client due diligence" must be based on a thorough risk-assessment that fully justifies the decision taken. It refers to a lower level of due diligence, where there is little opportunity of risk.

290 Financial Action Task Force 2012 "International standard on combating the money laundering and financing of terrorism and proliferation" http://fatf-gafi.org/publications/fatfrecommendations/#?hf=10&b=0&s=desc(fatf_releasedate).

291 Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf.

292 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

293 Chatain *et al Protecting Mobile Money against Financial Crime* xxxi.

294 Financial Action Task Force 2013 http:// fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf; Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

295 Article 13(2) and 13(11) of the *Second Money Laundering Directive, Directive 2001/97/EC* and recommendation 15 of the 2012 Financial Action Task Force Recommendations Financial Action Task Force 2012 http://fatf-gafi.org/publications/fatfrecommendations/#?hf=10&b=0&s=desc(fatf_releasedate).

296 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

focuses on the monitoring of telephone accounts were credit agreements are in place and not so much on prepaid phone transactions. Furthermore, the risk posed by anonymity has resulted in both the FATF and the EU prohibiting anonymous accounts.[297] As a result, identifying the relevant laws applicable to the gathering of evidence and the contravention relating to electronic transactions can become an unattainable task.

Although *FICA* is fundamentally rules-based, this did not deter the Financial Intelligence Centre (FIC), in its FIC Guidance Note 1 on identification of clients,[298] from recommending that banks should start implementing a risk-based framework, which would place them in a position to rate the perceived riskiness of their clients and products (i.e. m-banking).[299] Due to the barriers[300] placed upon the use of *Banks Act* Circular 6/2006 and Exemption 17 of *FICA* products, it is believed that these products which poses a low risk for ML and TF should be supported by adequate controls (e.g. transaction monitoring).[301] De Koker[302] cautions that the risk profile of low-risk products are subject to reviews as criminals identify vulnerabilities within the system to circumvent controls.

The FIC has noted that clients can avail of more than one financial product at any bank. However, the FIC also recommended[303] as a sound business practice that banks apply the concept of a "single view of a client's profile", suite of products and services within the bank. By being able to have a holistic view of the client's profile

---

297 Article 6 of the Second Money Laundering Directive, Directive 2001/97/EC and recommendation 10 of the Financial Action Task Force Recommendations 2012 http://fatf-gafi.org/publications/fatfrecommendations/#?hf=10&b=0&s=desc(fatf_releasedate).

298 Financial Intelligence Centre 2004 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf.

299 De Koker 2008 http://finmark.org.za/wp-content/uploads/pubs/Rep_ML_Riskmanagement_prodserv_SA_May08.pdf.

300 Limitations such as it could only be access by natural South African citizens/residents, in Rand, linked to a daily and monthly limit, within the confines of the Common Monetary Area (i.e. South Africa, Botswana, Lesotho, Swaziland and Zimbabwe).

301 De Koker 2008 http://finmark.org.za/wp-content/uploads/pubs/Rep_ML_Riskmanagement_prodserv_SA_May08.pdf.

302 De Koker 2009 *Journal of Money Laundering Controls* 333-334.

303 Financial Intelligence Centre 2014. https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/AP140213%20PCC26%20Single%20Client%20View.pdf.

and suite of products/services linked thereto, banks are able to consistently and coherently apply an RBA.

Risk is by nature elusive and fluid. In the words of Stokes:[304]

> …the fight against money laundering is one that will never be won, certainly without imposing excessive obligations on virtually any product and service provider; focusing attention on one area simply displaces laundering activities to another.

## 7 Economic and financial crime

Within the context of economic and financial crime, Grimmelamann[305] stated that "If power corrupts, then automatic power corrupts automatically." While automated payment systems, such as m-money, make financial services accessible to the unbanked, at the same time it creates a funnel of opportunities for criminals who have identified weaknesses within the financial system. The use of the financial payment system by criminals consists of multiple phases, executed by a borderless network of specialists. By using a combination of modalities (e.g. identity theft, data value smurfing etc.) criminals can quietly and systematically survey and map vulnerabilities in banks' financial crime controls and third-party processors' systems.[306]

In one of the largest international ML cases, where Liberty Reserve's[307] digital currency service was used to launder USD 6 billion, the US attorney, Preset Barbara stated the following:[308]

> …The only liberty that Liberty Reserve gave many of its users was the freedom to commit crimes. The coin of its realm was anonymity, and it became a popular hub for fraudsters, hackers, and traffickers…

The above case adds impetus to the theory that digital currencies, such as m-money, can become a more prevalent product for criminals to launder money and possibly

---

304 Stokes 2013 *Banking and Financial Service Policy Report* 2-6.

305 Grimmelamann 2014 http://ssrn.com/abstract=2358627.

306 Ernst and Young 2013 http://ey.com/Publication/vwLUAssets/The_evolution_of_borderless_financial_crime/$File/1310-1152512_FinancialCrimeMngt_Broch_v6.pdf.

307 *USA v Liberty Reserve S.A. and 7 others* [2013] CRIM 368 (United States District Court, Southern District of New York).

308 Samani, Paget and Hart 2014 http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf - Before its operations were closed, the Liberty Reserve digital currency service was used to launder US$6 billion, a sum that constituted the largest international money-laundering prosecution.

finance terrorist activities.[309] Captain[310] believes that m-money services are more susceptible to ML and TF activities in geographic areas where corrupt governments, traffickers and transnational crime kingpins thrive.

Exacerbating an already precarious situation, globally law enforcement agencies do not have the intelligence and expertise in m-money methodologies and technology to appropriately monitor, investigate and prosecute such activities. Law enforcement agencies struggle to grasp many low-tech, but highly effective, ways in which criminals launder money and finance terrorism. This, coupled with a lack of codified authority to examine abuse in the communications systems, simply adds to the challenge of obtaining physical evidence.[311] For instance, when funds are electronically transferred via a mobile phone and the phone is destroyed, it may become very complex to reconstruct the transaction. Even with a prepaid phone, the service provider may not be able to identify its client in the absence of credit risk and account monitoring. Criminals can buy prepaid mobile phone handsets with false identification and use the minutes preloaded on the phone without leaving a trace of a calling record.[312] Cassara also found that some m-money networks utilise security features which can deter efforts to identify and flag suspicious transactions.[313]

### *7.1 Illicit use of digital money such as mobile money*

The promotion of new payment systems such as m-money can vastly impact on how money is concealed, laundered or used to finance terrorist activities.[314] Stokes[315] found that technologically advanced payment instruments have a low degree of transparency due to the lack of face-to-face contact with the client and different payment models available. Through peer-to-peer movements, value can be

---

309 Samani, Paget and Hart 2014 http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf.

310 Chatain *et al Protecting Mobile Money against Financial Crime* xxix.

311 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

312 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

313 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

314 Cassara date unknown "Mobile payments, smurfs and emerging threats" http://sas.com/en_us/insights/articles/risk-fraud/mobile-payments-smurfs-emerging-threats.html.

315 Stokes 2013 *Banking and Financial Service Policy Report* 2-6.

transferred without interfacing with banks.[316] The general approach to AML/CFT regulations is the reliance on using financial institutions as *de facto* policemen and guardians of financial systems.[317]

To assess the extent to which the use of new innovative payment systems, such as m-money, can be attractive to criminals, it is important to evaluate the associated opportunities and limitations. The US Secret Service *inter alia* listed the follow reasons why criminals prefer using digital currencies:[318]

a. it has the ability to effect transfers rapidly, securely and with a perceived degree of anonymity (face-to-face identification and interaction are not required);

b. it provides an opportunity to extend financial crime without geographical barriers. Merlonghi found that this makes it difficult to determine the law applicable to the illicit action;[319]

c. due to the threshold limits, it has a low transactional value, but high volume and low volatility. M-money transactions are regarded as low risk, thus making them ideal transmission channels, especially in the financing of terrorism as simplified CIV is applied[320]; and

d. it is generally accepted in the criminal underworld.[321]

M-money is susceptible to many potential ML and TF scenarios. The following are the various methods used by criminals to abuse digital currencies, such as m-money, to launder money and/or finance terrorism:

### *7.1.1 Digital surfing*

Digital value smurfing[322] represents just one way in which criminals will exploit the mobile payment system to conceal illicit proceeds or finance terrorism.[323] Traditional

316 Stokes 2013 *Banking and Financial Service Policy Report* 2-6.
317 Stokes 2013 *Banking and Financial Service Policy Report* 2-6.
318 Trautman 2014 *Richmond Journal of Law and Technologies* 7.
319 Merlonghi 2010 *Journal of Money Laundering Control* 205-207.
320 Trautman 2014 *Richmond Journal of Law and Technologies* 7.
321 Trautman 2014 *Richmond Journal of Law and Technologies* 7.

ML in the form of smurfing takes place when large transactional amounts are divided up into smaller amounts that fall outside the reporting threshold or system alert limits.[324] In short, smurfing is the same as structuring. It requires a number of digital 'smurfs' to exchange these small amounts of illicit money for digital value which is stored on a mobile phone.[325] On the same basis, digital smurfing is used to sidestep regulated banks[326] and evade the reporting requirement[327] for the purpose of transferring the values held on the mobile phones to accounts controlled by organised crime.[328] It should be noted that threshold limits placed upon qualifying users of m-banking products, in terms of Exemption 17 of *FICA*, fall outside the cash reporting threshold limit of R24 999-99.[329] Furthermore, funds can also be transferred via a mobile phone as a contribution to a terrorist organisation, without raising any alerts.[330] De Koker[331] is of the view that Exemption 17 accounts are not immune to ML/TF abuse and could be used as a secondary account or even a primary account for the transfer of illicit funds. These funds could be easily access via different ATMs.[332] The avoidance of moving physical cash, the speed of converting cash into digital value and the potential to integrate different digital tools, such as smart and prepaid cards, makes digital smurfing a very attractive ML and TF technique for criminals.[333] Stemming from the above, one can argue that even criminals have realised the benefits of applying risk management to their criminal activities.

---

322 "Digital value smurfing" a termed coined by the Asian Development Bank. Also referred to as "splitting" - De Koker 2009 *Journal of Money Laundering Control* 330.

323 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

324 De Koker 2015 *South African Money Laundering and Terror Financing Law* 51.

325 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

326 "Smurfing" is regarded as a criminal offence in terms of s 64 of *FICA* 38 of 2001 – avoiding giving rise to a reporting duty.

327 Section 29 of *FICA* 38 of 2001 – requires the file of a suspicious or unusual transaction report with the Financial Intelligence Centre and S28 of *FICA* 38 of 2001 – requires the reporting of any cash transactions and the aggregation thereof in the excess of R24 999-99 within 2 days to the Centre.

328 Cassara 2015 http://mobilepaymentstoday.com/articles/out-of-africa-aml-compliance-for-mobile-payments/.

329 Section 28 of *FICA* 38 of 2001.

330 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

331 De Koker 2009 *Journal of Money Laundering Control* 330.

332 Reuters 2016 http://reuters.com/article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB - During end May 2016 criminals managed to counterfeit Standard Bank credit card and withdraw 1.4 billion yen (approximately USD 3 million) via effecting in 14 000 transactions using ATM machines.

333 Cassara 2008 http://state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm.

In October 2006 FATF reported on a new payment method and noted a case study of a suspicious activity report filed in the United States, which detailed a case where as single individual had managed to use over 300 prepaid cards to transfer approximately USD 2 million to Colombia.[334] This clearly exemplifies how much money can be laundered or used to finance terrorism through digital smurfing and using prepaid cards.

### *7.1.2 Fraud*

During April 2015 the High Court (Kampala's Anti-Corruption Court) in Kampala, Uganda, convicted six out of nine former MTN employees relating to a major m-money fraud case, implicated in defrauding the company of approximately USD 3.4 million.[335] Because MTN's suspense account did not have adequate reconciliation procedures in place, criminals managed to take advantage of MNT's frail Mobile Money system (called Fundamo). The fraudsters were able to manipulate the system internally, generating e-money on the m-money system and transferring millions through various mobile accounts, within the space of 7 months.[336] The e-money generated was, however, not backed by physical cash in MTN's bank account held with Stanbic, with the resulting effect being a substantial variation between the MTN's mobile general ledger account and its bank balance at Stanbic.[337] Tigo Tanzania's mobile service provider also lost USD 170 000, when it was defrauded during 2014, as a result of manipulation of the mobile money system by staff[338]. MNT Uganda was not the only company impacted by fraud, as Stemming from the above, it can be argued that this case illustrates the consequences of insufficient financial crime controls, a lack of monitoring and adequate governance. Fraud and ML of this

---

334 Financial Actions Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf and reference in Saksenberg, Sptiz and Meyer 2008 FICA Training Manual 38.

335 *Uganda v Sserunkuma and 8 others* [2015] UGHCACD 5 (High Court of Uganda Holden, case no. HCT-00-CR.SC 15/2013) and also see Morawczvnski 2015 http://cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion.

336 Morawczvnski 2015 http://cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion.

337 Morawczvnski 2015 http://cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion.

338 Anon 2014 http://itnewsafrica.com/2014/06/police-bring-down-tigo-call-credit-fraud-ring/.

nature can have a negative impact on client confidence and regulators' trust, and it significantly impacts on the integrity of the financial system.

### *7.1.3 Software vulnerabilities*

One of the biggest perceived advantages upon which the integrity of m-money rests is the assurance that the systems used are secured against any criminal attacks.[339] M-money has a close relationship with other technologies. The University of Florida[340] published a security analysis of m-money applications (hereinafter apps) assessed in developing countries. The research team found that smartphone apps with inappropriate access control, inadequate information security (information leak) and weak authentication/encryption could provide cyber attackers[341] with access to account information, and allow for both identity and monetary theft.[342] An example of weak system controls can be found in the case where a Starbucks app allowed clients to pay at the checkout with points using their m-money application.[343] It was noted and reported to Starbucks that in most cases when payment was effected via the m-money application, the application would simultaneously reload Starbucks[344] gift cards by automatically drawing funds from the client's bank account or PayPal account. Hackers had managed to gain access to a number of clients' accounts, loaded the Starbucks gift cards and transferred it to other accounts.[345] Starbucks[346] reported that

---

339 Reaves, Scaife, Bates, Traynor and Butler 2015 http:/cise.ufl.edu/~traynor/papers/reaves-usenix15a.pdf.

340 Reaves, Scaife, Bates, Traynor and Butler 2015 http://cise.ufl.edu/~traynor/papers/reaves-usenix15a.pdf.

341 During April 2013 the federal prosecutors of New York reported the arrest of seven suspects involved in the biggest, "surgical" cyber bank heist, which inter alia involved 40 50 ATM withdrawals and 17 pre-paid credit cards. Approximately USD 45 million was stolen and some of the funds were laundered in buying Rolex watches - Weber 2013 http://theweek.com/articles/464499/great-atm-heist-how-thieves-brazenly-stole-45-million-few-hours.

342 Traynor and Butler 2015 http://theguardian.com/global-development-professionals-network/2015/sep/24/mobile-money-apps-security-flaws-study-reveals.

343 Starbucks processes 7-million mobile money transaction per week and aims to play a significant role and want to leverage the equity of their brand in the way how people effect payments – Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/.

344 Starbucks processes 7-million mobile money transaction per week and aims to play a significant role and want to leverage the equity of their brand in the way how people effect payments – Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/.

345 Starbucks processes 7-million mobile money transaction per week and aims to play a significant role and want to leverage the equity of their brand in the way how people effect

during 2015, it processed about 7-million m-money transactions a week. Stemming from the above and due to inadequate Starbuck application software controls, if a hacker loaded an average of USD 5-00 Starbucks gift card on every m-money transaction, the criminal could potentially launder or contribute to terrorism an amount of USD 35 million per week.

During April 2016 the chief executive of Vodacom business, Vuyani Jarana,[347] conceded that cybercrime in mobile devises are becoming a more prevalent threat. During 2015 the Kaspersky Security Bulletin Overall Statistics Report for 2015[348] confirmed that for the first time mobile financial crime threats has rank among the top ten criminal methods to steal money from clients. The Kapersky Lab managed to identify over 145 00 new malicious programmes linked to mobile devices were identified and approximately 4-million malicious applications are used to distribute mobile malware to Android-based devise, which maleware is focused on depriving users of their money.[349]

### *7.1.4 False and ghost identity documents*

For the purpose of opening a bank account criminals can either opt to use false identity documents in the name of existing or non-existing (ghost) individuals.[350] In its October 2013 report,[351] the US Department of Justice announced that Nicolae Popescu and his criminal syndicate had managed to open bank accounts and procure high-value assets through the use of high-quality fake passports as identification. By using similar techniques, there is nothing preventing m-money products from being

---

payments – Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/.

346 Starbucks processes 7-million mobile money transaction per week and aims to play a significant role and want to leverage the equity of their brand in the way how people effect payments – Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/.

347 IT Web Security 2016 http://itweb.co.za/index.php?option=com_content&view=article&id=151192.

348 Kaspersky Lab 2015 http://kaspersky.com/about/news/virus/2015/Kaspersky-Lab-mobile-banking-threats-among-the-top-10-malicious-financial-programs-for-the-first-time.

349 Kaspersky Lab 2015 http://kaspersky.com/about/news/virus/2015/Kaspersky-Lab-mobile-banking-threats-among-the-top-10-malicious-financial-programs-for-the-first-time and https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf.

350 De Koker 2008 http://finmark.org.za/wp-content/uploads/pubs/Rep_ML_Riskmanagement_prodserv_SA_May08.pdf.

351 Department of Justice 2013 http://justice.gov/opa/pr/2013/Octobe/13-crm-1128.html.

abused for ML and TF purposes, as no face-to-face interaction is required once an account has been activated.

### *7.1.5 Drugs*

The close alliance between drug trafficking and global terrorist groups has become a major concern for most financial crime authorities. The most significant example of a site being responsible for the major sale of drugs and possible TF can be found in the case of Silk Roads, which operated as an intermediary by providing buyers and sellers with a transactional infrastructure platform.[352] Furthermore, the case of Liberty Reserve illustrates how a system can be manipulated to allow illicit financial transactions to be effected under multiple layers of anonymity and through the use of new payment systems such as digital currency.[353]

### *7.1.6 Politically exposed persons and sanction list*

In line with the FATF's Recommendations, South Africa's anti-ML regulations were drafted with one of its aims being the promotion of financial inclusion for the economically disadvantaged in the form of Exemption 17 of *FICA* . The exemption relaxed the requirement to identify and verify a client's residential address and paved the way for innovative products such as m-money accounts.[354] Due to the low cash transaction threshold limits, banks regard Exemption 17 products as low risk and as such could apply a SDD. Although exemption 17 products are intended to serve the poor, nothing prohibits politically exposed persons from opening such accounts.[355] Furthermore, the need to move money electronically and the application of SDD may leave banks vulnerable to possible funding of terrorism as transactions might only be screened against the notice issued by the President[356] (i.e. United Nations Security Council Resolutions[357] sanctions' lists) under section 25 of the *Protection of*

---

352 Mcdermid 2015 http://reuters.com/article/2015/10/05/us-usa-bitcoin-auction-idUSKCN0RZ1SP20151005.

353 Trautman 2014 *Richmond Journal of Law and Technologies* 87-89.

354 De Koker 2008 http://finmark.org.za/wp-content/uploads/pubs/Rep_ML_Riskmanagement_prodserv_SA_May08.pdf.

355 Exemption 17 of *FICA* 38 of 2001.

356 Section 28A of *FICA* 38 of 2001.

357 UNSCR sanctions list.

*Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004, after the transaction was effected.

### *7.1.7 Attacks on businesses*

Hacking attacks on businesses have been a prominent feature in newspapers in recent times.[358] These attacks are aimed at stealing intellectual property, gaining access to bank accounts,[359] distributing malware[360] and unsettling the financial integrity of the business sector.[361] It has been noted that many illicit cyber services are available and can be purchased with any form of digital money (i.e. credit card or electronic fund transfer (EFT)).[362]

## 8 Concluding remarks

It is becoming increasingly difficult to "follow the money" in a digital world. The synergy between mobile, banking and digital payment systems has opened the doors to financial participation for the economically deprived[363], but at the same time created opportunities for criminals to avoid detection working in a virtual world.

The backbone of a strong economy and stable financial market is found in well-functioning and sound payment systems. Whilst the demise of the use of physical cash is not imminent, banks need to continue to be innovative in an increasingly competitive operating environment. Regulators will therefore also have to ensure that the regulatory framework leaves enough room for payment innovation.[364] In this

---

358 CNNMoney (New York) 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/ and Bankrate 2015 http://bankrate.com/finance/savings/could-bank-hackers-steal-your-money-1.aspx**.**

359 Cluley 2015 http://hotforsecurity.com/blog/hackers-steal-5-million-from-ryanairs-bank-account-11744.html - it was reported that the budget airline Ryanair was hacked and managed to steal Euro 4.6-million (equal to USD 5-million) via a fraudulent electronic transfer to a Chinese Bank.

360 "Malware" (malicious software) can be defined as programmes which often masquerade as useful programmes that are aimed at carry out harmful actions - U.S. Gov't Accountability Office 2009 http://defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf.

361 Pinguelo and Muller 2011 http:/vjolt.net/vol16/issue1/v16i1_116-Pinguelo.pdf.

362 Department of Justice 2013 http://justice.gov/criminal/pr/speeches/2013/crm-speech-131118.html.

363 Demombynes andThegeya 2012 http://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5988.

364 Fung, Molico and Stuber 2014 http://banqueducanada.ca/wp-content/uploads/2014/04/dp2014-2.pdf.

regards, Lawack[365] is of the view that South Africa's regulatory framework is not entirely conducive for greater financial inclusion and he accordingly advocates for the implementation of an enhanced RBA to balance the regulation of risk and access to payment systems.

[365] Lawack 2013 *Washington Journal of Law, Technology and Arts* 318 – 344.

# CHAPTER 4

# INTERNATIONAL STANDARDS

*…the fight against money laundering is one that will never be won, certainly not without imposing excessive obligations on virtually any product and service provider; focusing attention on one area simply displaces laundering activities to another….*[366]

## 1 Introduction

The birth of electronic currencies,[367] facilitated by financial innovations such as m-banking, has heralded a new age of wider access to faster and more efficient commercial transactions. However, such innovative payment methods pose numerous potential threats.[368] Zagaris and MacDonald[369] already in 1992 warned that:

> …technological breakthroughs offer more sophisticated variations of traditional means to launder ill-gotten proceeds.

Supported by the application of international standards[370] and domestic legislation[371] focused on fighting the threats of ML/TF, a resilient economy and stable financial market are premised upon well-functioning and sound payment systems.

---

366 Stokes 2013 *Banking and Financial Service Policy Report*.

367 Electronic currencies are also referred to as digital currency. In the context of this dissertation, "digital currency" is taken to mean a legally established fiat currency (legal tender) which is stored and transferred electronically. It is essentially money that can be exchanged via the use of a computer or mobile phone, without using physical currency.. Consultative Group to Assist the Poor (CGAP) 2014 http://cgap.org/publications/bitcoin-vs-electronic-money and Bitcoin magazine 2014 https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507.

368 IT Web Security 2016 http:// tweb.co.za/index.php?option=com_content&view=article&id=151192.

369 Zagaris and MacDonald "199 George Washington Journal of Law and Economics" 26, 61 and 63.

370 Financial Action Task Force Recommendations, Wolfsberg Principles (best banking practices), the Basel Core Principles for Effective Banking Supervision (29 Core Principles), the Vienna Convention (i.e. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substance), Palermo Convention (i.e. United Nations Convention on Transnational Organised Crime) and the Terrorist Financing Convention (i.e. International Convention for the Suppression of the Financing of Terrorism).

371 The *Banks Act* 94 of 1990, *FICA* 38 of 2001, the *Prevention of Organised Crime Act* 121 of 1998 and *the Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004.

The signing and adoption of the United Nations[372] Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in December 1988 marked the beginning of a global effort to focus efforts on the fight against money laundering.[373] The terrorist attacks on the Twin Towers of the World Trade Center in the United States of America (USA) on 11 September 2001[374] highlighted the development of transnational terrorists networks such as Al Qaeda and the impact unlawful activities can have on a nation as well as the global economy. It also required law enforcement to place more emphasis on the implementation of effective, preventative measures to combat serious crimes such as money laundering and financing of terrorism. The recent terrorist events in Paris[375] and Brussels[376] re-affirmed the need for different pieces of legislation, rules and procedures to be aligned in an effort to make monetary transactions more transparent and monitorable, to implement control measures, and to manage ML/TF more appropriately. The continuing development in payment systems, products and services has not only provided access to the unbanked, but at the same time has provided a tool for criminals to communicate and access funds through the use of mobile phones. The proliferation of digital currencies further allows payment services and mechanisms to be used for financial abuse, such as ML, TF and cybercrime.[377]

Internationally, efforts generally tend to rely on the use of soft law to implement a common approach and policies by setting international standards to combat ML and TF.[378] Although soft law is non-binding, the flexibility and speed with which it may be

---

372 The United Nations was the first international organisation focused on combating money laundering on a global basis – Schott 2006 Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism.

373 United Nations 1988 https://unodc.org/pdf/convention_1988_en.pdf.

374 The United States of America Act, 2001, https://gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf. Commonly known as the "The Patriot Act" of 2001, it was percolated following the attacks on the Twin Towers of the World Trade Centre in New York in September 2001. This provided the US government with the appropriate tools required to intercept and obstruct terrorist acts.

375 BBC 2016 http://bbc.com/news/world-europe-35899353 – Belgian officials found that the DNA of Najim Laachraoui was also found on the site of the November 2015 terrorist Paris attracts.

376 Gramham *et al* "Brussels terror attacks metro airport suspects live" *Telegraph* (26 March 2016); Telegraph 2016 http://telegraph.co.uk/news/worldnews/europe/belgium/12204399/Brussels-terror-attacks-metro-airport-suspects-live.html.

377 McAfee unknown date http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf.

378 Delston and Walls 2009 *Case Western Reserve Journal of International Law* 89.

amended assist countries to facilitate and coordinate efforts to focus on emerging risks[379] of illicit activities such as ML/TF.[380]

Against the background provided above, this chapter will provide an overview of the multifaceted interaction between international financial regulation and innovative payment methods. As will be discussed in greater detail, regulation can disrupt or stifle innovation, but it may also spur on innovation.[381] This chapter will also analyse the implementation and effect of soft law in an attempt to curb the vulnerabilities and speed at which criminals are taking advantage of new innovative payment technologies, with due regard to the fact that technical innovations are developing at a much faster speed than preventative measures in ML/TF.

## 2 Soft law: Regulatory methodologies

The interrelationship between regulation and innovation almost invariably results in a mismatch and the subsequent balancing of equally important needs, such as a sound financial payment system, and relevant economic and social developments (i.e. access to banking services). The speed at which evolution takes place in the fields of technology and the pace at which laws are amended in the financial sphere do therefore not keep track. As such, policymakers find it difficult to design an approach to regulatory gaps within the ever-evolving ambit of economic commerce. The resulting effect is that globally, substantial reliance is placed on the application of soft law[382] to coordinate finance and banking regulations.[383] To achieve the desired

---

379 ISO 3100 (2009)/ISO Guide 73:2002 - "International risk management standards define risk as a function of likelihood of occurrence and the consequence of the risk event, where likelihood of occurrence is a function of the coexistence of the treat and vulnerability…". Examples of emerging ML/TF risk can be found in Gramham C *et al* "Brussels terror attacks metro airport suspects live" *Telegraph* (26 March 2016); Telegraph 2016 http://telegraph.co.uk/news/worldnews/europe/belgium/12204399/Brussels-terror-attacks-metro-airport-suspects-live.html and BBC 2016 http://bbc.com/news/world-europe-35899353 - Belgian officials found that the DNA of Najim Laachraoui was also found on the site of the November 2015 terrorist Paris attracts.

380 Delston and Walls 2009 *Case W. Res J.INT'L L.* 89-90.

381 White 1997 *Technological Change, Financial Innovation and Financial Regulation in the US: The Challenges for Public Policy* and Lexis Securities Mosaic 2000 http://lexissecuritiesmosaic.com/gateway/sec/speech/97_white.pdf.

382 Gold 1997 *The American Journal of International Law* stated that "Soft law confirms a preference and not an obligation that states should act or refrain from acting, in a specific manner". As such soft law contains no binding obligation.

383 Delston and Walls 2009 *Case W. Res J.INT'L L.*

outcome of international coordination, the use of *lex ferenda* (the law as it should be) as opposed to *lex lata* (the law as it exists), has served several important functions. Both methodologies[384] provide advantages and weaknesses, summarised in the interest of brevity in annexure 4.1.

In trying to balance the mismatch between financial regulation and market needs, regulation would typically go through a cycle of de-regulation and re-regulation.[385] Consequently, this interaction also creates vulnerabilities in the regulatory framework. Thus, in an attempt not to distort the rapid and beneficial innovation of new innovative payment methods, government's approach to emerging or perceived financial market risks can be assessed by applying two different methodologies of regulatory adjustment, namely either the *laissez-faire* or forward-thinking approach.[386]

### *2.1. Lex lata*[387]

It has been noted that most central banks opt to apply the *laissez-faire*[388] or "wait-and-see" approach to the possible regulation of new innovative payment technologies. This approach to risk mitigation holds that regulations should be technically neutral, allowing the industry to discover the best solution.[389] Favouring the freedom of the industry to facilitate rapid development of new payment technologies would permit central banks to monitor the impact (if any) of such products and services on the market, their function, and the regulatory and operational requirements.[390]

To avoid rigid regulations that might adversely impact the introduction of new technologies and impede financial growth, this approach depends on both the

384 Mboweni 1999 http://bis.org/review/R9991013b.pdf and Mann *The Legal Aspect of Money: With Special Reference to Comparative Private and Public International Law* 4th ed. 8.

385 Huang *The Law and Regulation of Central Counterparties* 129 - 130.

386 Mann 2004 TLR 702 - 704.

387 Also known as *de lege late*.

388 Unknown unknown date *Definition of Laissez-faire* http://investopedia.com/terms/l/laissezfaire.asp - described the laissez-faire approach as an 18th century economic theory, which advocates the believe that "less government is involved in free market capitalism, the better the business will be and then by extension society as a whole."

389 Huang *The Law and Regulation of Central Counterparties* 129-130.

390 Mboweni 1999 http://bis.org/review/r991013b.pdf; Mann 2004 TLR 703-704.

industry to regulate itself and litigation to mitigate any inequalities.[391] The wait-and-see approach largely shuns regulatory intervention, with proponents of this approach arguing that regulation might limit entry and competition.[392] This regulatory approach is thus less specific in nature and intends to permit attentive assessment of potential opportunities and risks, while allowing for business to develop before burdening it with regulations.[393] However, the attributes of this approach also reveal its flaws. For instance, the absence of a suitable legal framework to protect consumers against glitches in the system may stifle the speed of market entry. Stinglitz's[394] information asymmetry highlights another weakness of this approach, namely the knowledge disparity between the consumer and the suppliers of m-money apps. An example of information asymmetry is the case where Starbucks' gift card reload system was hacked and without the clients knowing of Starbucks' weak application protection software, clients' funds were illegally transferred to the criminal's account.[395] The knowledge disparity in this regard was that Starbucks' clients were under the impression that Starbucks' m-money application was protected by an adequate software security application. This also highlights the need for a legal framework to be in place to guard against systemic risks that flow from a lack of operational oversight by institutions that implement these products and services.[396] Consequently the wait-and-see approach to regulation causes an unequal playing field to those institutions that mitigate systemic and operational risks at the cost of limiting client intake when compared to institutions with no risk controls, which consequently would allow easy access to criminal organisations.

### *2.2. Lex ferenda*[397]

Financial institutions have realised that innovative payment technologies are changing the business landscape as clients, empowered by web access and e-money

---

391 White and Duram *America Goes Green: An Encyclopaedia of Eco-Friendly Culture in the United States* 389.

392 Carse 1999 http://bis.org/review/r991012c.pdf and Mann 2004 TLR 704.

393 Mann 2004 *TLR* 703 – 704.

394 White and Duram *America Goes Green: An Encyclopaedia of Eco-Friendly Culture in the United States* 389.

395 Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/.

396 Carse 1999 http://bis.org/review/r991012c.pdf.

397 Derived from the expression *de lege ferenda* that means "with a view of the future law".

functionality, are fast becoming more proactive and independent.[398] Consequently financial institutions are faced by the prospect of shrivelling traditional revenue streams as m-money provides faster, cheaper and easier access to participate in the financial market.[399] Stemming from the above, some central banks have applied a different focus to the regulation of innovative payment systems. As the name suggests, the forward-thinking approach requires regulatory and supervisory authorities to be forward thinking based on the available information at hand.[400] The forward-thinking approach requires regulatory authorities to anticipate any challenges that would result in adverse outcomes prior to the introduction of new payment systems.[401]

In its National Innovation Systems Project, the Organisation for Economic Co-operation and Development (OECD) highlighted the need for governments to change their objectives and policies to include greater focus on innovative payment systems.[402] The OECD accepts that e-money should be regulated within the ambit of banking supervision and regulation, taking cognisance of academic debates on whether the regulation of e-money should fall under the function of banking or non-banking institutions.[403] This approach results in an uneven business playing field as different regulatory models may be adapted to the regulation of e-money. The World Bank's Financial Sector Working Paper[404] focusing on AML identifies four different models applicable to e-payments, namely:

a. Merchant issuer model (also known as the operator-centric model[405]): In this model, traditional banking is not a party to the issuing of electronic payment and here the issuer of e-payment (e.g. stored-value smart cards) and the

398 Mboweni 1999 http:// bis.org/review/r991013b.pdf.
399 Chiu and Wong 2014 http://bostonfed.org/payments2014/papers/Chiu_Wong.pdf.
400 Feinson unknown http:// aau.org/sites/default/files/urg/docs/nis_overview_country-%20cases.pdf.
401 Working Group of the European Payment Systems 1994 http://ecb.europa.eu/pub/pdf/other/prepaidcards1994en.pdf?9fc7b56c72b0b1a42eb60ab5f97fb7d3.
402 OECD 1994 http:// oecd.org/pdf/M000014000/M00014640.pdf.
403 Mann 2004 *TLR* 704.
404 Kellermann 2006 http:// wds.workdbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_2006042114035/Rendered/PDF/359050rev0Mone1nCyberspace01.
405 Chaix and Torre 2011 http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf.

retailer are the same person[406] (e.g. gift cards from shopping centres). Funds are thus stored in a prepaid account maintained by the retailer[407];

b. Bank-issuer model (also known as the bank-centric model[408]): In this model the bank and retailer are separate entities and the operator effects payment using e-money. The transaction is cleared via normal financial systems[409] (e.g. Safaricom, Kenya's largest cellarer phone provider, used the M-pesa mobile payment product to deposit money into a virtual wallet account, to send money via the use of a mobile phone[410])[411];

c. Non-bank model (gatekeeper's strategy): In this model m-money products are sourced from a technology company. The retailer introduces the product either via a bank or to the client directly. The bank's primary function is to oversee entrance of e-money products into the market[412] (e.g. The South African Bank of Athens' Wizzit m-banking product, uses a transactional bank account via secure m-banking technologies[413]); and

d. Peer-to-peer model: This model is designed to be decentralised.[414] It uses cryptography[415] and the transfer of funds, which do not have the attributes of real currency (i.e. regarded as legal tender), could take place without the involvement of the bank (e.g. Bitcoin, a form of virtual currency[416]).[417]

---

406 Kellermann 2006 http://wds.workdbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_2006042114035/Rendered/PDF/359050rev0Mone1nCyberspace01.

407 Kersop and du Toit 2015 *Potchefstroomse Electroniese Regsblad* 1615.

408 Chaix and Torre 2011 http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf.

409 Kellermann 2006 http://wds.workdbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_2006042114035/Rendered/PDF/359050rev0Mone1nCyberspace01.

410 Vodacom unknown date http:// vodacom.co.za/vodacom/services/financial-solutions/m-pesa.

411 Mbiti and Weil 2001 http://nber.org/papers/w17129.pdf.

412 Kellermann 2006 http://wds.workdbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_2006042114035/Rendered/PDF/359050rev0Mone1nCyberspace01.

413 Lawack-Davids 2012 *JICLT* 320.

414 "Decentralised" means that there is no central entity in charge of issuing the currency and processing transactions.

415 Stokes 2012 *Information and Communications Technology Law 224* – 227.

416 Virtual currency: The European Central Bank (ECB) defines v-currency as "a type of unregulated, digital money, which is issued and usually controlled by its developer, and used and accepted among the members of a specific virtual community." European Central Bank 2012 http://ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

Diagram 1 illustrates the four different models applicable to e-payments and the interactive partnership between clients, retails, merchants and/or banks:[418]

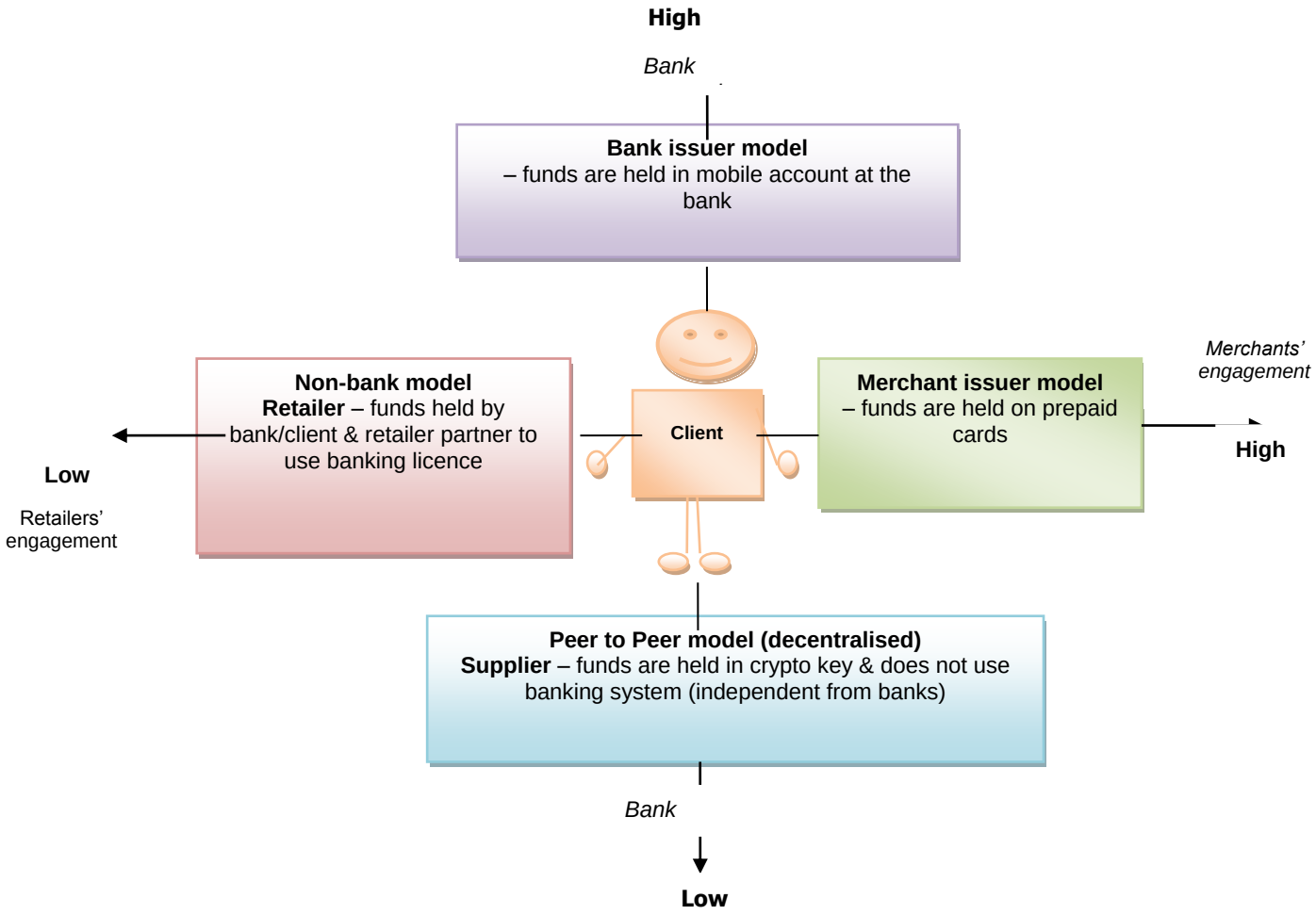



**Diagram 1: Engagement of parties involved in different models applicable to e-payments**[419]

Innovation is driven by achieving cost efficiency and regulatory arbitrage.[420] In this regard, White[421] believes that financial regulation is used as a "public interest" tool to

---

417 Kellermann 2006 http://wds.workdbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_2006042114035/Rendered/PDF/359050rev0Mone1nCyberspace01 and Chaix and Torre 2011 http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf.

418 Chaix and Torre 2011 http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf.

419 Chaix and Torre 2011 http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf.

420 White 1997 *Technological Change, Financial Innovation and Financial Regulation: The Challenges for Public Policy* in the USA 97 and Huang *The Law and Regulation of Central Counterparties* 129-130.

correct the imbalances of the market (e.g. monopoly or oligopoly). As long as financial regulation shapes innovation and innovation poses challenges for financial regulation, governments will have to find some equilibrium between these apparent opposing variables.

## 3 Financial Action Task Force

We live in the age of globalisation. It is characterised by the rapid mobility of funds through the introduction of faster payment systems, where basic, legal transactions such as the transfer of funds, via m-banking, can be used to transform illicit money into the appearance of legitimate funds.[422] This monetary system, which is easily manipulated by money launderers and terrorist financiers, involves a number of stakeholders such as the service providers, sellers, buyers and even regulators. The question that needs to be answered is whether businesses really know who their clients are? It is thus not surprising that the fight against ML and the TF calls for global interaction and a coordinated approach.

At the forefront of setting international standards in combating ML and TF is FATF.[423] It is an inter-governmental body established during the G-7 summit under the OECD[424] in 1989 and is tasked to give impetus to measures against ML and TF. Since then it has taken up additional responsibilities and focuses now on developing and promoting policies, both nationally and internationally, which *inter alia* include the eradication of ML and TF, monitoring the implementation of measures by member

---

421 White 1997 *Technological Change, Financial Innovation and Financial Regulation: The Challenges for Public Policy* in the USA 97.

422 *USA v Liberty Reserve S.A. and 7 others* [2013] CRIM 368 (United States District Court, Southern District of New York); Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf – case study of a suspicious activity report filed in the United States, which detailed a case where a single individual had managed to use over 300 prepaid cards to transfer approximately USD 2 million to Colombia; *Uganda v Sserunkuma and 8 others* [2015] UGHCACD 5 (High Court of Uganda Holden, case no. HCT-00-CR.SC 15/2013). Also see Morawczvnski 2015 http://cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion and Chaix and Torre 2011 http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf.

423 FATF is an inter-governmental body consisting of 36 members, which engages in the development and promotion of national and international policies and standards to combat money laundering and terrorist financing and De Koker 2013 *Washington Journal of Law, Technology and Arts* 167-169.

424 -The OECD houses the Financial Action Task Force secretariat and is situated in Paris. OECD unknown date http://oecd.org/about/.

states and reviewing ML and TF techniques.[425] As a policy-making body, FATF forms the central point for integrating legal, financial and law enforcement specialists to realise national legislation and regulatory AML/CFT reform.[426] South Africa became the 31st member of FATF during 2003 and as such committed itself to the global efforts of combating organised crime, by employing and complying with the international anti-money laundering and counter-terrorism financing standards of FATF.[427]

FATF implemented the Forty Recommendations and Nine Special Recommendations on TF in 1990 and revised them again in 1996 and 2001, before publishing the latest revised Forty and IX Recommendations in 2012.[428] Although not binding, these recommendations exhibit the flexibility, speed and effectiveness of soft law in setting international standards and requiring action to be taken against ML and TF.[429] The Forty Recommendations provide guidance on the adoption of preventative measures to mitigate ML and TF activities.[430] They have also been recognised by the International Monetary Fund and the World Bank as setting international standards to eradicate ML and TF. The FATF Recommendations, together with the Wolfsberg Group of International Financial Institutions' (hereinafter the Wolfsberg Group) various sets of AML Principles,[431] and Basel's Core Principles for Effective Banking Supervision (29 Core Principles)[432] provide international guidance of the minimum requirements to be followed by the commercial and economic sectors. Basel's Core Principles for Effective Banking Supervision highlighted the prudential method of

---

425 De Koker *South African Money Laundering and Terror Financing Law* 9-10; and Rachagan and Kasipillian 2013 *International company and Commercial Law Review* 278.

426 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III-8.

427 Financial Action Task Force unknown date http:// atf-gafi.org/countries/.

428 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

429 Delston and Walls 2009 *Case W. Res J.INT'L L.* 92 - 94.

430 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

431 Wolfsberg Group unknown date http://wolfsberg-principles.com/standards.html - Wolfsberg Guidance on the Risk-based approach for Managing Money Laundering Risks, Wolfsberg Trade Finance Principle, Wolfsberg Private Banking Principle, Wolfsberg Correspondent Banking Principles etc.

432 Bank for International Settlements 2012 http://bis.org/publ/bcbs230.pdf - Basel Committee Principle 29 which requires client due diligence to be applied.

"KYC" as an effective risk management tool.[433] The application of the above international principles is viewed as fundamental to the market integrity and financial stability of any country.

AML and CFT continue to be a key issue in many businesses and, depending on the emerging counter-measures applied by each country, ML and TF methods and techniques vary. It would appear from the analyses of the Forty Recommendations[434] that FATF applies a three-layers-of-defence approach to AML and CFT. The first layer, which is a key element in setting the foundation for eradicating and uncovering ML and TF is contained in FATF Recommendations 9 and 10, read with Recommendations 3 (criminalisation ML offences)[435] and 5 (criminalisation TF offences). In terms of Recommendations 3 and 5 and in line with the Vienna Convention[436], the Palermo Convention[437] and the Terrorist Financing Convention,[438]

---

433 Saksenberg *FICA Training Manual* 242.

434 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

435 United Nations Treaty Collection unknown date https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en – United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substance and International Peace Institute 2010 https://ciaonet.org/attachments/17631/uploads - Also known as the "United Nations Convention on Transnational Organised Crime" was established with its main aim to fight organised crime. Expanding the global fight on organised crime, the United Nations adopted *The International Convention Against Organised Crime 2000 (Palermo Convention)*, which is a United Nations treaty published and signed in 1999.

436 United Nations Treaty Collection unknown date https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en – United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substance, Vienna 20 December 1988. The United Nations noted a huge increase in international drug trafficking and the link to money laundering activities entering the banking system and via the United Nations Drug Control Program initiated an global focus on combating drug trafficking and money laundering. The 1988 Vienna Convention supported the enactment of legal provisions which would enable law enforcement to confiscate the proceeds of crime. Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III-2.

437 International Peace Institute 2010 https://ciaonet.org/attachments/17631/uploads - Also known as the "United Nations Convention on Transnational Organised Crime" was established with its main aim to fight organised crime. Expanding the global fight on organised crime, the United Nations adopted *The International Convention Against Organised Crime 2000 (Palermo Convention)*, which is a United Nations treaty published and signed in 1999, in which participating countries undertook to criminalise the financing of terrorism. Articles 6 and 7 of the Palermo Convention specifically obligates member countries to criminalise money laundering and to establish regulatory regimes to deter and detect all forms of money laundering which would include client identification, record keeping and transaction monitoring for unusual transactions. Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III-3.

which are regarded as issuers of the most influential instruments and most pertinent international fora, countries are required to criminalise ML, TF, terrorist organisations and individual acts of terrorism.[439] FATF Recommendations 9 and 10 highlight the need to have access to AML/CFT and KYC information as a tool to mitigate risks. As such these Recommendations[440] *inter alia* state that financial institutions[441] should be required to implement CDD measures (i.e. identifying and verifying the identity of the client) when establishing a business relationship, effecting a single transaction and/or noting a suspicious ML/TF transaction. It is also recommended that financial institutions do not keep anonymous accounts or accounts in fictitious names.[442] Accordingly, FATF recommended that CDD should necessitate the taking of the following steps:

1. identify and verify the client's identity by using an independent source document;

2. in the case of identifying a beneficial owner, reasonable steps have to be taken to ensure that the identity of the beneficial owner is known;

3. obtain information relating to the purpose and nature of the business relationship; and

---

438 United Nations 1999 https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf. Prior to the 1 September 2001 attacks the United Nations raised concerns over the financing of terrorism and in response thereto adopted the *International Convention for the Suppression of the Financing of Terrorism (1999)*. This convention obligates member countries to criminalise terrorism, terrorist organisations and terrorist acts which would make it illegal for any person to provide or collect funds with the intent for the funds to be used for or have knowledge of the use of funds to carry out any acts of terrorism. Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III-4.

439 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdfand De Koker *South African Money Laundering and Terror Financing Law* 554 - 556.

440 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

441 In terms of the Financial Action Task Force's Recommendations financial institutions can be defined as "any person or entity who conducts as a business one or more of the following activities or operation for or on behalf of a client: lending, financial leasing, transfer of money or value; accepting deposits and other repayable fund from the public; financial guarantees and commitments; trading in foreign exchange; money market instruments etc."

442 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

4. doing continuous due diligence on the business relationship and/or type of transaction, irrespective of the value to ensure that the institution's knowledge of its clients is aligned with its client and risk profile.[443]

FATF Recommendation 10 recognised that although it is not required that all the above CDD measures be implemented, it does place an obligation on financial institutions to verify the identity of its client and/or the beneficial owner before or during the establishment of the business relationship or conclusion of the transaction.[444] The application of CDD policies and procedures should, however, be applied to both new and existing clients. FATF further cautions that EDD measures need to be taken in the case of high-risk categories of clients (i.e. politically exposed persons),[445] non-face-to-face business relationships[446] or complex and unusual transactions (i.e. m-banking).[447] In cases where financial institutions are unable to identify and verify its client and/or the beneficial owner or the nature of the transaction, it is recommended that no account can be opened, transaction effected or business relationship established.[448] It is recommended that in these cases the business relationship be terminated and a suspicious transaction report be filed[449], which would form the basis for second layer of AML and CFT process.

FATF Recommendations 12 to 22 support Recommendation 10 in that they give further KYC guidance, stating that special attention is to be given to *inter alia* new

---

443 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

444 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

445 Financial Action Task Force Recommendation 12 - Financial Action Task Force FATF 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

446 Financial Action Task Force Recommendation 15 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

447 Financial Action Task Force Recommendations 10 and 15 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf

448 Financial Action Task Force Recommendations 9 and 10 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

449 Financial Action Task Force Recommendation 20 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

technologies that favour anonymity or complex transactions (Recommendations 14 and 15), intermediaries or third party performance (Recommendation 17) and non-financial businesses duty to do CDD (Recommendation 22). Another supporting but essential recommendation, which essentially sets the tone for the third layer of AML/CFT defence, can be found in FATF Recommendation 18. This recommendation requires financial institutions to formulate and implement internal controls that provide for documented step-by-step working methods focused on *inter alia* CDD, any reporting obligations[450], RBA[451], EDD, tipping off and confidentiality[452], to name but a few.

### *3.1 FATF's analysis of new payment methods*

Stemming from the above FATF published a report in October 2006 titled "New Payment Methods"[453], in which it acknowledges that new innovative payment methods for electronic cross-border transfers are gaining global popularity and can be a powerful tool to further financial inclusion. As technology is developing at a much faster pace than legislative adoption and monitoring could, FATF raised concern over the fact that the analysis of these products and services revealed a certain level of vulnerability, which could be exploited by criminals for ML and TF purposes.[454] Anonymity, global access to cash via m-money and wider availability of funds are just some of the factors that attract criminals to the use of new payment technologies.[455] De Koker believes that this is an indication that criminals are evolving and refining their financial crimes techniques to exploit the gaps in the new payment

---

450 Financial Action Task Force Recommendation 20 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

451 Financial Action Task Force Recommendation 1.

452 Financial Action Task Force Recommendation 21.

453 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf – the FATF project team analysed 33 case studies which focused on pre-paid cards, mobile banking transactions and internet payment systems.

454 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

455 Chatain *et al* 2008 http://siteresources.worldbank.org/INTAML/Resources/WP146_web.pdg and Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

technologies and the criminal proceeds thereof.[456] According to him, AML/CFT measures are rather aimed at deterrence than prevention.[457]

The FATF team found that many jurisdictions applied a range of different threshold or caps for new payment products and services (i.e. m-banking) to justify its categorisation of such products and services as low risk.[458] Notwithstanding the above, the FATF team was unable to find across jurisdictions uniform criteria that would confirm the categorisation of a product or service as low risk.[459] In cases of pre-defined ML/TF low-risk scenarios, some countries allowed for the application of a simplified CDD (e.g. only view client identification as opposed to obtaining identification and address information)[460] in an attempt to allow access to banking services despite a lack of formal identification documents.[461]

FATF's analyses of the developments in the telecommunications and banking system highlighted the fusion between payment methods and communication, which resulted in the following types of mobile payment products:[462]

1. Open-loop mobile pre-paid cards: These cards are connected to an account that allows clients access to the global ATM network via the handover of the prepaid card (e.g. Bidvest's world travel card).

2. Non-card ATM withdrawals: The transaction is linked to a unique code that allows for peer-to-peer transfer to a third party by passing the code to him/her, who would in return enter the code at an ATM to release the money transferred.

---

456 De Koker 2004 *TSAR* 715-741.

457 De Koker 2004 *TSAR* 715-741.

458 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

459 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

460 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

461 De Koker 2013 *Washington Journal of Law, Technology and Arts* 170.

462 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

3. Cooperation with third-party providers: This is where the client utilises traditional money remittance services (e.g. Western Union) to enable a third party who is not a client of the mobile payment service provider to send or receive money.[463]

Stemming from the above, the FATF team identified the following AML/CFT gaps:[464]

1. Situations where new payment products and services were provided by third parties that falls outside the AML/CFT regulatory and supervisory framework (e.g. the withdrawal of funds from retailers such as Checkers who do not fall under banking or telecommunications legislation). In the case of prepaid or SIM[465]- card, the FATF team found these products can be designed to allow for absolute anonymity and at the same time provide a high degree of functionality. For instance, there has recently been an increase in SIM swap fraud cases being reported where scammers are able to cancel the old and re-activate new SIM cards to hack into bank account.[466]

2. The establishment of non-face-to-face business without adequate application of AML/CFT controls, which is in accordance with FATF Recommendation 15 linked to "special risks".[467] This would consequently preclude the use of simplified CDD and calls for an enhanced approach to be applied to CDD.[468]

The FATF team realised that although the current FATF Recommendations proved a broadly adequate framework for addressing most ML/TF vulnerabilities linked to new

---

[463] Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

[464] Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

[465] SIM refers to a subscriber identification module.

[466] Murgia Telegraph 1, available on The Daily Telegraph's website 2016 http://telegraph.co.uk/technology/internet-security/11896024/How-to-protect-yourself-from-SIM-swap-scams.html. It has been reported that some clients in South African banks have lost approximately R650 000 (approximately €30 000) in SIM-swap fraud cases.

[467] Specific risk also refers to High risk - Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf .

[468] Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf

innovative payment products and services, the reality is that these products and services continue to evolve at a much faster rate than legislative controls. It follows therefore that more reliance should be placed on the use of appropriate, flexible and forward-thinking approaches (i.e. *lex ferenda*) to a FATF methodologies.

### *3.2 Risk-based approach*

Global improvements in terms of the functionality and use of new innovative payment products and services necessitate participating stakeholders to be more vigilant to possible exploitation thereof for ML/TF purposes.[469] In the absence of appropriate AML/CFT controls, the risks associated with new innovative payment methods such as mobile payments are high.[470] FATF conceded in its guidance document of 2013[471] that AML/CFT controls should not impede access to financial services as financial exclusions would destabilise the effectiveness of AML/CFT methodology.

Due to increased interconnectivity between payment services, MNOs are partnering with electronic transfer networks to increase their market capacity with regard to mobile payments. As such, m-banking is regarded as distinct from bank-centric mobile payment models as financial institutions that facilitate mobile payments can be traditional banks or non-bank payment service providers (also known as money or value transfer services).[472] It follows that mobile payments can either facilitate transactions on a person-to-business (P2B), person-to-person (P2P) or government to person (G2P) basis.[473] This allows different types of service providers to participate or even establish partnerships, depending on the available technology and business

---

469 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

470 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf.

471 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

472 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

473 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

model.[474] The two main m-banking models are the bank-centric and mobile network operator-centric mobile payment models. In a bank-centric mobile payment model, account holders with the bank are provided with a m-banking service, which differs from traditional banking service. As such, the financial institution can act as the provider of e-money that is not linked to an account or as a bank that offers a new payment service via the use of a mobile phone to the unbanked, subject to a threshold limit.[475] In partnering with software developers and payment processors clients can access funds via their mobile phones with the receipt of payment messages. The mobile network operator does not have access to the client's funds and only provides the telecommunication network platform for the transfer of payment messages.[476] As a means to add value to its core communication services, the funds of mobile network operator-centric mobile payment model clients are stored in a prepaid account, held by the MNOs that provide mobile payment services. It has been noted that depending on the governing legislation, MNOs would partner with a bank as it authorises dealing licences.[477]

From the analysis of the FATF Recommendations, it may be noted that there is no globally accepted definition of risk. This could be attributed to the ubiquity of risk in almost all aspects of human activities.[478] The International Organization for Standardization 3100 standard (2009), however, defined risk as the "effect of uncertainty of objectives".[479] Whilst the 2003 FATF recommendations provided for the implementation of a RBA in some areas, the 2012 revised FATF recommendations view the application of the RBA to an AML/CFT framework as essential. To mitigate ML/TF risks in accordance with 2012 FATF Recommendation 1, FATF endorses a holistic view of and approach to all risk factors, which would assist in assessing the

---

474 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

475 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

476 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

477 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

478 Ahumud unknown date http://www.academia.edu/5321031/Literature_Review_Risk_Based_Approach_to_AML_and_CTF.

479 De Koker 2013 *Washington Journal of Law, Technology and Arts* 182-183 and International Organization for Standardization (ISO) 2009 http://iso.org/iso/iso31000

risk linked to a specific new payment method.[480] Thus the foundation of a RBA is dependent on risk assessment and appropriate understanding of the relevant risks.[481] Countries are not only expected to identify ML/TF risks, but also to assess and understand the risks in order to apply risk mitigation measures that are commensurate with the identified risks.[482] The application of an effective RBA would place a financial institution in a position to understand how and to what extent it is vulnerable to ML/TF. FATF's Recommendation 1 is also supported the Basel's Core Principles 6 and 15, which state that sound risk management can only be effective once banks have identified and analysed the ML/TF risks to design and implement documented policies and procedures that are commensurate with the identified risks.[483] Higher identified ML/TF risks require the adoption of an enhanced risk mitigation approach.[484] FATF recommended in its 2006 and 2016 reports that the following factors need to be assessed and understood before ML/TF could be mitigated:[485]

1. Identification and verification measures: This control enables a financial institution to identify and understand who their clients and beneficial owners are, and whether a client is linked to multiple accounts. In the absence of face-to-face contact, a high risk rating should be applied, which would accordingly call for an enhanced approach or more rigorous controls to be applied (e.g. using third-party source verification).

2. Monitoring and reporting: Relying on computer technology, new payment methods leave an electronic footprint which provides an ideal platform for effective monitoring, analyses and reporting of unusual transactions (e.g. an

---

480 Financial Action Task Force Recommendation 15 (assess risk of new payment system prior to implementation) - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

481 De Koker 2013 *Washington Journal of Law, Technology and Arts* 173 - 174.

482 De Koker 2013 *Washington Journal of Law, Technology and Arts* 173.

483 Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf.

484 De Koker 2013 *Washington Journal of Law, Technology and Arts* 174.

485 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf and Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

account used by multiple users) or terrorist property reporting transactions (e.g. through the use of sanctions screening list).

3. Threshold limits: The restriction in frequency and value limits of transactions is used to deter criminals from accessing on a continuous basis large amounts of money. In most cases new payment products and services are subject to a RBA approach that often allows for a simplified CDD to be applied. The value and transaction threshold tool is accordingly believed to provide an extra layer of AML/CFT protection without placing an undue duty on the clients. Most jurisdictions are therefore of the opinion that the threshold tool renders these products less attractive for criminals.

4. Anonymous funding: this can be mitigated by limiting funding methods that are not linked to personalised payment methods.[486]

The degree of AML/CFT risks specific to m-money is dependent on the controls applied to the cumulative effect of combining all the following risk factors:[487]

1. Non-face-to-face relationships and anonymity: The technical advances in m-banking facilitate non-face-to-face interactions, often inadvertently promoting anonymous interactions which criminals could abuse through identity theft.[488] Thus the absence of face-to-face interaction would indicate greater ML and TF risks, in turn necessitating an enhanced approach (i.e. transaction monitoring) to be applied as mitigant.[489]

2. Geographical reach: The extent to which a particular innovative payment method is universally accepted, the implementation of domestic legislative controls and different forms of usage will impact ML/TF risk allocation.[490] For instance, in m-banking linked to open-loop prepaid cards, clients can effect

---

[486] Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

[487] Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

[488] De Koker 2013 *Washington Journal of Law, Technology and Arts* 169 – 170.

[489] Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

[490] Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

payments on a domestic and international level, which would evidently be very attractive for criminals.[491]

3. Techniques of funding: Anonymity of source of funds would escalate the ML/TF risk level and the funders of new innovative payment methods service providers would not be in the position to verify the identity of a client. In m-banking the receiver of the funds only needs to enter the unique SMS code at an ATM to receive funds without any form of verification or undergoing a CDD process, which make this an ideal tool for TF.[492]

4. Accessibility to cash: The ease with which funds may be accessed via ATM networks increases the ML and TF risks.

5. Segmentations of services: It has been noted that new innovative payment products and services can comprise a complex infrastructure, involving different stakeholders at various levels. Oversight over the application of AML/CFT controls by the different stakeholders can become inadequate as not all stakeholders are subject to international and/or legislative AML/CFT standards.[493] Furthermore, the level of information collection (i.e. CDD) differs and in most instances the sharing of information is prohibited.[494]

From the above it is clear that a prerequisite for the implementation of a sound RBA and effective ML and TF risk management is the accurate mapping of ML/TF risks.[495] The concept of implementing a RBA is simple. Identify, assess and understand the ML/TF risks that financial institutions are exposed to and allocate the limited resources (e.g. human and/or systems) in proportion to the identified ML/TF risks. The application thereof can become technical once the framework is supported by a risk matrix and weightings. It follows therefore that the ML/TF risk assessment

---

491 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

492 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

493 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

494 *Protection of Personal Information Act* 4 of 2013.

495 Chatain *et al Protecting Mobile Money against Financial Crime* xxxii.

should be informed by an understanding of the client's profile and the pertinent risks associated with that client.

### *3.3 The proportionality principle*

By understanding the ML/TF vulnerabilities and barriers within the existing regulatory framework, the application of the proportionality principle provides the exact balance between risks and benefits.[496] This principle, supported by the G20 Principles for Innovative Financial Inclusion,[497] promotes the tailoring of policies and regulatory frameworks in proportion to the risks and benefits associated with new innovative products and services, without imposing unwarranted regulatory obligations which could hamper innovation.[498] In line with the proportionality principle, the interpretive note linked to FATF Recommendation 1 confirms that subject to a proven low risk of ML and TF, countries have the discretion to not apply some of the FATF Recommendations that obligate financial institutions to take AML/CFT mitigating steps.[499] However, FATF has noted that small, low-value transactions such as the transactions that fall in the ambit of m-banking are particularly susceptible to TF risks.[500] In this regard, countries are encouraged to apply a RBA, which would justify the applications of, for instance, a simplified CDD to certain assessed low-risk products and services. The aim of applying a proportionate regulatory approach is to open the market to innovation which will encourage participation by the un- and under-banked.[501]

---

496 G20 Global Partnership for Financial Inclusions 2010 http://gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf.

497 Principle 8 of Proportionality Principles – G20 Global Partnership for Financial Inclusions 2010 http://gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf.

498 G20 Global Partnership for Financial Inclusions 2010 http://gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf.

499 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

500 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf and De Koker 2013 Washington Journal of Law, Technologies and Arts 184-185.

501 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

New innovative payment products and services such as m-money provide both the promise of development and the potential for its vulnerabilities to be abused by criminals. The G20 Principles for Innovative Financial Inclusion confirm that the need for innovative payment systems should be proportionate to the risks identified.[502]

## 4 Bank for International Settlements: Basel Committee on Effective Banking Supervision

Established in 1974,[503] Basel is regarded as the international standard-setting institution for the prudential regulation of banks and provides the platform for cooperating on banking supervisory issues.[504] Although it has no formal international supervisory or legal authority, Basel aims to enhance financial stability by providing guidance to strengthen regulation, supervision and banking practices on a global scale.[505] In line with Basel's mandate, it endorses the adoption and implementation of the FATF Recommendations[506] and three of its supervisory standards and guidance notes focus on ML issues.[507] Analysis of the supervisory standards and guidance provided by Basel reveals that both FATF standards and the Basel's Core Principles for Effective Banking Supervision across domestic and international banking supervision are incorporated therein.[508] Being risk averse, Basel embarks each year on a financial stability risk awareness programme, reviewing and updating previous guidance provided. The overall soundness and safety of banks and international financial systems are entrenched in the applications of sound ML/TF risk management.[509]

---

502 Centre for Global Development 2016 http://cgdev.org/sites/default/files/CGD-Policy-Paper-Gelb-KYC-Financial-Inclusion.pdf.

503 By the central bank governors of the Group of 10 countries - Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III-13 - III-14.

504 Bank for International Settlements 2015 http://bis.org/bcbs/about.htm.

505 Bank for International Settlements 2015 http://bis.org/bcbs/about.htm.

506 Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf.

507 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism III-13.*

508 Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf.

509 Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf and Bank for International Settlements 2012 http://bis.org/publ/bcbs213.pdf - Basel Core Principle 15 of the Core Principles of Effective Banking Supervision.

During January 2001 and in line with the Core Principles for Effective Banking Supervision,[510] Basel issued a comprehensive document focusing on the application of effective policies and stricter CDD measures for both new and existing clients as the core pillar of banking control policies.[511] The application of KYC controls serves a dual role, and relates to the application of both AML/CFT measures and prudential controls relating to banking regulation. The absence KYC measures can result in reputational, operational, legal and systemic risks as banks could unknowingly facilitate or participate in ML or TF activities.[512]

The Basel Committee's *Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering*[513], issued in 1988, outlines four principles of defence, which may be summarised as follows: [514]

1. banks are required to take reasonable steps to identify their clients;
2. banks should ensure that financial transactions are not associated with ML activities;
3. banks should cooperate fully with law enforcement (e.g. freezing an account) while maintaining due regard for client confidentiality; and
4. banks should adopt and implement step-by-step policies and procedures in line with the guidance and standards provided.

In mitigating ML/TF risks, Basel on a regular basis reviews and updates the CDD and KYC standards.[515] For instance, during February 2016 Basel published its paper titled

---

510 Bank for International Settlements 2012 http://bis.org/publ/bcbs213.pdf – Basel Core Principle 29 of the Core Principles of Effective Banking Supervision. The Core Principles for Effective Banking Supervision provide banks with a comprehensive guideline on an effective bank supervisory system. The Core Principles also deal with other topics such as KYC policies and procedures, which are regarded as crucial for an effective AML/CFT institutional framework. Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism III-15.*

511 Jun and Ai 2009 *Journal of Money Laundering Control* 407–408 and Bank for International Settlements 2012 http://bis.org/publ/bcbs213.pdf - Basel Core Principle 29 of the Core Principles of Effective Banking Supervision.

512 Jun and Ai 2009 *Journal of Money Laundering Control* 407-408.

513 Bank for International Settlements 1988 http://bis.org/pub/bcbsc137.pdf.

514 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism III-14.*

"Sound Management of Risks Related to ML and TF", in which it provided new guidance to manage ML/TF risk within the context of overall risk management. Particular attention was focused on the application of CDD at account opening.[516] These standards, and in line with the management of ML/TF risks, require banks to implement effective practices and procedures for KYC rules, including client acceptance, identification, monitoring and risk management policies.[517] Notwithstanding the promotion of the implementation of 2012 FATF Recommendation 1 (i.e. adoption and implementation of a risk-based approach), and from the analysis of these standards on account opening, the guidance provided appears to be very rules-based and -driven.[518] For instance, banks are *inter alia* still required to obtain a client's' identification documentation and financial transaction records or business correspondence.

Basel believes that ML/TF risk management consist of three lines of defence. Accordingly, business units are regarded as the first line of defence in identifying, assessing and controlling ML/TF risks, whereafter the second line of defence focuses on the function of the AML/CFT compliance officer, who essentially controls the compliance function and resources allocated thereto.[519] The last line of defence resides under the internal audit function, which independently evaluates risk management and controls implemented.[520]

Stemming from the above, it is clear that the guidance provided by the Basel not only supports the principles of the FATF Recommendations in combating ML/TF, but also plays a supportive role to ensure sound financial stability and to strengthen the effectiveness of financial regulation and supervision.

---

515 The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering issued 1988; the Core Principles for Effective Banking Supervision (i.e. implantation of sticker KYC rules) issued 1997; the Core Principles Methodology (i.e. CDD) issued in 1999.

516 Bank for International Settlements 2016 http://.bis.org/bcbs/publ/d353.pdf.

517 Bank for International Settlements 2016 http://.bis.org/bcbs/publ/d353.pdf.

518 Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf.

519 Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf.

520 Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf.

## 5 The Wolfsberg Group

The Wolfsberg Group is an international institution that issues self-regulatory principles focused on ML/TF, private banking and correspondent banking, to name but a few.[521] It comprises 13 global banks[522] focused on developing regulatory frameworks and guidance for financial crime risk management, KYC, AML and CTF policies.[523] The Wolfsberg Group's principles reflect the group's view on the appropriate AML/CFT controls to be implemented when dealing with high-risk individuals (e.g. politically exposed persons), entities (e.g. correspondent banking) or products (e.g. new innovative payment methods).[524] Over the years the Wolfsberg Group has managed to develop approximately 11 principles which *inter alia* include client acceptance; updating of client files; monitoring, control responsibilities, reporting, training, record retention, AML and new payment systems.[525] Principle 7 of the Wolfsberg Group's Suppression of the Financing of Terrorism[526] emphasizes the need for global cooperation by financial institutions to combat the financing of terrorism via the implementation of methods relating to prevention, detection, sanctions screening and sharing of information methods. This principle of the Wolfsberg Group relates to and endorses FATF Recommendation 5.[527]

The growing demand in the marketplace to migrate to electronic payments can broaden the payment methods and cause greater complexity in the AML/CTF sphere. In support of FATF's 2006 and 2010 *New Payment Methods Report;*[528] the Wolfsberg

---

521 Wolfsberg Group 2015 http://wolfsberg-principles.com/.

522 Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank, UBS.

523 Wolfsberg Group 2015 http:/wolfsberg-principles.com/.

524 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* IV4.

525 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* IV5.

526 Wolfsberg Group 2002 http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_(2002).pdf.

527 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* IV5.

528 Financial Action Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf and Financial Action Task Force 2010 http://fatf-

Group published a guidance document on prepaid and value stored cards in 2011.[529] The guidance document considers the ML vulnerabilities of physical prepaid and stored-value cards, and provides guidance on the mitigation of ML/TF risks.[530] It is noted that prepaid cards are convenient, easy to use, have no restriction on the nature of use, can be used on a non-face-to-face basis and involve a number of role players. All these features make this product very attractive to criminals in facilitating ML/TF.[531] Stemming from this analysis the Wolfsberg Group recommended that prepaid cards be designed in such a manner to limit the nature, place of use, reloading ability and/or the setting of a threshold limit.[532] This is believed to slow the speed at which criminals try to abuse new innovative payment products and services, and assist the financial industry to play catch-up in plugging ML/TF vulnerabilities.

## 6 Twin Peaks model of financial regulation

The 2008 international financial crisis[533] revealed the need for the implementation of minimum international standards and greater cooperation between national regulators.[534] Being internationally integrated, financial sectors were still regulated on a domestic level at the time, which was accordingly identified as a weakness.

---

gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html.

529 Wolfsberg Group 2011 http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf.

530 Wolfsberg Group 2011 http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf.

531 Wolfsberg Group 2011 http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf.

532 Wolfsberg Group 2011 http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf.

533 Financial Services Board 2013 https://fsb.co.za/Departments/twinpeaks/Documents/Twin%20Peaks%2001%20Feb%202013%20Final.pdf – The global crisis demonstrated the weakness of a light-touch financial regulatory system.

534 Financial Services Board 2013 https://fsb.co.za/Departments/twinpeaks/Documents/Twin%20Peaks%2001%20Feb%202013%20Final.pdf.

In line with enhanced international financial regulatory developments and financial stability improvements, the Minister of Finance[535] announced during the 2011 Budget Speech that South Africa would make the architectural move to a 'Twin Peaks' model of financial regulation. In terms of the proposed reforms to the financial services sector, the options were for the financial regulatory and supervisory sector to consist of either an integrated,[536] Twin Peaks,[537] functional/fragmented[538] or institutional[539] approach.[540] Following two policy papers[541] which highlighted the lessons learned from the 2008 international financial crisis, it was decided that the regulations governing South Africa's financial sector would shift from a fragmented model to a Twin Peaks model.[542] This would minimise regulatory arbitrage and streamline the various licensing, supervisory, enforcement and client protection processes.[543]

The Twin Peaks model of financial regulation will be legislatively effected through the promulgation of the *Financial Sector Regulation Bill* and will cause the creation of a distinct prudential and a market conduct regulator. The to-be established Prudential Authority will be housed in the SARB, while the to-be established

---

535 National Treasury 2011 http://gov.za/2011-budget-speech-minister-finance-pravin-gordhan.

536 Integrated approach = Refers to a single, universal supervisory approach, where one supervisor has to oversee the safety, soundness and business conduct regulation of all sectors of the financial market. Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

537 Twin Peaks approach refers to a separation of the regulatory functions between two or more supervisors, with one for instance regulating the safety and soundness of the market, whilst the other would regulate market conduct. Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

538 Functional/fragmented approach refers to where a business determines the supervisory oversight that is being transacted by financial institutions without regard to legal status, resulting in a separation of supervisory oversight link to each business. Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

539 Institutional approach refers to the legal status of the financial institution would determine the type of supervisory oversight for its activities. Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

540 Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

541 National Treasury 2011 http://treasury.gov.za/documents/national%20budget/2011/A%20safer%20financial%20sector%20to%20serve%20South%20Africa%20better.pdf.

542 National Treasury 2011 http://gov.za/2011-budget-speech-minister-finance-pravin-gordhan.

543 National Treasury 2014 https://jutalaw.co.za/media/filestore/2015/03/2014_12_12_Response_document.pdf.

Financial Sector Conduct Authority will be housed in what is currently known as the Financial Services Board. It is anticipated that the *Financial Sector Regulation Bill* would be enacted by end June/July2016.[544]

The Twin Peaks approach is designed to underpin a comprehensive regulatory system with the following objectives:[545]

1. strengthen the approach to market conduct regulations by improving client confidence;
2. create a resilient, stable, sound financial system;
3. develop financial inclusion; and
4. combat financial crime (e.g. fraud, money laundering etc.) and prevent market abuse.[546]

An important component of both prudential and market conduct supervision is adherence to AML/CFT international standard and legislation.[547] The AML/CFT supervision of financial institutions will fall within the ambit of the Prudential Authority, whilst the Financial Sector Conduct Authority will supervise all market conduct matters as they will not fall under the Prudential Supervisor.[548]

From the preliminary assessment of the *Financial Sector Regulation Bill* it would appear that the implementation of the Twin Peaks model can increasingly become burdensome to financial institutions operating in South Africa. The increase in regulation might have both positive and undesirable effects on the financial market. An increase in compliance costs and the need to appoint regulatory resources (e.g. staff and monitoring systems) can affect investors' view of investment opportunities. On the other hand, it is believed that the Twin Peaks

---

544 Smit *Financial Mail* 1.

545 Juta Law 2015 https://jutalaw.co.za .

546 National Treasury 2014 https://jutalaw.co.za/media/filestore/2015/03/2014_12_12_Response_document.pdf.

547 Financial Services Board 2013 https://fsb.co.za/Departments/twinpeaks/Documents/Twin%20Peaks%2001%20Feb%202013%20Final.pdf.

548 Financial Services Board 2013 https://fsb.co.za/Departments/twinpeaks/Documents/Twin%20Peaks%2001%20Feb%202013%20Final.pdf.

approach would provide greater transparency, improved market integrity and better client protection.[549] The increase in regulations could be viewed as another proactive, preventative measure to prevent a re-occurrence of a global financial crisis.[550]

The enhanced Twin Peaks approach will require financial institutions to calibrate their objectives in an attempt to prevent a duplication of efforts and realise mutual goals.[551] The National Treasury advocates that these goals are attainable because the Twin Peaks model requires equal focus on prudential and market conduct regulation, through implementation of authorities responsible for each area.[552]

## 7 International cooperation

In order to hide the illicit origins of the proceeds of crime, criminals are increasingly taking advantage of an open international financing system to benefit from the free movement of funds across borders.[553] Combating ML/TF from a global perspective requires rapid sharing of information and effective international cooperation from various government organisations. [554]

FATF Recommendations 36 and 37 suggest that countries should not only ensure the implementation of the Vienna Convention[555], the Palermo Convention[556] and the

---

549 KPMG 2013 https://kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Financial-Services/Documents/KPMG%20Twin%20peaks.pdf.

550 KPMG 2013 https://kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Financial-Services/Documents/KPMG%20Twin%20peaks.pdf.

551 KPMG 2013 https://kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Financial-Services/Documents/KPMG%20Twin%20peaks.pdf.

552 National Treasury 2014 https://jutalaw.co.za/media/filestore/2015/03/2014_12_12_Response_document.pdf.

553 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* VIII-1 – VIII-2.

554 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* VIII-1 – VIII-2.

555 United Nations Treaty Collection unknown date https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en – United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substance, Vienna 20 December 1988. Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III 2.

556 International Peace Institute 2010 https://ciaonet.org/attachments/17631/uploads - Also known as the *United Nations Convention on Transnational Organised Crime (Palermo Convention).* Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III-3.

Terrorist Financing Convention,[557] but also encourage countries to provide the widest possible mutual legal assistance to prevent ML/TF.[558] This is made possible through the application of FATF Recommendation 29, which requires countries to establish a financial intelligence unit (hereinafter the FIU) who would receive and analyse any suspicious or unusual transaction reports. Following the establishment of an FIU and in promoting domestic and international cooperation, articles 7(1)(b), 7(3) and 7(4) of the 2000 Palermo Conventions *inter alia* obligate all ratifying countries[559] to authorise cooperative sharing of information among administrative, regulatory, law enforcement and other authorities.[560] This principle is also endorsed in the application of the Twin Peaks model of financial regulation. Chapter 4 of the *Financial Sector Regulation Bill* ensures the facilitation of cooperative supervisory responsibilities and the synchronisation of efforts between the prudential and market conduct regulators.[561]

The FIU's ability to function and cooperate[562] on a global level is contingent on the principle of mutual recognition and trust.[563] The exchange of information is achieved by the implementation of a mutual agreement (i.e. memorandums of understanding or treaties) which sets out the scope and terms of information exchange.[564] This principle of information exchange is supported by the Basel Committee,[565] which cautions that branch supervisors of banking groups should not be restricted in

---

557 United Nations 1999 https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf.

558 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* VIII-6.

559 On 29 September 2003 147 countries have in forced the obligations and 82 countries ratified it – http://unodc.org/unodc/crime_cicp_signatures_convention.html.

560 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* III-3 - III-4.

561 National Treasury 2014 https://jutalaw.co.za/media/filestore/2015/03/2014_12_12_Response_document.pdf.

562 Principle 3 of the Egmont Group Principles described "cooperation" as the free exchange of information for the purposes of analysis on a FIU level and protection of confidentiality of information. - Egmont Group 2013 https://egmontgroup.org/library/download/290.

563 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* VIII-6 and Egmont Group 2013 http://egmontgroup.org/library/download/290.

564 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* VIII-5.

565 Bank for International Settlements 2001 http://bis.org/pub/bcbs85.pdf.

sharing consolidated reports regarding the transferral of funds where called for by the home-country supervisor.[566]

The application of suitable legislation and procedures would guide the effectiveness of mutual assistance between branches of host and home countries and global FIUs, in effectively mitigating AML/CFT risks.

## 8 Concluding remarks

New payment technologies such as m-banking present both opportunities for and pose risks to the developing world. The use of soft law, such as the FATF Recommendations and Basel's Core Principles, enables banking industries to design their own financial services model and AML/CFT risk management programme.[567] From the guidance provided in FATF Recommendation 1, regulators and mobile money providers are placed in a position to better align financial inclusion and the financial integrity objective, based on the design of AML/CFT risk management control framework.[568] As such it is recommended that financial regulation should be proportionate to the potential threat posed to systemic stability without stifling beneficial innovation.[569]

It is clear that the implementation of sound soft law has a direct impact on setting flexible global, coordinated standards that are focused on emerging ML/TF risks. These standards have left an entrenched footprint on financial, AML and CFT regulation for domestic legislation.

Whilst the debate regarding implementation of AML/CFT controls and financial inclusion in new innovative payment products and services is ongoing and theoretical debates are ever-changing with the evolution of new innovative payment products and services, financial regulation will always have a role to play in shaping innovation

---

566 Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* VIII-9.

567 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf and Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

568 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

569 Huang *The Law and Regulation of Central Counterparties* 129-130.

and *vice versa*.[570] Due to the exchange of information, the virtual world of international m-banking adds an extra layer of complexity. It accordingly becomes problematic to establish jurisdictions and criminals are taking advantage of this space of uncertainty and lack of oversight.

[570] White 1997 *Technological Change, Financial Innovation and Financial Regulation in the USA: The Challenges for Public Policy* 97.

# CHAPTER 5

# NATIONAL LEGISLATION: REGULATORY CHALLENGES POSED BY MOBILE INNOVATION

*Compliance culture can also be regarded as a type of "preventive law" in which the proactive identification of potential treats and reporting thereof are regarded as fatal.*[571]

## 1 Introduction

The digital revolution[572] has not only transformed the way in which clients interact and access financial services and products, but has also forced legislators to rethink their regulatory approach.[573] The legislative approach[574] to AML and CFT has required financial institutions to assess and understand who their clients are,[575] forcing them to reshape the value proposition[576] and engender a compliance culture.[577] Taking a firm stand both domestically and internationally in support of an effective AML/CFT compliance culture has become contentious yet essential for a financial sector wishing to mitigate reputational risk.[578] Previous chapters of this study have shown that the regulatory framework is not entirely conducive to the principle of financial inclusion for low-income individuals who are not able to produce verifiable

---

571 Saksenberg *et al.* (2008) *FICA Training Manual* 3.

572 According to Juniper Research, mobile payments globally (including prepaid top-ups) are estimated to exceed USD 25 billion by 2018, which would mean an increase of 67% compared to the 2015 results (Juniper Research 2016 https://juniperresearch.com/press/press-releases/mobile-international-remittances-to-exceed-$25bn-b).

573 PWC Global FinTech Report 2014 https://pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf.

574 Encapsulated by, among others, the following pieces of legislation: *Banks Act* 94 of 1990; FICA; *Prevention of Organised Crime Act* 121 of 1998; *Protection of Constitutional Democracy Against Terrorist and Related Activities* Act 33 of 2004; *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002.

575 Section 21 of *FICA*; Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf; Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf and de Koker 2013 *Washington Journal of Law, Technology and Arts* 173-174.

576 "Value proposition" can be defined as the statement which articulates the benefits a client would receive by purchasing a product or service (Business Dictionary unknown http://businessdictionary.com/definition/value-proposition.html).

577 PWC Global FinTech Report 2014 https://pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf.

578 Saksenberg *et al* (2008) *FICA Training Manual* 3.

documentation proving their residential address.[579] The South African legislator realised that this would require a balance between financial inclusion and ML/TF risks.[580] The Minister of Finance promulgated an exemption[581] under *FICA* to relax[582] the standard CDD requirements.[583]

This chapter assesses the appropriateness of the legal and regulatory framework in the application of the KYC principle pertaining to m-banking transactions and examines whether the exemption provided to low-income individuals, in the spirit of financial inclusion integrity, does mitigate potential ML and TF risks. In this regard, Lawack[584] is of the view that South African regulation could be more flexible to enhance financial inclusion in the use of m-money. Regulatory gaps and areas of enhancement are therefore highlighted.

## 2 Governing statutes and regulations

The evolution of new payment technologies has forced central banks globally to review their regulatory and supervisory policy responses to these developments. For instance, the Bank for International Settlements' Committee on Payments and Market Infrastructure's[585] 2015 report on digital currencies highlighted the possible implications of emerging payment technologies for central banks (e.g., payment system, financial stability and monetary policy implications). From a South African regulatory perspective, m-banking has mostly been referred to as e-money as a subset of e-banking, meaning that the legal and regulatory framework linked to e-banking would apply to m-banking.[586] The primary statutes and regulations

---

579 De Koker 2009 *Journal of Money Laundering Control* 324-325.

580 Lawack 2013 *Washington Journal of Law, Technology and Arts* 318-344.

581 GN R.1596 in GG 24176 of 20 December 2002.

582 The publication of Exemption 17 of the *FICA* 38 of 2001, promoted financial inclusion and enabled 4 of the large 5 banks (i.e. Absa, Nedbank, Standard Bank, FirstRand Bank) and smaller banks to implement the Mzansi bank account focused on the unbanked (Finmark 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf).

583 De Koker 2009 *Journal of Money Laundering Control* 324 – 325.

584 Lawack 2013 *Washington Journal of Law, Technology and Arts* 318.

585 Bank for International Settlements' Committee on Payments and Market Infrastructures 2015 http://bis.org/cpmi/publ/d137.pdf.

586 Lawack-Davids 2012 *Journal of International Commercial Law and Technology (JICLT)* 319-320.

specifically governing the South African e-banking, AML/CFT and in particular m-banking and mobile payments are as follows:

- *Banks Act* and regulations published in terms thereof[587];
- *Currency and Exchanges Act* 9 of 1933 (hereinafter the *C&E Act*) read with the *Exchange Control Regulations* of 1961 issued in terms of *C&E Act* 9 of 1933, in the case of cross-border transactions, (hereinafter the *Exchange Control Regulations*);
- *SARB Act* 90 of 1989;
- *National Payment System Act* 78 of 1998 (hereinafter the *NPS Act*);
- *Prevention of Organised Crime Act* 121 of 1998 (hereinafter the *POCA*);
- *FICA*;
- *Protection of Constitutional Democracy Against Terrorist and Related Activities* Act 33 of 2004 (hereinafter the *POCDATARA*);
- *Exchange Control Regulations;*
- *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002 (hereinafter the *RICA*);
- *Electronic Communications Act* 36 of 2005;[588] and
- SARB Position Paper on Electronic Money.[589]

---

587 South African Government 2015 http://gov.za/documents/deposit-taking-institutions-act-6-mar-2015-1030. The *Banks Act* was first promulgated in 1990 as the *Deposit-taking Institutional Act* 94 of 1990 and renamed the *Banks Act* in 1993. It is primarily responsible for regulating and supervising public companies taking deposits from the public in support of sound and effective banking systems.

588 The *Electronic Communications Act* 36 of 2005 replaced the *Telecommunications Act* 103 of 1996, which was limited to the coverage of broadcasting and telecommunications under one regulator.

589 The South African Reserve Bank 2009 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem%28NPS%29/Legal/Documents/Position%20Paper/PP2009_01.pdf.

Most of South Africa's AML/CFT regulatory framework is based on international standards set by, *inter alia*, the FATF,[590] Basel[591] and the Wolfsberg Group.[592] Annexure 5.1 of this chapter illustrates how the international AML/CFT standards feed into the documentation and implementation of South Africa's AML/CFT regulatory framework.

To ensure effective oversight in the implementation of some of the above legislation, regulatory (e.g. FIC) and supervisory (e.g. SARB) authorities are legislatively appointed with specific authority and scope of application.

## 3 Regulatory authorities

The SARB, as the central bank, is responsible for achieving and maintaining price stability in the interest of balanced and sustainable economic growth.[593] In particular, the Registrar of Banks is responsible for bank regulation and supervision in South Africa.[594] In terms of the *NPS Act*, the Payment Association of South Africa is recognised as the payment management body tasked with organising, managing and regulating participants' participation in the payment system.

The FIC was legislatively established in terms of *FICA* and is appropriately positioned at the heart of South Africa's battle against ML and TF.[595] The FIC oversees compliance with *FICA* by all banks and provides guidance on the fulfilment of these duties. Section 45B, read with Schedule 2 (i.e., list of supervisory bodies) of *FICA* ,

---

590 The Financial Action Task Force is an inter-governmental body consisting of 36 members, which engages in the development and promotion of national and international policies and standards to combat ML and TF (de Koker 2013 *Washington Journal of Law, Technology and Arts* 167-169).

591 The Basel Committee on Banking Supervision is regarded as the international standard-setting institution for the prudential regulation of banks and provides the platform for cooperating on banking supervisory issues (Bank for International Settlements 2015 http://bis.org/bcbs/ about.htm).

592 The Wolfsburg Group of International Financial Institutions is an international institution that issues self-regulatory principles focused on ML/TF, private banking and correspondent banking, to name but a few (Wolfsberg Group 2015 http://wolfsberg-principles.com/).

593 The South African Reserve Bank date unknown http://resbank.co.za/Pages/default.aspx and this is confirmed in terms of ss 223 to 225 of the *Constitution of the Republic of South Africa Act* 108 of 1996 (hereinafter "the Constitution"). In particular s 224 of the Constitution requires the South African Reserve Bank to perform its functions independently and without fear, favour of prejudice.

594 In terms of ss 3 and 6 of the *Banks Act*.

595 Section 2 of *FICA* 38 of 2001 and Saksenberg *et al FICA Training Manual* 23-26.

empowers, *inter alia*, the Bank Supervision Department (hereinafter the BSD) of the Reserve Bank[596] to conduct AML/CFT inspections at banks. The BSD is responsible for collating and analysing reportable information;[597] providing guidance on the implementation of *FICA* and exchanging information with law enforcement agencies (e.g., South African Police Service) in an attempt to assist in the detection, prevention and deterrence of ML and TF activities.[598] The BSD, in collaboration with the National Payment System Department (hereinafter the NPSD) and FinSurv, is designated in terms of *FICA*[599] as a supervisory body and was delegated the following primary responsibilities:

- Supervising and enforcing compliance with legislative requirements (i.e., *FICA*, *Banks Act*) and international standards (i.e., FATF's 40 Recommendations, Committee on Banking Supervision's Core Principles);
- Promoting consistent interpretation and application of the AML/CFT legislative framework; and
- Engaging with all internal[600] and external stakeholders[601] to build an effective AML/CFT regime.

## 4 The *National Payment System Act*

Domestically and internationally, the effective functioning of a financial system is dependent on a sound and secure payment system.[602] An insufficiently protected system could cause risks within credit, liquidity and settlement, which could have a ripple effect and trigger systemic risks[603] in the financial market. A sound and secure

596 Section 45B read with schedule 2, item 2 of *FICA*.
597 Sections 27, 28, 28A, 29 and 32 of *FICA* 38 of 2001.
598 Section 3 of *FICA* 38 of 2001 and de Koker *South African Money Laundering and Terror Financing Law* 83-84.
599 Schedule 2.
600 For instance, the Financial Intelligence Centre, South African Police Service and the National Prosecuting Authority
601 Interpol, Financial Action Task Force, World Bank, Basel Committee on Banking Supervision and so on.
602 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 321.
603 Systemic risks are defined as the "risk that an event will trigger a loss of economic value or confidence in and attendant increases in uncertainty about, a substantial portion of the financial system that is serious enough to quite probably have significant adverse effects on the real economy" (European Parliament 2009

payment system is based on an unambiguous legal background.[604] All participants know exactly what their rights and obligations are in effecting system payments.

The SARB is required to perform such functions, implement such rules and procedures and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems.[605] The *NPS Act* is the enabling Act that reaffirms this authority.[606] The Bank's NPSD's mandate is to supervise the payment system which emanated from the said legislation.[607]

Section 3 of the *Banks Act* states that the Registrar of Banks is authorised to supervise the banking industry and section 6 gives the Registrar the authority to publish a circular or guidance note or directive, in consultation with all stakeholders[608] providing guidance regarding the application and interpretation of the provision of the *Banks Act*. In March 2016 the Bank's FinSurv[609] issued its first guidance note regarding m-banking, which stated that authorised dealer with limited authority may on application provide cross-border m-money services.[610]

Stemming from the above one could argue that the character of the product or service would determine which department would have oversight.[611] In the case of

---

http://europarl.europa.eu/document/activities/cont/200911/20091119ATT64822/20091119ATT64822EN.pdf).

604 Bank for International Settlements 2012 http://bis.org/publ/bcbs230.pdf.

605 Section 10(1)(c) of the *SARB Act*.

606 Section 2.

607 South African Reserve Bank 2015 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem%28NPS%29/Documents/Overview/Vision2015.pdf.

608 Stakeholders are banks, controlling, companies, representative offices, eligible institutions or authors of banks or controlling companies.

609 The Financial Surveillance Department is responsible for the day-to-day administration of exchange controls which is aimed at the prevention of loss of foreign currency resources through the transfer abroad of real or financial capital assets held in South Africa, whilst concurrently avoiding interference with the efficient operation of the commercial, industrial and financial system (South African Reserve Bank Financial Surveillance Department unknown date unknown dated https://resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/FAQs/Pages/General-Information.aspx.

610 South African Reserve Bank Financial Surveillance Department 2016 https://resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/Guidelines/Guidelines%20and%20public%20awareness/ADLA%20guidelines%20March%2016.pdf.

611 Lawack 2013 *Washington Journal of Law, Technology and Art* 324-325; in Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 321.

m-banking, there is no provision in the *Banks Act* precluding financial institutions from offering m-banking products or services. Having regard to the possible systemic risks that mobile payments might pose, the NPSD would be best placed to consider the threat to stability and confidence of the national payment system.[612]

The SARB published a Position Paper[613] on e-money in 2009[614] in which "e-money" was defined 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* [emphasis added].

The 2009 Position Paper points out the condition that the monetary value has to be convertible into physical cash or deposited into a bank account on demand.[615] Should the electronic value be unchangeable, it would not meet the requirements and would fall outside the ambit of legal tender. Furthermore, the *NPS Act* states that a person may, as a consistent feature of that person's business, accept payment instructions from any other person for the purposes of effecting payment on behalf of the first person, to a third party, to whom the payment is due.[616] It is not certain which situations would justify when a payment would be regarded as "being due".[617] Thus, the reference to the monetary value (i.e., electronic payment) being denoted by a "claim on the issuer" provides a clear distinction between payments to third parties, as set out in the *NPS Act* and the sending of electronic payments to a beneficiary for encashment thereof.[618] According to the position paper,[619] an electronic payment is

---

612 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 322.

613 In 1999 the South African Reserve Bank originally published a Position Paper on Electronic Money, which was amended in 2006 and 2009. Lawack 2013 *Washington Journal of Law, Technology and* Art 326.

614 South African Reserve Bank National Payment System Department 2009 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf.

615 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 322.

616 Section 7.

617 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 322.

618 Section 4. Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 322.

sent by the payer to a beneficiary and this payment (i.e., money) is not ordinarily "due" to the beneficiary in terms of an obligation. The resulting effect is that this might be regarded as a contravention of section 7 of the *NPS Act* as it bears the features of "deposit-taking".[620] However, the *Banks Act*[621] prohibits the taking of deposits from the general public by an unregistered bank (non-bank). This places a limitation on non-banks entering the market and accessing the payment system if they are not a registered bank or sponsored by a bank.[622]

In this regard, Klein and Mayer[623] believe that m-banking could be disaggregated into elements of service, storage, exchange, transfer or investment around which regulation could be structured. It is, however, unclear to them what kind of regulations would be appropriate for each element.[624] The author agrees with their arguments because the rapid innovation of emerging technologies in different areas of banking and telecommunications are making it difficult to create an open market since duplication or triplication of regulators occurs. Furthermore, the current SARB Position Paper on electronic payments is limited to a non-bank stakeholder who wishes to enter the market where banks are not able to assist the unbanked.

## 5 The *Banks Act*

Before the implementation of *FICA* in 2003 and in line with Basel's Core Principles for Effective Banking Supervision the *Banks Act*, *inter alia*, requires banks to implement controls to mitigate ML and TF risks. For instance, the Act states that the aim of the regulation is to provide guidance on the implementation and maintenance of effective risk management.[625] Regulation 39 of the *Banks Act* discusses the process of

---

619 South African Reserve Bank National Payment System Department 2009 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf.

620 Sections 1, 11 and 91(8) of the *Banks Act.*

621 Section 91(8) of the *Banks Act*.

622 For example, the Bank of Athens which is regarded as the agent bank of the Wizzit product. The Wizzit m-banking product uses a transactional bank account via secure m-banking technologies. Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 323.

623 Klein and Mayer 2013 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/ibrdmbankingregulation27-1.pdf.

624 Klein and Mayer 2013 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/ibrdmbankingregulation27-1.pdf.

625 Regulation 1.

corporate governance and requires banks to manage their risks.[626] To achieve this objective, banks are required to have a comprehensive risk management process, procedure and process in place that would assist them in the detection and prevention of criminal activities.[627] Regulation 50 of the *Banks Act* reaffirms this duty by requiring banks to implement and maintain robust controls, policies and processes to guard against the bank being abused for, *inter alia*, TF and ML. Another enabling control in the fight against ML/TF deals with reportable offences.[628] Banks are required to report any offences in writing to the Registrar within 30 days after the bank has become aware of any ML/TF activities.[629] This includes ML/TF activities in which the bank was involved and which were not identified in a timely manner.[630] Although this regulation also supports and strengthens the reporting obligations contained in *FICA*[631] it does not provide officials with inspection authority as prescribed.[632]

## 6 *Financial Intelligence Centre Act* 2001: CDD

Following on from the FATF Forty Recommendations, South Africa implement its own AML and CFT preventative measures via the application of legislation, namely the (i) *POC Act*, (ii) *FICA*, (iii) Money Laundering and Terrorist Financing Control Regulations (hereinafter the Regulations) read with the Exemptions in terms of *FICA,* (iv) *RICA* and (v) *POCDATARA*.[633] The FATF's Recommendations formed the contextual foundation for *FICA* and at the centre of its implementation lies South Africa's own financial intelligence unit, the FIC.[634] The purpose of *FICA* is to form a legislative framework[635] for effective identification of the proceeds of illicit activities;

---

626 Regulation 39(3)(a) to (aa) of the *Banks Act* list inter alia the following types of risk: capital, compliance, concentration, counterparty, currency, operational, reputational, technological and translation risks to name a few.

627 Regulation 39(4) of the *Banks Act* 94 of 1990.

628 In terms of Regulation 47(2) of the Banks Act.

629 Regulation 47(3)(e) of the *Banks Act* 94 of 1990.

630 Regulation 47(3)(e) of the *Banks Act* 94 of 1990.

631 Regulation 47(3)(e) of the *Banks Act* 94 of 1990 read with ss 27, 28, 28A, 29 and 32 *FICA* 38 of 2001.

632 Section 45B of *FICA* 38 of 2001.

633 De Koker 2009 *Journal of Money Laundering Control* 324-325.

634 Section 2 of *FICA* 38 of 2001.

635 Identification and verification of clients, record-keeping, reporting obligations, training of staff, appointment of a compliance officer and the establishment of the Financial Intelligence Centre.

combating ML and CTF and related activities. It plays an integral part in the fight against ML and TF.[636]

In line with FAFT Recommendation 3,[637] section 4 of the *POC Act* laid the foundation for the criminalisation of ML as a predicate offence. It supports the implementation of a number of ML measures aimed at the detection, investigation, reporting and/or implementation of control to unveil ML activities.[638]

The ML/TF mitigating techniques are based on eight basic principles,[639] of which four form the foundation: (i) "KYC", requiring intermediaries of financial systems to do CDD;[640] (ii) the preservation of both client and transaction information for the purpose of having an audit trail (i.e., record-keeping) (iii) the reporting principle, which requires the detection and reporting of cash transactions above R24 999.99,[641] suspected and unusual transactions,[642] and terrorist property reporting[643] to the FIC for further analysis. The fourth principle also requires the

---

636 Sections 28, 28A and 29 of *FICA*.

637 Financial Action Task Force Recommendation 3 recommended that countries should on the basis of the Viena Convention and the Palermo Convention, criminalised money laundering- Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf read with United Nations Treaty Collection unknown date https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en – United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substance and International Peace Institute 2010 https://ciaonet.org/attachments/17631/uploads - Also known as the "United Nations Convention on Transnational Organised Crime" was established with its main aim to fight organised crime. Expanding the global fight on organised crime, the United Nations adopted *The International Convention Against Organised Crime 2000 (Palermo Convention)*, which is a United Nations treaty published and signed in 1999.

638 In terms of the provisions of *FICA* 38 of 2001: ss 21 (KYC), 23 (client and transaction record-keeping), 28 (cash threshold reporting), 28A (terrorist property reporting), 29 (suspicious and unusual transaction reporting), 27 and 32 (FIC investigation information requests).

639 The eight principles as per *FICA* are (i) client identification and verification; (ii) record-keeping, (iii) reporting obligations (i.e., cash threshold reporting, terrorist financing reporting, and suspicions and unusual transaction reporting), (iv) training, (v) appointment of a money laundering compliance officer; (vi) documenting of policies and procedures; (vii) application of enhanced due diligence measures; and (viii) the application of a risk-based approach.

640 Client due diligence is the knowledge an accountable institution has about its client and the accountable institution's understanding of the business that the client is conducting with it. This principle of combating ML and TF, from a risk management control point of view, is codified in FICA in the form of s 21.

641 Section 28 of *FICA* 38 of 2001.

642 Section 29 of *FICA* 38 of 2001.

643 Section 28A of *FICA* 38 of 2001.

implementation of internal rules[644] to ensure the documentation of step-by-step working methods in respect of all *FICA* obligations.[645]

Notwithstanding the above and in terms of common law,[646] the requirement of client verification and identification at the opening of an account were already required before the implementation of *FICA*.[647] In the case of *Indac Electronics (Pty) Ltd vs Volkskas Bank Ltd*[648] the court held that the collecting banker owed the owner of a cheque a "duty of care" not to negligently[649] collect and proceed on behalf of another who is not the named payee. The court further stated that the duty of care encompassed an obligation placed upon the banker to take reasonable care when receiving and processing account opening applications.[650] In the case of *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* [651], the court noted and confirmed the trial court's statement that a bank was required to review all documentation at its disposal adequately and to apply its mind when opening an account or effecting a transaction.[652]

Based on the case law,[653] which expanded the duty of care, a bank has the following distinct obligations when opening an account:

---

644 Internal rules are documented anti-money laundering and countering the financing step-by-step policies and procedures as per s 42 of the of *FICA* 38 of 2001 and supported by Financial Action Task Force Recommendation 18 relating to internal controls (Financial Action Task Force Recommendation February 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

645 Section 42(1)(a) to (e) of *FICA* 38 of 2001.

646 *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* 2001 (3) SA 132 (W) and *Columbus Joint Venture v ABSA Bank Ltd* 2002 (1) SA 90 (SCA) par 5.

647 De Koker 2009 *Journal of Money Laundering Control* 325.

648 2001 (3) SA 132 (W), par 122.

649 Where a bank negligently processed a cheque the owner of the cheque can proceed against the bank with a delictual *Aquilian* action and as such the following elements had to prove: wrongful act or omission, fault, causation and loss (i.e. pure economic loss) (University of Johannesburg unknown date https://ujdigispace.uj.ac.za/bitstream/handle/10210/1836/DISSERTATIONfdff.pdf?sequence=1.

650 *KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd* 1995 (1) SA 377 (D) and *Powell and another v ABSA Bank Ltd t/a Volkskas Bank* 1998 (2) SA 807 (SE).

651 2001 (3) SA 132 (W).

652 The Court referred with approval to also paras 135, 136, 137 and 139 of the case under discussion.

653 *KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd* 1995 (1) SA 377 (D), *Powell and another v ABSA Bank Ltd t/a Volkskas Bank* 1998 (2) SA 807 (SE), *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* 2001 (3) SA 132 (W) and *Columbus Joint Venture v ABSA Bank Ltd* 2002 (1) SA 90 (SCA) par 5 and De Koker 2009 *Journal of Money Laundering Control* 325.

1. A common law duty to prevent fraudulent exploitation of the account and payment system by safeguarding the true owner and the public;[654] and

2. A statutory duty to:

    a. prevent a bank account from being abused for ML schemes or manipulated to avoid detection of criminal activities[655]; and

    b. maintain the safety and soundness of banks by ensuring that the bank knows who its clients are before entering into a business relationship or transaction.[656]

It is important to note that the above obligations were not substituted by the provisions of *FICA* and while a bank may comply with *FICA*'s obligation of CIV, it might omit to meet its common law obligations.[657]

## 7 Risk-based approach to simplified due diligence and exemptions

The flexibility of Internet and m-banking has increased not only financial institutions' geographical capacity, but also elevated financial inclusion.[658] Although software applications installed on payment systems provide a safety net to clients, they are not immune to financial crime, ML and TF risks.[659]

---

654 *Indac Electronics (Pty) Ltd vs Volkskas Bank Ltd* 2001 (3) SA 132 (W), par 122.

655 Regulations 39 and 50 of the *Banks Act*.

656 Regulations 39 and 50 of the *Banks Act*.

657 De Koker 2009 *Journal of Money Laundering Control* 325.

658 Booyens *A Legal Perspective on the Risks Relating to Internet Banking* 28.

659 During April 2013 the federal prosecutors of New York reported the arrest of seven suspects involved in the biggest, "surgical" cyber bank heist, which *inter alia* involved 40 50 ATM withdrawals and 17 pre-paid credit cards. Approximately USD 45 million was stolen and some of the funds were laundered in buying Rolex watches (Weber 2013 http://theweek.com/articles/464499/great-atm-heist-how-thieves-brazenly-stole-45-million-few-hours; Reaves, Scaife, Bates, Traynor and Butler 2015 http://cise.ufl.edu/~traynor/papers/reaves-usenix15a.pdf.) The University of Florida research on the security analysis of m-money apps assessed in developing countries revealed that smartphone apps with inappropriate access control, inadequate information security (information leak) and weak authentication/encryption could provide for cyber attackers, which would allow for both identity and monetary theft.

Following the publication of 2012 FATF Recommendations, most countries' AML/CFT strategies shifted from a rule-based to an RBA.[660] An assessment of *FICA* indicates that most of its sections are rule-based. It could be argued that the concept of an RBA has filtered through to the Regulations and Exemptions of *FICA*.[661] The application of an RBA was also evident in the revised 2012 FATF Recommendation 1[662] and South Africa's FIC Guidance Notes[663] and Public Compliance Communications[664] (hereinafter the PCC). FIC Guidance Note 1 confirms that accountable institutions can, based on an assessment of the ML/TF risks, take a decision on the appropriate method and level of verification it wishes to apply in a specific situation, subject to the application of a documented risk framework.[665] The note recommends that a degree of due diligence be applied, which should be equal to the client's level of ML/TF risks.[666] This would allow accountable institutions to focus their time and resources on the areas that require more attention due to the perceived ML/TF risks they pose to the business.[667]

---

660 Unger and van Waarden 2009 *Review of Law and Economics* 955-956 and Ali 2012 *Journal of Money Laundering Controls* 199.

661 FinMark Trust 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.

662 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf – In the interpretive notes to Recommendation 1 of Financial Action Task Force Recommendations and Financial Action Task Force 2015 http://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

663 Financial Intelligence Centre unknown date https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf and Financial Intelligence Centre 2013; https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf.

664 Financial Intelligence Centre 2014 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/new140213%20Website%20Statement%20PCC26%20wef%2013%20Feb%202014.pdf.

665 Financial Intelligence Centre unknown date https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf.

666 De Koker 2004 *TSAR* 719-720; Financial Intelligence Centre unknown date https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf and Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

667 De Koker 2004 *TSAR* 720 and Financial Intelligence Centre unknown date https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf.

The transformation from a rule-based to an RBA is founded on the fact that there is no universally accepted approach[668] to managing ML/TF risks, as financial institutions do not provide the same services or products to the same types of clients or in the same geographical areas.[669] Table 5.1, illustrates the differences in the rule-based and RBAs and provides the silent rationale for the FATF recommending[670] that an RBA rather be applied to mitigate ML/TF risks.

**Table 5.1: Differences between rule-based and risk-bases approaches**

| **Rule-based approach** | **Risk-based approach** |
|---|---|
| 1. Based on a precise norm of rules and fairly rigid- standard compliance.[671] | 1. Based on a less precise norm of standards and allows for flexibility – enhanced compliance. [672] |
| 2. Guided by documented and enacted rules found in AML/CFT legislation – technical adherence based on a tick box checklist. [673] | 2. Guided by the financial institution's identification, assessment and understanding of ML/TF risk levels, and the holistic implementation of documented and adequate AML/CFT |

668 Financial Action Task Force Recommendation 1 read with interpretive notes 1, 10 and 12- Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf

669 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf. In the interpretive notes to Recommendation 1 of Recommendations and Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/ RBA-Effective-supervision-and-enforcement.pdf.

670 Financial Action Task Force Recommendation 1 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

671 Unger and van Waarden 2009 *Review of Law and Economics* 955-956; Schäfer 2002 *German Working Paper in Law and Economics* 1-2 and Ali 2012 *Journal of Money Laundering Controls* 201-202.

672 Unger and van Waarden 2009 *Review of Law and Economics* 955-956 and Ali 2012 *Journal of Money Laundering Controls* 201-202.

673 Unger and van Waarden 2009 *Review of Law and Economics* 955-956 and Ali 2012 *Journal of Money Laundering Controls* 201-202.

| Rule-based approach | Risk-based approach |
|---|---|
| | controls based on the understanding of ML/TF risks.[674] |
| 3. Unyielding to adoption of changes in market ML/TF techniques, international standards and/or domestic legislation (e.g., set threshold limits for monitoring cash transactions. [675] | 3. Flexible to adjust to changes in the market, ML/TF techniques, international standards and domestic legislation. [676] |

Ai[677] believes that the implementation of a successful RBA to ML/TF risks depends on an understanding of the threats and vulnerabilities. Thus, the degree of due diligence applied should be communicated with the ML/TF risks identified, assessed and understood.[678] In terms of the new approach to risk management, financial institutions will be the drivers behind the adoption of customised solutions in relation to real ML/TF risks.[679] An RBA requires financial institutions' senior management to manage the responsibility of designing and implementing a risk-based framework based on the identification, assessment and understanding of the ML/TF risks facing the institution.[680]

In terms of FATF's Recommendation interpretive note 1, countries may elect to apply either an enhanced approach to identified ML/TF high risks or SDD controls to confirmed low risks, subject to a documented and implemented risk identification and

674 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf and De Koker 2013 *Washington Journal of Law, Technology and Arts* 173.

675 Unger and van Waarden 2009 *Review of Law and Economics* 955-956 and Ali 2012 *Journal of Money Laundering Controls* 201-202.

676 Costanzo 2007 http://2.econ.uu.nl/users/unger/papers/Costanzo.pdf and Ali 2012 *Journal of Money Laundering Controls* 199-200.

677 Ali 2012 *Journal of Money Laundering Controls* 201.

678 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf; De Koker *South African Money Laundering and Terror Financing Law* 216-288 and FinMark Trust 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.

679 Killick and Parody 2007 *Journal of Financial and Regulatory Compliance* 215-216.

680 Killick and Parody 2007 *Journal of Financial and Regulatory Compliance* 215-216.

assessment framework.[681] Demetriades[682] believes that in appropriate situations the application of "old-fashioned due diligence measures" might provide more insight into high-risk clients. However, he does not address what "appropriate situations" would be.

In circumstances defined as "low risk", accountable institutions can be exempted[683] from some CDD requirements.[684] The application of an exemption in AML/CFT legislation is subject to:[685] identified and confirmed low ML/TF risks; it being only applied in limited and justified situations that are linked to a particular financial activity; and the financial activity being effected on a limited basis by a natural or legal person.

SDD[686] refers to limited situations where it is acceptable for accountable institutions to apply a lower standard of CDD measures.[687] In practice, where accountable institutions elect to apply SDD, they are only required to identify and not verify all client information and documentation to such an extent where they would be in a position to understand the nature and purpose of the relationship.[688] What is interesting to note is that there is no FATF Recommendation and/or requirement in terms of *FICA* to conduct on-going due diligence or to understand the controlling structure of the low-risk client. There are also no sections in *FICA* that require a

---

681 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 341 and Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

682 Demetriades 2016 *Journal of Money Laundering Control* 88.

683 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 341 – 342 and Financial Action Task Force's Interpretive note 1- Financial Action Task Force 2012 http://fatf-gafi.org/ media/ fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

684 Client due diligence requirements can *inter alia* include but are not limited to obtaining certified copies of identification documentation; obtaining acceptable address verification; retaining identification and verification documentation, annual review of client's profile and transaction records etc.

685 Financial Action Task Force's Interpretive note 1 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/ recommendations/pdfs/FATF_Recommendations.pdf.

686 Financial Action Task Force's Interpretive Note 12- Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_ Recommendations.pdf.

687 Financial Action Task Force's Interpretive note 10 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

688 Financial Action Task Force's Interpretive note 10 - Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

financial institution to scrutinise and consider the identification documentation it received.

Therefore, it would appear that the ideal position would be to find an equilibrium between a light risk management and over-stringent regulatory approach that would decrease ethical risk, and enhance financial innovation and inclusion.[689] Given the ever-changing financial, geographical and financial technology environments, financial institutions may, based on their RBA, elect to apply both a rule-based approach (i.e., follow legislative rules) and RBA-based approach (i.e., change legislative rules to either a simplified[690] or an enhanced approach[691]) to AML/CFT. The approach applied would determine the nature and level of due diligence controls applied to a client, product or service.[692]

## 8 Know your client and record-keeping

One of the first indicators used to combat ML and to raise the standards of financial institutions in exercising due care[693] was the implementation of a CDD policy.[694] It is not surprising that this recommendation was incorporated into *FICA*, which prohibits accountable institutions[695] from establishing any business relationship[696] or to effect a single transaction (irrespective of the value), until it has established and verified the client's identity or the identity of any person acting on behalf of the client or on

689 Ali 2012 *Journal of Money Laundering Controls* 208.

690 Simplified approach: For example, only requires the client's fingerprint for identification purposes at on-boarding as opposed to a certified copy of the client's identification document.

691 Enhanced approach: For example, require the client to provide over and above the normal client identification document and address, salary advice and tax return.

692 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf – In the interpretive notes to Recommendation 1 of Financial Action Task Force Recommendations; Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf; De Koker 2013 *Washington Journal of Law, Technology and Arts* 173-174.

693 *KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd* 1995 (1) SA 377 (D) and *Powell and another v ABSA Bank Ltd t/a Volkskas Bank* 1998 (2) SA 807 (SE).

694 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf-FATF Recommendation 10.

695 In the form of s 21 read with Regulations 3 to 16 and 19. Schedule 1 of *FICA* defines accountable institutions as *inter alia* a person who carries on the "business of a bank" as defined in the Banks Act 94 of 1990.

696 Section 1 of *FICA*, defines a business relationship as "an arrangement between a client and an accountable institution for the purpose of concluding transactions on a regular basis".

whose behalf the client is acting.[697] This duty of client verification is limited to accountable institutions.[698] From the list of accountable institutions it would appear that only entities that are established and/or mandated to perform a specific function in terms of a statute can be regard as an accountable institution.[699]

A prescribed process to establish and verify a client's identity must be implemented.[700] Regulations were published in December 2002 that describe in detail the measures accountable institutions need to take when establishing and verifying their clients' identity.[701] They are required to do CDD in accordance with the specifications of the regulations. Regulations 3 to 16 explicitly deal with what type of information should be verified and/or obtained, having regard to the specific client category (i.e., natural persons, legal persons, partnerships or trust). It follows, therefore, that it would be sufficient to view the original documentation and obtain a copy thereof, which can be certified by a Commissioner of Oaths. In addition, provision is made for enhanced requirements in cases where a person acts on the authority of another.[702] Regulation 18 deals with the situation of verification in the absence of a person (i.e. non-face-to-face).[703] Although Regulation 19 requires an accountable institution to maintain the correctness of the information, namely keeping the KYC information up to date, the FIC is silent on the requirements of authenticity.

---

697 This requirement is also known as 'KYC'. Saksenberg *et al. FICA Training Manual* 65 – 68.

698 As set out in Chapter 3 of *FICA*. Schedule 1 provides a list of accountable institutions.

699 For example, (a) Banks-A person who carries on the "business of a bank" as defined in the Banks Act 94 of 1990; b) attorneys – a practitioner who practices as defined in s 1 of the Attorneys Act 53 of 1979; c) authorised dealer or authorised dealer with limited authority-a person who carries on the business of dealing in foreign exchange etc.

700 Section 21(1) of *FICA*.

701 Section 77 of FICA Financial Intelligence Centre 2009 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/FATF/MER%20South%20Africa%20full.pdf; Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-2040%20Recommendations%20rc.pdf.

702 Regulation 17.

703 Regulations 10 and 11. Regulations 3 to 18 of *FICA*; Financial Intelligence Centre date unknown https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf and Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf.

In accordance with FATF Recommendations,[704] *FICA* provides for the keeping of records[705] relating to business relationships and transactions.[706] FIC Guidance Notes 1[707] and 3A,[708] provide, *inter alia*, financial institutions with guidance on the application of an RBA,[709] risk indicators to consider and client profiling. In practice a combination of different factors would define the level of ML/TF risks a particular client poses and this would speak to the type of information an accountable institution would require before establishing the relationship or effecting a transaction.

### *8.1 FIC Guidance Notes*

From time to time the FIC issues guidance notes[710] that are of an authoritative nature and require accountable institutions to adhere to them.[711] In terms of FIC Guidance Note 3[712] and in line with FATF Recommendation 15,[713] accountable institutions should have documented internal policies and procedures aimed at mitigating ML and TF risks. Guidance Note 1[714] suggests that *FICA* and Regulations should be applied using an RBA. This implies that accountable institutions are able to accurately and

---

704 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

705 Section 22.

706 Section 23 confirms that the records must be stored for at least five years after the conclusion of the transaction; s 24 gives guidance on the storing of records by third parties; s 25 explains the admissibility of the records and s 26 deals with the FIC's access to the records.

707 Financial Intelligence Centre 2005 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/Guidance%20Note%203.pdf.

708 Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf.

709 Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf – provides a list of risk indicators which financial institutions could consider in the design and implementation of a risk matrix.

710 In terms of s 4(c) of *FICA* 38 of 2001,

711 Financial Intelligence Centre unknown https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf- The guidance provided does not substitute any part of *FICA* and is not legally binding.

712 Financial Intelligence Centre 2005 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/Guidance%20Note%203.pdf

713 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

714 Financial Intelligence Centre date unknown https:/fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf.

systematically identify and assess the risk involved which would put them in a position to take an informed decision as to the suitable controls to put in place (e.g., transaction monitoring, simplified or EDD). There is no requirement to follow "a-one-size-fits-all" methodology.[715] It is imperative that accountable institutions determine ML and TF risks using a holistic approach, which would provide an ultimate risk rating in accordance with a particular business relationship or transaction where all the factors that may be relevant were considered at both a clients and/or product and/or transaction level of risk (i.e., low, medium or high).[716]

### *8.2. Accountable institutions*

As the first point of entry into the financial system, accountable institutions have been identified as being vulnerable to exposure to the storing and transfer of illicit funds (e.g., identity fraud).[717] The term "accountable institution" is defined in *FICA*[718] as an individual or organisation that carries on the business of any entity listed in Schedule 1 of *FICA*. The list consists of 19 institutions that are required to give effect to various obligations imposed by *FICA.*[719] An accountable institution's obligations are thus not limited to identification and verification of clients, but also, *inter alia*, to record-keeping, monitoring and reporting of transactions and training of staff.

In respect of deposit-taking and in terms of section 1 of *the Banks Act*, MNOs are prohibited from offering any cash-out or mobile wallet facilities unless they are authorised to operate the "business as a bank" as defined in the *Banks Act*. Owing to this limitation, trusted third parties can nevertheless be appointed as a branchless bank for the purpose of leveraging the ubiquitous cellular networks and minimising

---

715 Financial Intelligence Centre 2014 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf.

716 Financial Intelligence Centre unknown date https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf; Financial Intelligence Centre 2014 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/new140213%20Website%20Statement%20PCC26%20wef%2013%20Feb%202014.pdf and Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf.

717 Lawack 2013 *Washington Journal of Law, Technologies and Arts* 339; and Kersop and du Toit 2015 *Potchefstroom Electronic Law Journal* 1643.

718 Section 1

719 Sections 21 to 24, 27 to 32, 42 and 43 of *FICA* 38 of 2001.

the barriers to financial services to the poor. Kersop and du Toit[720] believe that as MNOs are required to hold a banking licence, the effect thereof of is that MNOs "become, in part, a division of a financial institution". They argue that it could be implied that MNOs are accountable institutions.[721]

The South Africa banking industry follows a bank-centric mobile payment model[722] where MNOs provide the telecommunications network and accountable institutions (i.e., banks) the electronic payment infrastructure.[723] Accountable institutions are regarded as being the main role players in the provision of mobile payment services.[724] Although retail outlets manage the bulk of cash transactions on behalf of the accountable institutions' clients, they are still the cash distribution hub for the non-bank retail outlets.[725] MNOs will only be authorised to take deposits if they leverage off a banking licence partnership. In this regard, the compliance responsibilities with *FICA* reside with the accountable institutions (e.g., banks) to take all reasonable steps to ensure compliance with AML/CFT international standards and local legislation.[726] Any act of non-compliance by the MNOs would be deemed to be non-compliance by the accountable institution.

In view of the above and based on legislative requirements,[727] MNOs cannot be regarded as accountable institutions. Only entities designated within the said Schedule of *FICA* meet the definition of accountable institution. *FICA* obligations related to MNOs arise because of the accountable institutions (e.g., bank) associated with the issuance of the product. Hence, a client becomes a client of the accountable institution by virtue of a partnership or the MNO is regarded as a conduit[728] of an actual banking product. For now, most regulated entities that require a licence to operate appear to fall within the ambit of the definition. However, it is within

720 Kersop and du Toit 2015 *Potchefstroom Electronic Law Journal* 1617.
721 Kersop and du Toit 2015 *Potchefstroom Electronic Law Journal* 1617.
722 Chaix and Torre "Which economic model for mobile payments?" 2-3 and 9-10.
723 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/ Guidance-RBA-NPPS.pdf.
724 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.
725 Alexandre, Mas and Radcliffe 2010 http://ssrn.com/abstract=1664644.
726 Chatain P et al *Protecting Mobile Money against Financial Crime* xxxi.
727 Section 1 of *the Banks Act* 94 of 1990 and s 1 read with Schedule 1 (list of accountable institutions) of *FICA* .
728 Delivery channel.

policymakers' (i.e., National Treasury and FIC) discretion whether or not this definition should be expanded to MNOs.

### *8.3 Exemption 17 of FICA*

During the drafting of the Regulations the legislature had cognisance of the difficulties rural low-income individuals and those living in informal settlements may face in providing proof of a physical residential address.[729] To encourage financial inclusion and to overcome the said issue, the FIC published Exemption 17[730] of *FICA*, which provided relaxation in complying with section 21 of the Act*,* subject to certain terms and conditions.[731] In 2004 Exemption 17 was redrafted to provide a more practical application to reduce certain forms of identification,[732] and ease verification and record-keeping requirements[733] at the account opening stage or when effecting a single transaction.[734] *FICA* imposes certain conditions on accountable institutions[735] with regard to, *inter alia*, a

- duty to identify clients[736];
- duty to maintain and keep records[737];
- reporting duty[738] and access to information[739]; and
- duty to document step-by-step methods[740] to promote compliance by the accountable institution.

---

729 In terms of s 21 of *FICA*. De Koker 2009 *Journal of Money Laundering Control* 326.
730 GN R.1596 in GG 24176 of 20 December 2002.
731 The publication of Exemption 17 of *FICA*, promoted financial inclusion and enabled most of the large 5 banks (i.e. Absa, Nedbank, Standard Bank, FirstRand and Investec Bank) and smaller banks to implement the Mzansi bank account focused on the unbanked – Finmark 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.
732 Identification requirements consist of obtaining a copy of client's identity documents, but is not required in terms of s 21 read with Exemption 17 of *FICA* 38 of 2001 to obtain a copy of the proof of address.
733 Set out in Chapter 3 of FICA.
734 De Koker 2009 *Journal of Money Laundering Control* 326.
735 Set out in Chapter 3.
736 Section 21 of *FICA* 38 of 2001.
737 Section 22 of *FICA* 38 of 2001.
738 Sections 28, 28A and 29 of *FICA* 38 of 2001.
739 Section 42 of *FICA* 38 of 2001.

The application of SDD can be found in the terms and conditions set out in Exemption 17 of *FICA*. Table 5.2, illustrates the strict conditions and limited transactions to which Exemption 17 could be applied.

**Table 5.2: Strict criteria in respect of Exemption 17products**

| **Applies to** | **Conditions** | |
|---|---|---|
| | **Transactional amount** | **Client identification** |
| Limited to clients of the accountable institution who are:<br>1. natural persons, South African citizens or residents[741] effecting only domestic (including to the Common Monetary Area[742]) transactions; and<br>2. subject to the conditions of Exemption 17(3), (4) and (5), set out in the next two columns[743]. | The following conditions are applicable in case of single transactions and business relationships that:<br>1. would permit a client to withdraw or transfer or make payments of an amount not exceeding R5 000.00 a day and not exceed R25 000.00 in a monthly cycle;[744]<br>2. is limited to domestic transactions in the Republic of South Africa, except for a transfer as a result of point-of-sale payment or cash withdrawals in the | The following client identification conditions are applicable:<br>1. only offered to natural persons with South African identity documents;[747]<br>2. at account opening, the bank view the identity of client; and<br>3. the bank must have control measures to prevent the opening of more than one Exemption 17 account.[748] |

740 Sections 40, 45A and 45B of *FICA* 38 of 2001.
741 Exemption 17(2) of *FICA* 38 of 2001.
742 Common Monetary Area = consist of Lesotho, Namibia, South Africa and Swaziland as prescribed in terms of South African Reserve Bank Exchange Control Rulings issued in terms of s 9 of the *Currency and Exchanges Act* 9 of 1933 see South African Reserve Bank date unknown https://resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/Legislation/Documents/Exchange%20Control%20Regulations,%201961.pdf.
743 Exemption 17(3) of *FICA* 38 of 2001.
744 Exemption 17(1) to (5) of *FICA* 38 of 2001.

| Applies to | Conditions | |
|---|---|---|
| | **Transactional amount** | **Client identification** |
| | country in the rand Common Monetary Area;[745] and<br>3. is, however, subject to the balance in the account not exceeding R25 000.00, at any time.[746] | |

Should the conditions set out above be met, an accountable institution is exempt from complying with the following:[749]

1. Identification and verification obligation in respect of clients that are South African citizens or residents;
2. Obtaining and verifying the income tax registration number of clients;
3. Obtaining and verifying the residential address of clients;
4. Obtaining the contact particulars of a person acting on behalf of clients; and
5. The duty to keep record of the above information.[750]

Notwithstanding the above, Exemption 17 of *FICA* does not exempt an accountable institution from keeping record of the remaining client particulars that must be verified within the provision, as well as the requirements as set out in section 22 of *FICA* and the reporting obligation.[751] In order to provide better guidance on the scope

---

747 Exemption 17(2) of *FICA* 38 of 2001.
748 Exemption 17(4)(b) of *FICA* 38 of 2001.
745 Exemption 17(3)(b) of *FICA* 38 of 2001.
746 Exemption 17(4)(a) of *FICA* 38 of 2001.
749 Exemption 17(2) of *FICA* 38 of 2001.
750 Exemptions 17(2) and 17(4) of *FICA* of 38 of 2001.
751 Sections 28, 28A and 29 of *FICA* 38 of 2001.

and application of Exemption 17 of *FICA*, the FIC issued PCC 21.[752] It confirms that accountable institutions would not be exempted from maintaining a copy of the client's identity document, transactional record and/or all accounts linked to the transaction.[753]

An accountable institution is therefore only exempted from obtaining residential address information but is still required to obtain and verify all other CDD information.[754] Furthermore, should a client at any stage omit to comply with the conditions set out above, the accountable institution should have ML/TF controls in place that would trigger a full CDD to be done.[755] Based on FAFT Recommendations 1 and 15, and in the application of a holistic RBA[756] where an accountable institution has identified and assessed a high-risk client, it should apply an enhanced approach to account opening. The resulting effect would be that the application of a SDD process would not apply.[757]

### *8.3.1. Analysis of Exemption 17 of FICA products*

Analysis of Exemption 17 of *FICA*, indicates that:

1. although it was drafted to encourage financial inclusion for the low-income population it is not confined to a particular product;

2. should an accountable institution elect to offer Exemption 17 of *FICA* and comply with all the provisions thereof, it would not provide them with the

---

752 Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/PCC%2021%20Exemption%2017%20final.pdf.

753 Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/PCC%2021%20Exemption%2017%20final.pdf and FinMark Trust Compliance and Risk Resources 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.

754 De Koker 2009 *Journal of Money Laundering Control* 327 – namely identification documentation.

755 In compliance with s 21 of *FICA* 38 of 2001. S 42 of *FICA* – requires accountable institutions to have documented step-by-step working methods.

756 De Koker 2009 *Journal of Money Laundering Control* 327.

757 Financial Action Task Force Recommendations 1 and 15 (assess risk of new payment system prior to implementation)- Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf.

assurance that they are protected against ML/TF or fraud risks.[758] It was noted that the provisions of Exemption 17 of *FICA* came into effect before the application of *POCDATARA* (i.e. South Africa's CTF legislation);[759]

3. the provisions of Exemption 17 requires a face-to-face engagement with the client and does not exempt an accountable institution from complying with regulations 3(1)(a) to (c) and 4(1)(a) of *FICA*. Should an accountable institution wish to open an Exemption 17 account, it will still have to comply with regulation 18[760] of *FICA* read with FIC's Guidance Notes 1, 3 and 3A;[761]

4. the provisions of Exemption 17 of *FICA* is limited to South African citizens and residents, thus refugees and temporary residents without a valid identity document will not be allowed to open such accounts. It was also noted that the terms 'citizen' and 'resident' are not defined; and

5. while Exemption 17 of *FICA* prohibits the same person from opening more than one Exemption 17 account at an accountable institution, nothing prevents the same person from opening multiple Exemption 17 accounts with different accountable institutions, in order to be regarded as a low-risk client, thus avoiding the rigorous CDD requirements set out in sections 21 and 22 of *FICA*. Criminals might see these types of products as an excellent vehicle to apply the ML technique of mulling and smurfing to exit funds without the scrutiny applied to medium- or high-risk clients/products (i.e., transaction monitoring or annual client re-identification.

---

758 De Koker 2009 *Journal of Money Laundering Control* 327.

759 Sections 2 and 3 of *POCDATARA* and de Koker 2009 *Journal of Money Laundering Control* 327.

760 Regulation 18 of *FICA* 38 of 2001 requires an enhanced approach to be followed when opening an account on a non-face-to-face basis, which would defeat the purpose of the application of Exemption 17 of *FICA* 38 of 2001.

761 Financial Intelligence Centre unknown https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf and Financial Intelligence Centre 2012 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf

Exemption 17 of *FICA* remains silent on whether high-risk clients, such as politically exposed persons[762] or domestically/foreign prominent persons[763] (collectively referred to hereinafter the PEPs), should not be prohibited from opening such accounts. In this scenario, such an account would not be subject to the same scrutiny[764] (i.e., request for additional information) normally applied to PEP relationship, as it would make the application of the exemption obsolete.

During a 2015 FATF Australian AML/CFT mutual evaluation, FATF raised concerns about the excessive use of exemptions (i.e., simplified CDD) which could diminish the application of CDD.[765] Having regard to the findings raised by FATF's Australia Mutual Evaluation Report,[766] FATF's insistence on applying a holistic RBA[767] and the envisaged enactment of the *Financial Intelligence Centre Amendment Bill*, the question arises as to whether the legislator would use this opportunity to abandon the application of exemptions.

It should be noted that notwithstanding the fact that the current *FICA* does not legislatively provide for, *inter alia*, a specific section on PEPs[768] or the application of an RBA,[769] the envisaged *Financial Intelligence Centre Amendment Bill* will. In line with international standards, once accountable institutions have documented and implemented an RBA framework[770] and matrix,[771] it is anticipated that accountable

---

762 Politically exposed persons (PEPs) are domestic PEPs (e.g. members of parliament, judges, police) are individuals who have been or still are intrusted with domestically prominent public functions and inter terms of the Financial Action Task Force Recommendations possess a possible higher risk of being vulnerable to criminal (e.g. fraud, bribery etc.) and money laundering or terrorist financing activities and it is recommended that enhance due diligence should be applied when effecting transactions on behalf of the high risk individual – Financial Action Task Force Recommendation February 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf and de Koker *South African Money Laundering and Terror Financing Law* 577.

763 Section 21G of the *Financial Intelligence Centre Amendment Bill*.

764 Financial Action Task Force Recommendation February 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf-FATF Recommendation 6.

765 Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf.

766 Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf.

767 Section 3 of the *Financial Intelligence Centre Bill.*

768 Section 21G of the *Financial Intelligence Centre Amendment Bill*.

769 Section 42 of the *Financial Intelligence Centre Amendment Bill*.

770 Refers to the documented step-by-step working method.

771 Refer to the algorithmic rules used to risk rate a client, product, service, jurisdiction etc.

institutions should be able to manage the identified ML/TF risks[772] and have the discretion to apply SDD, CDD or EDD to their client base.

## 8.4 *Banks Act Guidance Note 6/2008*[773]

With the emergence of new innovative technologies focused on easy and convenient transfer of funds via the use of a mobile telephones and the creation of mobile bank accounts, the SARB took cognisance of the promotion of financial inclusion and the application of Exemption 17 of *FICA.* In the spirit of financial inclusion and integrity, on 13 July 2006 the bank issued *Banks Act* Circular 06/2006[774] relating to cellular telephone (hereinafter cell phone) banking. The AML/CFT controls applied to m-banking were considered after the Standard Bank of South Africa Limited[775] entered into a partnership agreement with MTN mobile, which resulted in m-banking accounts being opened on a non-face-to-face basis (i.e., without personal contact

with the bank), without reasonable steps being taken to verify the identity of the client.[776] On review and during 2008, *Banks Act* Circular 6/2008 was withdrawn and the Registrar of Banks[777] replaced *Banks Act* Circular 6/2008 with GN 6.[778]

---

772 Killick and Parody 2007 *Journal of Financial and Regulatory Compliance* 215-216.

773 South African Reserve Bank 2008 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/3290/g6%20of%202008.pdf.

774 South African Reserve Bank 2006 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/3058/banks%20act%20circ%206%20of%202006.pdf and South African Reserve Bank 2006 https://resbank.co.za/Publications/Reports/Documents/Annual%20Report%202006.pdf.

775 Porteous 2007 http://microfinancegateway.org/sites/default/files/mfg-en-paper-just-how-transformational-is-m-banking-feb-2007.pdf and De Koker 2009 *Journal of Money Laundering Control* 327.

776 Section 21 read with regulation 18 of *FICA*– verification in the absence of contact with a client; Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf and Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/PCC20.pdf.

777 In terms of s 6(5) of *the Banks Act*. S 6(5) of the *Banks Act* states: "The Registrar may from time to time by means of a guidance note furnish banks, controlling companies, representative offices, eligible institutions and auditors of banks or controlling companies with information in respect of market practices or market or industry developments within or outside the Republic.".

778 South African Reserve Bank 2016 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/ 7080/ G1%20of%202016.pdf.

GN 6 was issued by the Register of Banks with the aim to provide better guidance on the opening of m-banking accounts via a non-face-to-face process, linked to a bank account opened in terms of Exemption 17 of *FICA*. It follows therefore that GN 6 products will be limited within the constraints contained in Exemption 17.[779] It allows for the application of SDD to be performed and thus reducing the requirement of section 21 of *FICA's* verification and identification obligations. Similar to the Exemption 17 products, GN 6 requires the implementation of strict conditions that, *inter alia*, include the requirements of taking adequate steps to verify the identity of the client and cross-referencing the date against an independent and accepted third-party database (e.g., Department of Home Affairs).[780] The minimum criteria set out in GN 6 products are contained in Table 5.3:

**Table 5.3: Minimum criteria for Guidance Note 6 products[781]**

| **Applies to:** | **Conditions** | |
|---|---|---|
| | **Transactional amount** | **Client identification** |
| M-banking products linked to a bank account opened in terms of Exemption 17 of *FICA.* | The following transactional conditions are applicable:<br>1. The Bank may not open more than one GN 6 account; and<br>2. Opening of non-face-to-face accounts for low-value transactions and debits from the account is limited to R1 | The following client identification conditions are applicable:<br>1. Only offered to natural persons with South African identity documents;<br>2. At account opening, the bank must confirm the that the identity of the client is valid (e.g., not deceased/ |

779 De Koker 2009 *Journal of Money Laundering Control* 327.

780 South African Reserve Bank 2006 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/3058/banks%20act%20circ%206%20of%202006.pdf and South African Reserve Bank 2006 https://resbank.co.za/Publications/Reports/Documents/Annual%20Report%202006.pdf.

781 South African Reserve Bank 2006 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/3058/banks%20act%20circ%206%20of%202006.pdf and FinMark Trust Compliance and Risk Resources 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.

| Applies to: | Conditions | |
|---|---|---|
| | **Transactional amount** | **Client identification** |
| | 000.00 a day; and<br>3. If R1 000.00 is exceeded, the conditions of a face-to-face client identification in terms of Exemption 17 of *FICA* applies, which would require face-to-face verification process being applied; and<br>4. If limits of Exemption 17 of *FICA* are exceeded, section 21 of *FICA* applies.[782] | emigrated);<br>3. Confirm that name of the client does not appear on a database relating to fraud convictions;<br>4. Identity of the client must be verified by cross-referencing it against an in depended and accepted third-party database (i.e., identity number verified with Department of Home Affairs);<br>5. The bank must have control measures to prevent the opening of more than one GN 6 account; and<br>6. The bank must apply enhanced controls to monitor and assess the transaction activity for suspicious or unusual transactions.[783] |

[782] Exemption 17(5) of *FICA* 38 of 2001.

[783] Section 29 of *FICA* inter alia explains the reporting obligations relating to becoming aware of any suspicious or unusual transactions, which suspicion have to be reported to the Financial Intelligence Centre within 15 business days of becoming aware.

It is therefore evident that:

1. should any of the conditions contained in GN 6 not be met, the requirements of Exemption 17 of *FICA* will be applicable; or

2. should any of the conditions set out in Exemption 17 of *FICA* not be met, the exemption would lapse and the accountable institution would be required to comply with the CIV obligations set out in section 22 of *FICA*; and

3. should a bank fail to implement and apply additional due diligence controls to verify the identity of its client in terms of GN6 and/or Exemption 17 of *FICA*, the bank would be not able to proof that it complied with the common law obligations.[784]

### *8.4.1 Non-face-to-face verification*

Although FATF Recommendation 15[785] provides guidance on the mitigation of potential abuse of new technological development, such as m-banking, there is no section in *FICA* that specifically addressed this recommendation. However, in terms of Regulation 18 of *FICA*, banks are required to take reasonable measures to establish the existence or verify the identity of a natural person in situations where the client is not physically present (non-face-to-face),[786] when the business relationship is established or a single transaction is effected. During June 2005 the FIC published Guidance Note 3, for Banks on Client Identification and Verification and Related matters[787] which confirmed that banks should implement effective client

---

784 Banks are required to adequately review all documentation at its disposal and to apply its mind when opening an account or effecting a transaction as confirmed in, *inter alia*, *Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* 2001 (3) SA 132 (W) and *Columbus Joint Venture v ABSA Bank Ltd* 2002 (1) SA 90 (SCA) para 5. South African Reserve Bank 2006 https://resbank.co.za/Lists/News%20and%20Publications/ Attachments/ 3058/banks%20act%20circ%206%20of%202006.pdf and de Koker 2009 *Journal of Money Laundering Control* 327.

785 Financial Action Task Force Recommendation February 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf-FATF; Recommendation 15 and FinMark Trust Compliance and Risk Resources 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.

786 Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/ PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf.

787 GN 715 in GG 27803 of 18 July 2005.

identification procedures and ongoing monitoring standards for non-face-to-face clients. These measures could include requesting additional documentation normally obtained on face-to-face bases, which could take the form of independent contact with the client and/or uses of independent third party database.[788]

### *8.4.2 Analysis of Banks Act GN 6 products*

Assessment of *Banks Act* Circular 6/2006 and GN 6, read with Exemption 17 of *FICA*, showed the following:

1. Notwithstanding the introduction of money remitters, which conduct domestic transactions, in the 2004 amended Exemption 17 of *FICA*, both *Banks Act* Circular 6/2006 and GN 6 will not apply to products that are not aligned with the requirements of Exemption 17 account;[789]

2. GN 6 definitely requires the existence of a bank account;

3. GN 6 does not elaborate on the mechanism(s) that may be used to access the account, for instance, via the use of a bank card or ATMs. It follows, therefore, that GN 6 does not expressly state that the application is limited to m-banking as a way to access the bank account. GN6 is vague on the products it wishes to provide guidance on;

4. The scope of application of GN 6 is not clear because the term 'cell phone banking type products' was not defined. This lack of transparency creates opportunities for accountable institutions to design products that are linked to GN 6, but might evade the requirements of Exemption 17 of *FICA.* It could be argued that the addition of a reload card (e.g. Visa bank card) linked to a GN 6 m-banking product should be viewed as an additional mechanism, that provides the client with additional transactional capability (e.g. effect payments

[788] Financial Intelligence Centre 2005 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/Guidance%20Note%203.pdf.

[789] FinMark Trust Compliance and Risk Resources 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.

or withdrawals at an ATM). It is noted that the verification process applied to a reload card is different from GN 6 or Exemption 17 accounts; and

5. Analysis of the application of the non-face-to-face verification process shows up discrepancies between GN 6 and the Regulation 18 of *FICA*. Regulation 18 of *FICA* requires banks to take reasonable measures when establishing the existence or verifying the identity of a natural person in situations where the client is not physically present, while GN 6 states that in respect of low-value transactions and debits smaller or equal to R1 000.00 a day, non-face-to-face verification is permissible.[790] This creates the impression that non-face-to-face verification could be linked to a threshold limit, which is not stated in Regulation 18 of *FICA* read with FIC's Guidance Note[791].

It could be argued that the lack of clarity on the scope of the application of GN 6 can result in the application of SDD being extended to bank cards. This is a vulnerability that could cause banks to circumvent the requirements of Regulation 18 and/or Exemption 17 of *FICA* when issuing bank cards linked to GN 6 products. The assumption that low-risk products are not susceptible to ML/TF, combined with the contradiction in the application of non-face-to-face verification process, could defeat the purposes of CDD and reporting since the bank might not know who its client is and thus would not have sufficient information to monitor and report any suspicious or unusual transactions.[792]

---

[790] South African Reserve Bank 2006 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/3058/banks%20act%20circ%206%20of%202006.pdf and South African Reserve Bank 2006 https://resbank.co.za/Publications/Reports/Documents/Annual%20Report%202006.pdf.

[791] GN 715 in GG 27803 of 18 July 2005 and Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf.

[792] Sections 28A and 29 of *FICA* 38 of 2001.

### *8.5 Financial Surveillance Department: Cross-Border Remittance Exemption*

One of the functions of the SARB's FinSurv[793] is to ensure banking and financial soundness, which includes protecting the value of the South African currency.[794] FinSurv is responsible for administering[795] the *Exchange Control Regulations,*[796] made in terms of section 9 of the *C&E Act*, which forms the foundation for the exchange control in South Africa.[797] The Governor-General[798] is authorised to implement regulations relating to or affecting the currency, banking or exchanges.

In terms of *Exchange Control Regulations*, FinSurv issues orders and rules that also contain exemptions, forms and procedural arrangements that include the appointment of certain banks to act as authorised dealers[799] or authorised dealers with limited authority[800] (hereinafter the ADLAR).[801] FinSurv issues Exchange Control Rulings (hereinafter the Rulings) and Circulars that provide authorised dealers and/or ADLAs with administrative measures, permissions, conditions and limits applicable to foreign currency transactions. In the assessment of the Rulings it could be argued that they are in themselves not law as FinSurv does

---

793 The Treasury is defined in terms of Exchange Control Regulations 1 as: "In relation to any matter contemplated in these Regulations the Minister of Finance or an officer in the Department of Finance who, by virtue of the division of work in that department, deals with the matter on the authority of the Minister of Finance."

794 Section 3 of the *South African Reserve Bank Act* 90 of 1989; ss 223 to 225 of the *Constitution of the Republic of South Africa*, 1996; and South African Reserve Bank unknown date http://resbank.co.za/AboutUs/Functions/Pages/default.aspx.

795 In terms of the Exchange Control Regulations, regulation 1, the control over South Africa's foreign currency reserves as well as the accruals and spending thereof is vested in the Treasury.

796 Made in terms of s 9 of the C&E Ac.t Was promulgated on 1 December 1961 in terms of GN R1111 in GG Extraordinary 123 of 1 December 1961.

797 Published in GN R1111 in GG Extraordinary 123, of 1 December 1961, and as amended from time to time.

798 In terms of s 9(1) of the C&E Act. According to the definitions clause of the *Interpretation Act* 33 of 1957, the status of a "Governor-General" today means the President of the Republic of South Africa.

799 "Authorised Dealers" refers to bank dealing in foreign exchange which gives the authority by the South African Reserve Bank to buy and sell foreign exchange subject to the conditions and within the limits prescribed by the Department. They are not agents of the Financial Surveillance Department, but act on behalf of their clients in seeking approval to deal in foreign currency – Regulation 2 of the *Exchange Control Regulations, 1961*.

800 South African Reserve Bank unknown https:// resbank.co.za/ RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/Pages/CurrencyandExchangesdocuments.aspx.

801 GN R1111 in GG Extraordinary 123 of 1 December 1961, as amended.

not have any legislative power. The Rulings are, however, issued by the *Exchange Control Regulations* which do provide for, for instance, the granting of permission to effect foreign exchange transaction that would otherwise be prohibited by the Regulations. Thus the Rulings have legal status and force.[802]

On 1 July 2015, the Minister of Finance approved an exemption to be implemented relating to cross-border remittances[803] that allow accountable institutions to reduce compliance with the identification requirements[804] and lightens the verification and record-keeping[805] requirements, subject to certain terms and conditions being adhered to. Table 5.4, illustrates the strict conditions and limited transactions to which the cross-border exemption[806] could be applied.

**Table 5.4: Strict criteria in respect of application of the cross-border remittance exemption**

| | **Conditions** | |
|---|---|---|
| **Applies to** | **Transactional amount** | **Client identification** |
| The implementation of the exemption is limited to the following accountable institutions:<br>1. All banks;<br>2. Mutual banks;<br>3. Post bank;<br>4. Ithala Development | The following conditions are applicable:[808]<br>1. To only a single transaction where funds are transferred or remitted to a jurisdiction outside South Africa;<br>2. Not exceeding an amount of R3 000.00 a day and within a limit of R10 000.00 in a | The following client identification conditions are applicable:<br>1. Only transfers between natural persons are permitted;[810] and<br>2. A transaction with juristic persons (e.g., trust, companies) is not |

802 *Sylla and Others v Minster of the Department of Finance and Another* (08/38696) [2011] SAGPJHC 200.

803 GN 461 in GG No. 38844 of 5 June 2015 and Exchange Control Circular No 22/2015 dated 30 June 2015.

804 Section 21 of *FICA* 38 of 2001 sets out the requirements for identification and verification of clients.

805 Section 22 of *FICA* 38 of 2001 sets out the requirements for maintaining client and transactional records.

806 GN 461 in GG No. 38844 of 5 June 2015.

| Applies to | Conditions | |
|---|---|---|
| | **Transactional amount** | **Client identification** |
| Corporation; and<br>5. Money remitter.[807] | calendar month, and<br>3. Transaction limit is only bound to outward transactions.[809] | permitted. [811] |

The purpose of the exemption is to reduce some of the regulatory requirements in respect of cross-border remittance services and encourage financial inclusion.[812] In July 2015 the FIC issued guidance[813] on the scope and application of the cross-border remittance exemption. Should the conditions contained in the said exemption be met, an accountable institution is exempt from complying with the obligation and verifying the residential address;[814] obtaining and verifying the income tax registration number of client;[815] and the duty to keep record of the manner in which

808 GN 461 in GG No. 38844 of 5 June 2015.

810 Financial Intelligence Centre 2015 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/Web%20note%20-%20cross%20border%20remittances%20-%20PCC%2032.pdf.

807 Financial Intelligence Centre 2015 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/Web%20note%20-%20cross%20border%20remittances%20-%20PCC%2032.pdf.

809 Financial Intelligence Centre 2015 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/Web%20note%20-%20cross%20border%20remittances%20-%20PCC%2032.pdf.

811 Financial Intelligence Centre 2015 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/Web%20note%20-%20cross%20border%20remittances%20-%20PCC%2032.pdf.

812 Financial Intelligence Centre 2015 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/Web%20note%20-%20cross%20border%20remittances%20-%20PCC%2032.pdf.

813 Financial Intelligence Centre 2015 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/Web%20note%20-%20cross%20border%20remittances%20-%20PCC%2032.pdf.

814 Regulations 3(1)(e), 3(2)(d), 4(3) and 5(1)(f) of *FICA* of 38 of 2001.

815 Regulations 3(1)(d), 4(2) and 5(1)(e) of *FICA* of 38 of 2001.

the identity of the client was established;[816] and the name of the person who obtained the information[817] above.

The cross-border remittance exemption still requires accountable institution to[818] obtain the address of a person acting on behalf of client;[819] maintain records of the identity of the client, client who is acting on behalf of another client and person acting on behalf to the client;[820] retain the nature of the business relationship or transaction;[821] and maintain account and transactional records.[822]

### *8.5.1 Analysis of the Financial Surveillance Department's cross-border remittance exemption*

Analysis of the cross-border remittance exemption shows that:

1. the terms and conditions almost mirror that of Exemption 17 of *FICA*, except for being more stringent on the record-keeping requirements;

2. the terms and conditions are silent on whether a face-to-face engagement would be required for the single transaction to be effected. It could, therefore, be interpreted that non-face-to-face single transactions would be permissible. Accountable institutions would still have to comply with regulation 18 of *FICA* read with FIC's Guidance Notes 1, 3 and 3A;[823]

3. while the exemption only permits single transactions not exceeding R3 000.00 and R10 000.00 per calendar month, per person, nothing prohibits the same person from effecting multiple transactions within the said limits at different accountable institutions, thus avoiding opening a bank account and the rigorous CDD requirements set out in sections 21 and 22 of *FICA*. This exemption could

816 Section 22(1)(d) *FICA* of 38 of 2001.
817 Section 22(1)(h) *FICA* of 38 of 2001.
818 GN 461 in GG No. 38844 of 5 June 2015.
819 Regulations 3(2)(e) of *FICA* of 38 of 2001.
820 Sections 22(1)(a) to (c) of *FICA* of 38 of 2001.
821 Sections 22(1)(e) of *FICA* of 38 of 2001.
822 Sections 22(1)(f) and (g) of *FICA* of 38 of 2001.
823 Financial Intelligence Centre unknown https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf and Financial Intelligence Centre 2012 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf.

be susceptible to ML and TF techniques, without the scrutiny normally being applied to such products (i.e. transaction monitoring or annual client re-identification etc.); and

4. even if the accountable institution complies with all the terms and conditions of this exemption it would not provide it with the assurance that it is protected against ML/TF or fraud risks.

Accountable institutions are therefore only exempted from obtaining residential address information and are still required to obtain and verify all other clients' identity documents.[824] A reading of Exemption 17 of *FICA* and the cross-border remittance exemption raises the question of whether or not this new exemption is not merely an extension of Exemption 17, which allows for foreign transactions being effected at a lower threshold limit.

## *9 Financial Intelligence Centre Amendment Bill*

Financial crime and the use of ML and TF techniques remain key issues on the global and local agendas of law enforcement.[825] Since the first publication of the FATF Recommendations in 2003,[826] international standards[827] on the combating of ML and TF have evolved.

Following the FATF mutual evaluation of South Africa during 2009, significant vulnerabilities[828] in South Africa's regulatory AML/CFT system were identified.[829] The

---

824 GN 461 in GG No. 38844 of 5 June 2015.

825 Demetriades 2016 *Journal of Money Laundering Control* 80 and the European Parliament and Council 2005 *Official Journal of the European Union, paragraph 5* and can also be found on The European Parliament and Council 2005 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=en.

826 Financial Action Task Force unknown date http://atf-gafi.org/countries/ .

827 Financial Action Task Force Recommendation February 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf and United Nations Convention against Transitional Organised Crime and the Protocols Thereof (Palermo Convention), 15 November 2000 relating to the freezing of assets.

828 Financial Action Task Force 2009 http://fatf-gafi.org/media/fatf/documents/reports/mer/MER%20South%20Africa%20full.pdf-FATF identified following gaps in South Africa's regulatory framework: *The Financial Institutions Act* of 38 of 2001 were regarded as being too prescriptive and rules-based on certain provisions; Constitutional Court Decision of *Estate Agency Affairs Board v Auction Alliance (Pty) Ltd and Others* [2014] ZACC 3 prohibited the non-routine inspections subject to certain condition;

purpose of the *Financial Intelligence Centre Amendment Bill* is to implement a sound and stronger AML/CFT regulatory framework for addressing them,[830] *inter alia*, by legislatively enhancing the CDD requirements; requiring the application of an RBA in identifying, assessing and implementing controls to manage ML and TF risks; providing for the employment of the United Nations Security Council Resolution relating to freezing of assets in the terrorist property reporting area; extending the objectives and function of the FIC in relation to the exchange of information, suspicious transaction monitoring; and the enhancement of administrative and enforcement activities.[831]

In trying to meet the expectations of the FATF Recommendation, the Bill has broadened the application of CDD by introducing two new concepts, namely (i) the application of on-going due diligence on clients' transaction records and (ii) enhanced measures for persons in prominent public/private industry,[832] referred to as 'prominent influential persons' (hereinafter the PIPs, previously known as 'PEPs').[833] Furthermore, the application of a risk-based management system will assist accountable intuitions with proactively focusing their efforts and resources on those clients and/or products or services that have a higher probability of being abused by

---

absence of private sector prominent influential persons (PIPs) list (implementation difficult thereof difficult to identify and enforce), etc.

829 Financial Action Task Force 2009 http://fatf-gafi.org/media/fatf/documents/reports/mer/MER%20South%20Africa%20full.pdf.

830 Department: National Treasury and the Financial Intelligence Centre "Financial Intelligence Centre Amendment Bill, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation 20 April 2016 and Financial Action Task Force 2009 http://fatf-gafi.org/media/fatf/documents/reports/mer/MER%20South%20Africa%20full.pdf.

831 Objective of the *Financial Intelligence Centre Amendment Bill* - Department: National Treasury and the Financial Intelligence Centre "Financial Intelligence Centre Amendment Bill, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation 20 April 2016.

832 Section 21G of the *Financial Intelligence Centre Amendment Bill* - Department: National Treasury and the Financial Intelligence Centre "Financial Intelligence Centre Amendment Bill, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation 20 April 2016.

833 Department: National Treasury and the Financial Intelligence Centre "Financial Intelligence Centre Amendment Bill, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation 20 April 2016. It would appear from the proposed enhancement and addition of ss 1(g), (i), 21F and 21G in the *Financial Intelligence Centre Amendment Bill* that the definition of prominent influential persons (PIPs) would have a broader field of review of client relationships (i.e., related parties and associates to the identified PIP would also be under scrutiny) compared to the control measures applied to politically exposed persons (PEPs).

criminals.[834] The Bill requires accountable institutions to design, document, maintain and implement an AML/CFT Risk Management Compliance Programme.[835]

The regulatory and contextual foundation created by the bill will address the vulnerabilities identified in the FATF's evaluation, which would prevent the downgrading of the country's compliancy rating and strengthen the AML/CFT regulatory framework.

## 10 *The Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002

The most rapid development in the recent past has been in the symbiotic relationship that ensued between banking and telecommunications, in the form of m-banking. As the opportunities of m-banking increase, so too does its vulnerably to abuse. The question as to whether the regulation of e-money should fall under the function of banking or non-banking institutions, such as MNOs, has been an ongoing academic debate.[836] Multiple regulators were pulled into this space of oversight of payments and telecommunications.[837] The SARB's NPSD's Position Paper[838] read with section 91(8) of the *Banks Act,* however, confirms that the issuer of e-money has to be a registered South African bank. As already stated, the regulation of banks and payments falls within the ambit of the SARB,[839] while the regulation of telecommunications falls within the ambit of the *Electronic Communications Act* 36 of 2005.[840] In this instance and in terms of section 3 of the *Independent*

---

834 Section 42 of the *Financial Intelligence Centre Amendment Bill* - Department: National Treasury and the Financial Intelligence Centre "Financial Intelligence Centre Amendment Bill, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation 20 April 2016.

835 Sections 1(q), 21(1), 21A and 21B of the *Financial Intelligence Centre Amendment Bill* - Department: National Treasury and the Financial Intelligence Centre "Financial Intelligence Centre Amendment Bill, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation 20 April 2016.

836 Mann 2004 *TLR* 704.

837 Lawack 2013 *Washington Journal of Law, Technology and Art* 328.

838 South African Reserve Bank National Payment System Department 2009 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf.

839 *Banks Act* 94 of 1990*, National Payment Systems Act* 78 of 1998, *South African Reserve Bank Act 90 of 1989 and the Currency and Exchanges Act* 9 of 1933 read with the *Exchange Control Regulations.*

840 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 324*.*

*Communications Authority of South Africa Act* 13 of 2000, the main authority is the Independent Communications Authority.

The aim of *RICA* was, *inter alia*, to provide a mechanism to lawfully intercept communication and monitor information to combat crime.[841] Burner phones[842] have become a prevalent mechanism to commit financial crime, such as fraud, identity theft and hacking with the aim to transfer funds unlawfully. Authorities have released the need to amend *RICA*, in order also to mitigate ML/TF risks. Thus, connected to the CDD applied at account opening. During 2009, *RICA* was amended to make provision for the implementation of CIV controls, in respect of mobile telephone users.[843]

Almost aligned to the requirements of sections 21 and 22 of *FICA*, section 39 of *RICA* requires a telecommunications service provider to identify, verify and maintain records of the client's identify, business or postal address before entering into a contract for telecommunications service.[844] Furthermore, section 40 of *RICA* states that MNOs are prohibited from activating a SIM[845] card on their electronic communications systems before adhering to the requirements of the face-to-face identification and verification.[846] An interesting development regarding SIM card face-to-face identification was that the Nigerian Communications Commission issued an administrative sanction against South Africa' MNO MNT for failure to disconnect unregistered SIM users, which could be used by Islamist Groups (e.g., Boko Haram) to finance terrorist activities.[847] In view of the face-to-face identification requirements

---

841 Section 1 of *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002.

842 "Burner phones" are regarded as unregistered (unregulated) prepaid phoned specifically used for a purpose and then disposed of in an attempt to hid from being detected (Miller *et al.* 2016 http://arxiv.org/pdf/1602.05048.pdf).

843 De Koker 2010 http://cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf and Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 340.

844 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 340.

845 SIM refer to a subscriber identity module. It is a smart card that is held in a mobile telephone capable of storing an identification number unique to the owner and personal data.

846 Section 39 of *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002.

847 Eyewitness News 2016 http://ewn.co.za/2016/02/29/Nigerian-regulator-confirms-MTN-has-paid-250-mln-in-fine-dispute-Regulators administrative fine was United States Dollar 3.9-billion.

contained in *RICA,* de Koker[848] is of the view that *RICA* does not support the provisions of GN 6,[849] which allows for non-face-to-face verification in confirmed low-risk m-banking.[850]

Compared to the identification and verification requirements set out in sections 21 and 22 of *FICA, RICA* permits clients to use a wide range of identification documents, which are not limited to the client's identification document (i.e., green bar-coded identity document[851]), listed in FIC's Guidance Note 3.[852] Furthermore, *RICA* requires MNOs to obtain a client's business or postal address, which is not limited to a physical residential address as required in terms of Regulations 3 to 17 of *FICA*.[853] It can be argued that the identification and verification requirement in *RICA* and *FICA* are not seamlessly aligned in respect of Exemption 17 of *FICA* and GN 6 products. *RICA* furthermore does not provide for exemptions to the identification and verifications requirements[854] and it would appear to be contradicting the spirit of financial inclusion set out in Exemption 17 and GN 6 products.

Another element of misalignment is that *RICA* does not provide for maintaining (i.e., re-verification) the correctness of the information obtained as set out in Regulation 19 of *FICA*. De Koker[855] believes that *RICA*'s identification and verification

---

848 De Koker 2010 http://cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf

849 South African Reserve Bank 2006 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/3058/banks%20act%20circ%206%20of%202006.pdf and FinMark Trust Compliance and Risk Resources 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf.

850 De Koker 2010 http://cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf.

851 Financial Intelligence Centre 2005 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/Guidance%20Note%203.pdf; and Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf.

852 Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf

853 Regulations 3(1)(e), 3(2)(d), 5(1)(f), 5(2)(e), 7(c),7(f)(ii), etc. of *FICA* 38 of 2001; Financial Intelligence Centre 2005 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/Guidance%20Note%203.pdf; and Financial Intelligence Centre 2013 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/130328%20GUIDANCE%20NOTE%203A.pdf. De Koker 2010 http://cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf.

854 Section 39 of *the Protection of Personal Information Act* 4 of 2013.

855 De Koker 2010 http://cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf.

process were not subject to the same rigorous integrity checks as are applied in the banking sphere. Since the implementation of section 39 of *RICA*, the identification and verification process would appear to be aligned with the information required by an accountable institution (e.g., banks). Thus, it can be argued that *RICA* does indirectly provide for re-verification through the process of upgrading a mobile telephone contract. Furthermore, the new identification management solutions are becoming more popular and thus the use of biometric (e.g., fingerprints, voice recording or pupil scanning)[856] to identify clients could replace the paper base identification process.[857] Fingerprint identification applications are already used in some smartphones to lock or unlock the keypad and Net1 uses biometric identification to mitigate identity fraud with social grants.[858]

It would appear that the biggest challenges in the financial technical innovation sphere are outdated information and legal uncertainty, that regulatory arbitrage could create and criminals would take advantage of regulatory lacunae.[859]

## 11. Regulatory challenges

M-banking provides a remittance channel that increases confidence in the banking system and development of payment systems for all. Conversely, great advantages in innovative technologies, particularly in the area of finance, imply far-reaching changes and challenges.[860] Legislation unavoidably tails innovation. It appears legislation is trying to catch up in order to manage potential threats. Based on its adverse and innovative traits, m-banking, and especially mobile payments, has a

856 The Department of Home Affairs' South Africa's Social Security Agency (SASS) together with Net1 is using biometric finger print identification process to mitigate fraud in awarding social grants (Cronje *Mail & Guardian* no page and also on *Mail & Guardian* 2015 http://mg.co.za/article/2015-10-14-net1-the-company-that-runs-the-social-grant-payment-system; and PWC Global FinTech Report 2014 https://pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf

857 PWC Global FinTech Report 2014 https://pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf

858 Net1 together with Grindrod Bank Limited was appointed the Minister of Welfare and Development to manage the allocation of social grants, mitigate indentity fraud and encourage financial inclusion by opening of GN6 and Exemption 17 accounts, for those low-income individuals residing in informal settlements-Net1 2012 http://net1.com/legal/terms-and-conditions-for-the-use-of-the-sassa-card-and-sassa-account/.

859 Lawack 2013 *Washington Journal of Law, Technology and Art* 328.

860 Eurofi 2014 https://eurofi.net/wp-content/uploads/2014/09/Electronic-Payment-services-WEB.pdf.

significant impact on both the banking and regulatory environment.[861] Regulators are constantly forced to muster an equal amount of ingenuity to balance both the advantages and threats posed by financial payment innovation.[862]

Lawack-Davids[863] believe that emerging technologies can influence a change in the structure and functions of financial institutions as traditional lines of demarcation become vague. Migrating workers sending money informally creates both opportunities for unbanked clients and gaps for identity fraud.[864] Owing to widespread usage and complex technological systems, innovative technologies such as m-banking can also alter the nature and scope of existing risks by creating new risks (e.g., new ML/TF techniques, cyber-crime).[865] This can have an adverse effect on the traditional methods of safety and soundness of supervision, which would require regulators to re-think their regulatory approach and rules.[866] One of the key operational risks for mobile payment systems is the prevention of abuse and fraud due to unsecure software applications or systems and the consequence of ML and TF.[867] Examples of unauthorised access techniques used to retrieve and use confidential information (e.g., bank account numbers) are spoofing, skimming, back-doors, hacking or high-jacking.[868] These techniques have caused the financial sector great loss.[869]

As already noted, regulations can impact on the ability to send money given the stringent legislation. The requirement of proof of physical address from individuals

---

861 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 325.

862 Motsi 2016 *Financial Regulations International* 8.

863 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 325.

864 Bester *et al* 2010 http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf.

865 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 325.

866 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 325.

867 Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/. An example of weak system controls can be found in the case where a Starbucks' software application allowed clients to pay at the checkout with points using their m-money application. Owing to unsecured and inadequate software applications used by Starbucks, hackers managed to gain access to a number of clients' accounts, loaded the Starbucks gift cards and transferred them to other illegal accounts.

868 Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 325.

869 For instance, during June 2016 the Standard Bank of South Africa confirmed a loss of R300 million in a credit card scam involving the withdrawal of cash using fictitious cards at various ATMs. Eyewitness news 2016 http://ewn.co.za/2016/05/23/Standard-Bank-confirms-R300m-lost-in-credit-card-scam.

situated in informal settlements creates absolute barriers to access to the financial market.[870] By using the informal market for sending money, which is solely based on trust, these individuals are in the vulnerable situation of being exploited; and it creates opportunities for fraud, theft and the crime prevention organisations in a market which is not regulated and where finding the money via a paper-tail becomes impossible. Bester *et al*[871] believe that the regularisation of undocumented migrants in South Africa is a contentious political issue and is viewed as another barrier.

De Kocker[872] cautions that the risk profile of low-risk products, such as m-banking transactions, should be subject to reviews as criminals identify vulnerabilities within the system to circumvent controls. It is interesting to note that in respect of low-risk clients or products, the risk-based methodology banks currently does not require it to do an annual review of a client's profile and/or conduct transaction monitoring. Confirmed low-risk clients or products are only reviewed between three to five years, with no system monitoring. This elevates the risks that dated client or product information is used to mitigate ML/TF risks, allowing opportunities for criminals to abuse the system until the next client review.

An assessment of the practical implication of GN 6[873] indicates that any relaxation of the legislative requirements (i.e. CIV in terms of section 21 of *FICA*) would necessitate a more stringent application of control measures (e.g., third-party verification, biometrics, transaction monitoring) by the accountable institution in terms of section 42[874] of *FICA.* The reality is that should a bank elect to offer GN 6[875]

---

870 Bester *et al* 2010 http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf.

871 Bester *et al* 2010 http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf.

872 De Koker 2009 *Journal of Money Laundering Controls* 333-334.

873 South African Reserve Bank 2016 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/7080/G1%20of%202016.pdf.

874 Section 42 read with regulations 25, 26 and 27 of *FICA* of 38 of 2001-requires accountable institutions to formulate, document and outline clear standards (i.e., expected processes) step-by-step working methods that are to be followed by employees when dealing with exemptions to *FICA* of 38 of 2001, which requires an alternative approach to be followed which is not documented in the legislation. Saksenberg *et al*. (2008) *FICA Training Manual* 117 -118.

875 South African Reserve Bank 2016 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/7080/G1%20of%202016.pdf.

and/or Exemption 17[876] accounts it will, based on the additional AML/CFT controls applied, incur added costs for the bank and ultimately its clients. The costs include, but are not limited to, the employment of additional staff and implementation of transaction-monitoring systems that would, *inter alia*, alert the bank if a client has exceeded the permissible transaction threshold limits[877] or possible abuse of the account. In May 2015, Thomas Reuters[878] published its Annual Cost of Compliance Survey, which highlighted the sheer volume of regulatory costs incurred by entities in complying with both international standards and domestic legations. The following are the key findings identified:[879]

- Owing to snowballing regulations and being held accountable admits an ever-escalating volume of ever-changing legislation,[880] the expectation of being conversant and added pressure of possible administrative sanctions have augmented regulatory fatigue by compliance officers; and

- The sheer value of work could cause a rise in personal liability by compliance officers.[881]

Phil Cotter,[882] Managing Director of Thomson Reuters, concluded that the survey indicated that any entity who wished to thrive would have to consistently invest in risk management and control functions. Clients would bear the cost for the purpose

---

876 *FICA* of 38 of 2001.

877 For example, in terms of Exemption 17(1) to (5) of *FICA* 38 of 2001, the payments of an amount not exceeding R5 000.00 per day and not exceed R25 000.00 in monthly cycle.

878 Thomas Reuters 2015 http://thomsonreuters.com/en/press-releases/2015/05/cost-of-compliance-survey-shows-regulatory-fatigue-resource-challenges-personal-liability-to-increase.html-surveyed nearly 600 entities form financial services firms (i.e., banks, insures, brokers and asset managers) from Africa, Americas, Asia, Australia, Europe and the Middle East.

879 Thomas Reuters 2015 http://thomsonreuters.com/en/press-releases/2015/05/cost-of-compliance-survey-shows-regulatory-fatigue-resource-challenges-personal-liability-to-increase.html.

880 For instance, the *Financial Intelligence Centre Amendment Bill, Cybercrime and Cybersecurity Bill* and *The Financial Sector Regulations Bill* (i.e., Twin Peaks model) all expected to be signed, promulgated and ready for implementation at the end of 2016.

881 Section 45C(3)(e) of *FICA* 38 of 2001.

882 Thomas Reuters 2015 http://thomsonreuters.com/en/press-releases/2015/05/cost-of-compliance-survey-shows-regulatory-fatigue-resource-challenges-personal-liability-to-increase.html-surveyed nearly 600 entities form financial services firms (i.e., banks, insures, brokers and asset managers) from Africa, the Americas, Asia, Australia, Europe and the Middle East.

of financial inclusion for low-income individuals. This could not be what was envisaged in the spirit of financial inclusion.

## 12 Concluding remarks

The ultimate purpose of the application of CDD is to provide a foundation for banks to understand their clients' potential exposure to ML/TF risks.[883] The effectiveness of m-banking transactions is primarily influence by the application of CDD obligations.[884] The extent to which AML/CFT regulations are applied depends on the vulnerabilities of ML/TF risks that mobile transactions pose. Notwithstanding the control measures applicable to Exemption 17 and/or GN 6 accounts, these accounts are not immune to ML/TF abuse[885] and could be used as a secondary account or even a primary account for the transfer of illicit funds.[886] These funds could easily be accessed via different ATMs.[887]

Although m-banking transactions create a remittance channel that increases trust in the banking system, it is not without regulatory challenges.[888] Without a standardised approach to what is regarded as acceptable CDD documentation by both banks and

---

883 Demetriades 2016 *Journal of Money Laundering Control* 88.

884 Sections 21 and 23 read with regulations 3 to 20 of *FICA* of 38 of 2001, ss 39 and 40 of *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002, ss 4 to 6 of the *Prevention of Organised Crime* Act 121 of 1998 and so on; Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 331.

885 Starbucks processes 7 million mobile money transactions a week and aims to play a significant role and wants to leverage the equity of its brand in the way people effect payments (Sullivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/ ; During April 2013 the federal prosecutors of New York reported the arrest of seven suspects involved in the biggest, "surgical" cyber bank heist which, *inter alia*, involved 40 50 ATM withdrawals and 17 pre-paid credit cards. Approximately USD 45 million was stolen and some of the funds were laundered in buying Rolex watches-Weber 2013 http://theweek.com/articles/464499/great-atm-heist-how-thieves-brazenly-stole-45-million-few-hours; Reuters 2016 http://reuters.com/ article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB. AT the end of May 2016 criminals managed to counterfeit Standard Bank credit cards and withdraw 1.4 billion yen (approximately USD 3 million) via 14 000 transactions using ATM machines.

886 De Koker 2009 *Journal of Money Laundering Control* 330.

887 Reuters 2016 http://reuters.com/article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB- During end May 2016 criminals managed to counterfeit Standard Bank credit card and withdraw 1.4 billion yen (approximately USD 3 million) via effecting in 14 000 transactions using ATM machines.

888 Bester *et al* 2010 http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf.

telecommunications providers, clients are left feeling frustrated and confused. This does not contribute to support for AML/CFT efforts. Furthermore, the duplication or triplication of regulators in the areas of banking and telecommunications does not enhance legal certainty and transparency; it simply highlights vulnerabilities, and displaces ML and TF activities.[889]

On the eve of the signing of the new *Financial Intelligence Centre Amendment Bill* and a strong reliance on the application of an RBA to AML/CFT, domestic legislation might prove to be more flexible in the spirit of financial inclusion, but at the cost of what or to whom? In pursuit of financial inclusion and a cashless environment, payment transfer via m-banking, data storage card and Internet connections inadvertently benefits financial crime.[890]

A more integrated approach to information and knowledge sharing between different law enforcement agencies should take place in order to be more effective.[891] FATF echoed the same sentiments in its 2013 paper[892] on corruption. FATF Recommendation 18 encourages financial organisations to implement group-wide policies and procedures for sharing information for AML/CFT purposes.[893]

889 Stokes 2013 *Banking and Financial Service Policy Report*.

890 Thomas Reuters 2015 https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/ risk/expert-talk/financial-inclusion-initiatives-money-launderers-playground-expert-talk.pdf.

891 Chaikin and Sharman *Corruption and Money Laundering: A Symbiotic Relationship* 6, 115 to 118.

892 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/ recommendations/BPP-Use-of-FATF-Recs-Corruption.pdf.

893 Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/BPP-Use-of-FATF-Recs-Corruption.pdf.

# CHAPTER 6

# RESEARCH SUMMARIES, CONCLUSIONS AND RECOMMENDATIONS

*The challenges technology presents continues to beat even the best legal minds in the world.* [894]

## 1 Dissertation summary and general conclusion

Strong, stable and transparent economies and financial markets are built on effective and sound payment systems. The emergence of new financial ecosystems known as MNOs,[895] with products such as m-money, have proven itself to increase financial inclusion for those individuals living in low-income who do not have access to traditional banking. Conversely such innovations create numerous opportunities for criminals who have identified weaknesses within the financial system.

As explained in chapter 1, this study was born out of the need to assess the effectiveness of the legal and regulatory framework in the application of the simplified CDD principle pertaining to m-banking transactions. It also set out to examine whether this presumably low-risk product, client or transactions, the application of an exemption (i.e. SDD) to the CIV requirements for low-income individuals, and in the spirit of financial inclusion, do indeed mitigate potential ML and TF risks. Though qualitative research this study provided a comprehensive overview of the legal, regulatory and technical challenges facing the application of AML/CFT controls within innovative financial services technologies, such as emerging m-banking technologies. In order to achieve this, an almost all-inclusive AML/CFT international standards and domestic legislative analysis approach to the problem statement was followed. The technical application of m-banking within the financial sector was reviewed and examples of new ML/TF vulnerabilities within m-banking transactions were highlighted. This study therefore examined whether within the current application of South Africa legislation mobile transactions could be used as a

---

894 Justice Michael Kirby 2007 https://cnet.com/news/judge-on-privacy-computer-code-trumps-the-law/.

895 Mobile Network Operators operate the uses of mobile airtime currency which is prefunded electronic stores of value which is housed in stored value accounts on a mobile phone, subject to s 1 of the *Banks Act*.

medium of laundering money, due to its low-risk status, through the acceptance and storage of individuals' funds and the transfer thereof to mobile phones.

This study has found the following:

1. The literature review of the concepts such as money, legal tender, unbanked, branchless banking, e-banking, m-banking, m-money, ML and TF in Chapter 2 confirmed that m-banking activities fall within the ambit of prudential supervision, including the oversight of banking business activities.[896] I noted that the commercial application of the term "m-money" lacks a universal approach due to the constant evolution of the product or service in the virtual world of transacting. Although various forms of e-banking[897] amount to "money", from the assessment of traditional approaches followed and based on the legal requirements of money set out in the *locus classicus* of *Spratt v Hobhouse*[898], *Moss v Hancock* [899] (hereinafter the *Moss*) and *Miller v Race* [900] (hereinafter the *Miller*), it can be deduced that the traditional legal methodologies applied to money have not kept abreast with the emergence of intangible, dematerialised and sometimes decentralised new payment technologies fighting to be recognized as "money". For instance, in the *Moss* and *Miller* cases, money was based on a quantitative, tangible and economic approach which followed the Orthodox[901] economic theory. Conversely, Du Toit[902]'s approach accepts that property law guides the way we think about money. From the analysis of the transformation that the concept of money has undergone, it can be argued that it has reached a doctrinal misalliance

---

896 Webb 2010 *Journal of Banking Regulations* 129.

897 Electronic banking can be defined as "provision of retail and smaller value banking products and services through electronic channels", as described in Basel Committee on Banking Supervision 1998 http://bis.org/publ/bcbx35.pdf.

898 (1827) 4 Bing 179.

899 (1899) 2 QB 111 116.

900 (1758) 1 Burr 452.

901 Law *Money and Trade Considered* 6-8. The Orthodox School economists define money as anything which can be expressed as a standard unit to which store value (a price or debt can be measured) and is widely accepted in payment of goods. While Geva and Kianieff 2005 http://goo.gl/QfR4y did not agree with Mann's inclusion of a tangible thing, for instance a chattle, in the definition of money, they agreed with the appropriation of an economic definition to money by law, however, failed to analyse what is meant by "tangible".

902 Du Toit 2009 *TSAR* 1-2.

between the common law and Orthodox economic approach to money. I have noted that the focus has shifted from the concept of money to new innovative payment systems, which are essentially intangible.

Kendall[903] suggests that the transient, transactional nature of m-money transactions transforms the fundamental notion of a "deposit". As already noted in chapter 2, "deposit-taking" is the key element differentiating the "business of a bank". However, in the case of m-money transactions, "money" is transformed from an acceptance of physical funds into a transient source, which is used for transactional system-based payments. I have also noted that the multifaceted nature of m-banking transactions, based on contracts between participants, requires the immersion of multiple players such as financial institutions, payment systems providers and telecommunications representatives. The reality is that not all these players fall within the ambit of banking, and by default under AML and CFT regulation and supervision. It further follows that it could be proposed that the value received and stored on a mobile phone and the entities involved in the process of sending and receiving funds fall outside the ambit of the "business of a bank",[904] which is limited to a bank-only policy approach.[905]

2. From the analysis of the new and various types of illicit[906] uses of digital money such as m-money (e.g. digital smurfing, fraud, mulling, drug financing

---

903 Kendall and Machoka 2011 http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/ssrnid1830704.pdf.

904 Section 11 of the *Banks Act*.

905 Section 91(8) of the *Banks Act*. The taking of deposits, which also includes soliciting a deposit, from the general public by an unregistered person (non-bank) is regarded as a criminal offence.

906 Starbucks processes 7 million mobile money transactions per week and aims to play a significant role and want to leverage the equity of their brand in the way in which people effect payments – Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/. During April 2013 the federal prosecutors of New York reported the arrest of seven suspects involved in the biggest, "surgical" cyber bank heist, which inter alia involved 50 ATM withdrawals and 17 pre-paid credit cards. Approximately USD 45 million was stolen and some of the funds were laundered in buying Rolex watches - Weber 2013 http://theweek.com/articles/464499/great-atm-heist-how-thieves-brazenly-stole-45-million-few-hours and Reuters 2016 http://reuters.com/article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB. During the end of May 2016 criminals managed to counterfeit Standard Bank credit cards and withdraw 1.4 billion yen (approximately USD 3 million) by effecting 14 000 transactions using ATM machines.

etc.) discussed in Chapter 3, the study found that it has become increasingly difficult to "follow the money" in a digital world. The synergy between and anonymity associated with mobile, telecommunications, banking and digital payment systems have opened the doors to financial participation for the economically deprived,[907] but at the same time created opportunities for criminals to avoid detection working in the shadows of a virtual world. The proliferation of intelligence held in the SIM card of a mobile phone, which stores the value of the mobile account, has shifted conventional m-banking transactions to invisible and faceless carriers.[908]

Chapter 3 confirms that the nature of banking is changing and as such the traditional lines between players within the banking and non-banking sphere are becoming increasingly blurred and ambiguous. The fact that whilst new payment systems such as m-money transactions have reduced the inherent risks of a cash-based system, the elusiveness, anonymity, low risk rating, high marketability, global access to bank networks and poor supervision are all vulnerabilities that money launderers will use to their advantage.[909] The application of effective and financially inclusive AML/CFT measures is vital in protecting the safety and soundness of banks, and the integrity of international financial systems.[910]

3. Following in the footprints of a risk-based approach, chapter 4 confirmed that the use of soft law, such as that "prescribed" by the FATF Recommendations and the Basel Committee's Core Principles for Banking Supervision supports the banking industry and provides it with the necessary discretion to design their own financial services model, and AML and CFT regulations based on domestic legislation[911] without stifling beneficial innovation.[912] Stemming from

---

907 Demombynes and Thegeya 2012 http://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5988.

908 Vlcek 2011 *Development Policy Review* 424.

909 Solin and Zerzan 2010 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/amlfinal35.pdf.

910 Basel Committee on Banking Supervision 2014 http://bis.org/press/p140115.htm.

911 Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf and Financial Action Task Force 2013

the above it can be deduced that South African banking law and *FICA* are influenced by FATF and the Basel Committee's international standards. Domestic legislation is implicitly bound by these recommendations. Conversely, the exchange of information through the use of SIM cards held in smartphones causes the virtual world of international m-banking to add an extra layer of complexity. It accordingly becomes vexing to establish how and which jurisdictions have authority and criminals are taking advantage of this space of uncertainty and lack of oversight.

4. In chapter 5 it was noted there are essentially two non-exclusive legislative approaches to AML/CFT, namely the role of prevention through the application of a standardised disclosure approach of CIV, and the liability consequences (e.g. reputational risks, administrative sanctions etc.) for non-adherence thereto. It is quite clear that the ultimate purpose of the application of CDD is to provide a foundation for banks to understand their clients' potential exposure to ML/TF risks.[913] The effectiveness of m-banking transactions is thus primarily influenced by the application of CDD obligations.[914] Conversely, the extent to which AML/CFT regulations are applied will depend on the vulnerabilities of ML/TF risks mobile transactions pose. Exemption 17 of *FICA* regulations and GN 6 permit banks to open m-banking accounts for only client-facing individuals, with South African national identity documents being a requirement, subject to prescribed transactional amount limits (i.e. not exceeding R5 000.00 per day and not exceeding R25 000.00 in a monthly cycle).[915] Stemming from the above, it would appear that most of the provisions contained in *FICA* require amounts "sounding" in money. Consequently, it could be interpreted that these provisions do not inevitably

---

http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

912 Huang *The Law and Regulation of Central Counterparties* 129-130.

913 Demetriades 2016 *Journal of Money Laundering Control* 88.

914 Sections 21 and 23 read with regulations 3 to 20 of *FICA* of 38 of 2001, ss 39 and 40 of *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002, ss 4 to 6 of *Prevention of Organised Crime* Act 121 of 1998 etc. and Lawack-Davids 2012 *Journal of International Commercial Law and Technology* 331.

915 Section 21 read with Exemption 17 of *FICA* 38 of 2001.

include the scope of non-money airtime value being transferred via a mobile phone, on a domestic or cross-border level.

Although m-banking transactions create a remittance channel that increases trust in the banking system, it is not without regulatory challenges.[916] Without a standardised approach to what is regarded as acceptable CDD documentation by both banks and telecommunications providers, clients are left feeling frustrated and confused. This does not contribute to the support of AML/CFT efforts. Furthermore, the duplication or triplication of regulators within the areas of banking and telecommunications does not enhance legal certainty and transparency, but simply highlights vulnerabilities and transfers ML and TF activities from one player to another.[917]

From my analysis of South African domestic legislation and the introduction of innovative financial service technologies, such as emerging m-banking technologies, I have noted that legislative and compliance risks develop outside the ambit of current legislation. As such the South African law in this regard is not entirely codified and aspects of soft law are not legislated. This is also echoed in the amendments to the *FIC Amendment Bill*. As such the ever-changing multi-faced and multi-doctrinal nature of these new entrants into the financial markets has revealed the law and policymakers to be ill prepared. The untested nature of new innovative technologies (i.e. software applications within the SIM card) exposes the regulatory void and equivocation in the application of AML/CFT legislation, especially where regulations and supervision are absent or unable to effectively regulate the system due to the duplication of supervision by the financial sectors and telecommunications industry (e.g. CIV application applied in *FICA* vs *RICA*. It is, however, posited that the application of a legislatively required risk-based approach might mitigate the regulatory void. This would become a key approach should the

916 Bester *et al* 2010 http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf.

917 Stokes 2013 *Banking and Financial Service Policy Report*.

new *FIC Amendment Bill* retract any exemptions (e.g. Exemption 17) afforded under the current *FICA*.

## 2 Recommendations

Stemming from the extensive discussions contained within the respective chapters of this study, the following recommendations are made:

1. The evolution of transactional banking necessitates a re-evaluation of the concepts "deposit-taking" and "business of a bank" as it is conceded that reference to transactional banking should not ineludibly denote deposit-taking. In terms of the nature of "deposit-taking", as a trigger for the "business of a bank", it is proposed that these concepts should be transformed from the narrow parameters of the common law towards a more practical, subjective and transactional payment approach. This would cause most new innovative payment activities to fall within the ambit of the "business of a bank" and be subject to the application of AML/CFT regulations and supervision.

2. In terms of sections 11 and 12 of the *POPI Act;*[918] clients can consent to the exchange of information between MNOs and banks. It has been noted that the *Banks Act* GN6 provided for cross-referencing of the client's information against a third-party database, which is not limited to the Department of Home Affairs.[919] Notwithstanding the misalignment of identification and verification standards between *FICA* and *RICA* and in the spirit of co-operation,[920] banks could make use of the *RICA* database to assist with *FICA* verification[921] and/or transaction monitoring. It could be proposed that the supervisors of *FICA* and *RICA* could enter into a co-operative and information

[918] *Protection of Personal Information Act* 4 of 2013.

[919] South African Reserve Bank 2006 https://resbank.co.za/Lists/News%20and%20Publications/Attachments/3058/banks%20act%20circ%206%20of%202006.pdf and de Koker 2009 *Journal of Money Laundering Control* 327.

[920] Principle 3 of the Egmont Group Principles described "cooperation" as the free exchange of information for the purposes of analysis on a FIU level and protection of confidentiality of information. - Egmont Group 2013 https://egmontgroup.org/library/download/290 and OECD 1994 http://oecd.org/pdf/M000014000/M00014640.pdf.

[921] De Koker 2010 http://cenfri.org/documents/Financial%20inclusion/2010/RICA%20impact%20on%20financial%20inclusion_final.pdf.

exchange agreement to establish a CIV hub for the purpose of identification and verification of individual information through a trusted third-party source. This would mitigate the stringent account-opening process of obtaining documentation from clients, and enhance financial inclusion for the low-income individuals who are not in a position to provide the required documents due to the difficulty of providing proof of address in informal settlements.

In the m-banking space, banks do not always have a full view of the information of the counterparty to the transactions because CDD requirements are only applicable to bank clients. By having limited access to information contained within the ambit of *RICA* systems and for the purpose of AML/CFT, the banking sector would be in a position to identify any anomalies of syndicate or mulling schemes, because they would know who the counterparty to the transaction is.

3. Several useful recommendations have been made in this study as to how a risk-based approach may be applied to be in a position to understand, identify, classify and manage the risk with existing resources. As no risk is absolute, it is important to note that once a bank has defined, developed and implemented its own risk-based approach and matrix, it should monitor the risks to ensure that it aligns with the ever-changing market, products and criminal environment.

4. It is posited that based on the assumption that South Africa's *FICA* would appear to regulate and supervise values "sounding in money" that the *FIC Amendment Bill* may need to be amended to include values that do not inevitably and explicitly amount to money, such as m-money transactions or loyalty points (e.g. Standard Bank Limited's U-count reward programme or FirstRand Bank Limited's Ebucks).

## 3 Implications for further research

This study did not deal with the quantitative or qualitative assessment of ML/TF risks within m-banking transactions. Furthermore, Lawack[922] acceded that she could not find any documented, formal risk assessment relating to m-money. Understanding and identifying the actual ML/TF risks within m-money truncations are accordingly key in designing ML/TF controls which would effectively target these threats.

Although this study may have alluded to the economic, financial, telecommunication and political factors which could influence the growth in m-banking,[923] they were not discussed or examined in detail. It might be interesting to do a comparative study relating to the observations made between the successes of m-banking in Kenya compared to South Africa's MTN Mpesa service.

## 4 Concluding remarks

The aim of this study was to determine to what extent, if any, presumably low-risk products such as m-banking transactions and the application of an exemption to the CIV requirements, in the spirit of financial inclusion, could make it susceptible to ML and TF risks. As a result, this study provides a comprehensive review of the international and domestic legislative and regulatory frameworks applicable to m-banking transactions. Although the legislative and regulatory frameworks are found to be fairly sound, specifically relating to the control measures applicable to Exemption 17 of *FICA* Regulations and/or Banks Act GN6 accounts, it has been found that these accounts are not immune to ML/TF abuse. It could be used as a secondary account or even a primary account for the transfer of illicit funds.[924]

The shift in low-value cash transactions from a physical to a digital format provides a better platform for monitoring and tracing illegal proceeds of crime.[925] As such, m-money reduces the dependency on cash and generates an array of data on client habits and transactions, which through integrated analytics can be used to identify

---

922 Lawack 2013 *Washington Journal of Law, Technologies and Arts* 341-342.
923 Kleijnen *et al* 2004 *Journal of Financial Services Marketing* 205-208.
924 De Koker 2009 *Journal of Money Laundering Control* 330.
925 Di Castri *et al* 2015 http://gsma.com/mobilefordevelopment/wp-content/uploads/2015/10/Proportional-risk-based-AMLCFT-regimes-for-mobile-money.pdf.

and flag suspicious transitions. This could enhance the purpose of AML/CFT controls, which are based on effective and proportional risk management without being unduly rigorous.[926] The information contained in the data could be shared with law enforcement in an effort to mitigate financial crime, ML and TF.

On the proverbial eve of the signing of the new *FIC Centre Amendment Bill* and a strong reliance on the application of a risk-based approach to AML/CFT, the domestic legislation might prove to be more flexible to the spirit of financial inclusion, but at what cost to whom? In the pursuit of financial inclusion and a cashless environment, payment transfers via m-banking, data storage cards and internet connections might prove to be also beneficial for financial crime.[927] Furthermore, AML/CFT controls found in *FICA* are limited to the establishment of a business relationship or concluding a single transactions[928], which jurisdiction has no bearing on data stored on a card.

Stemming from the above, this study concluded that m-banking transactions are not immune to financial crime, and AML and CFT activities. Furthermore, the ever-changing multi-faced and multi-doctrinal nature of innovative payment systems such as m-banking transactions has revealed the law and policymakers to be ill prepared. In this age of globalisation the need for rapid mobility of funds forces legislators to move into the unknown and change their approach to codifying legislation at the same pace as the evolution of innovative payment systems.

The nature of banking is changing. If legislation, regulation and supervision in the sphere of AML/CFT do not adapt, criminals will, and indeed already have.

---

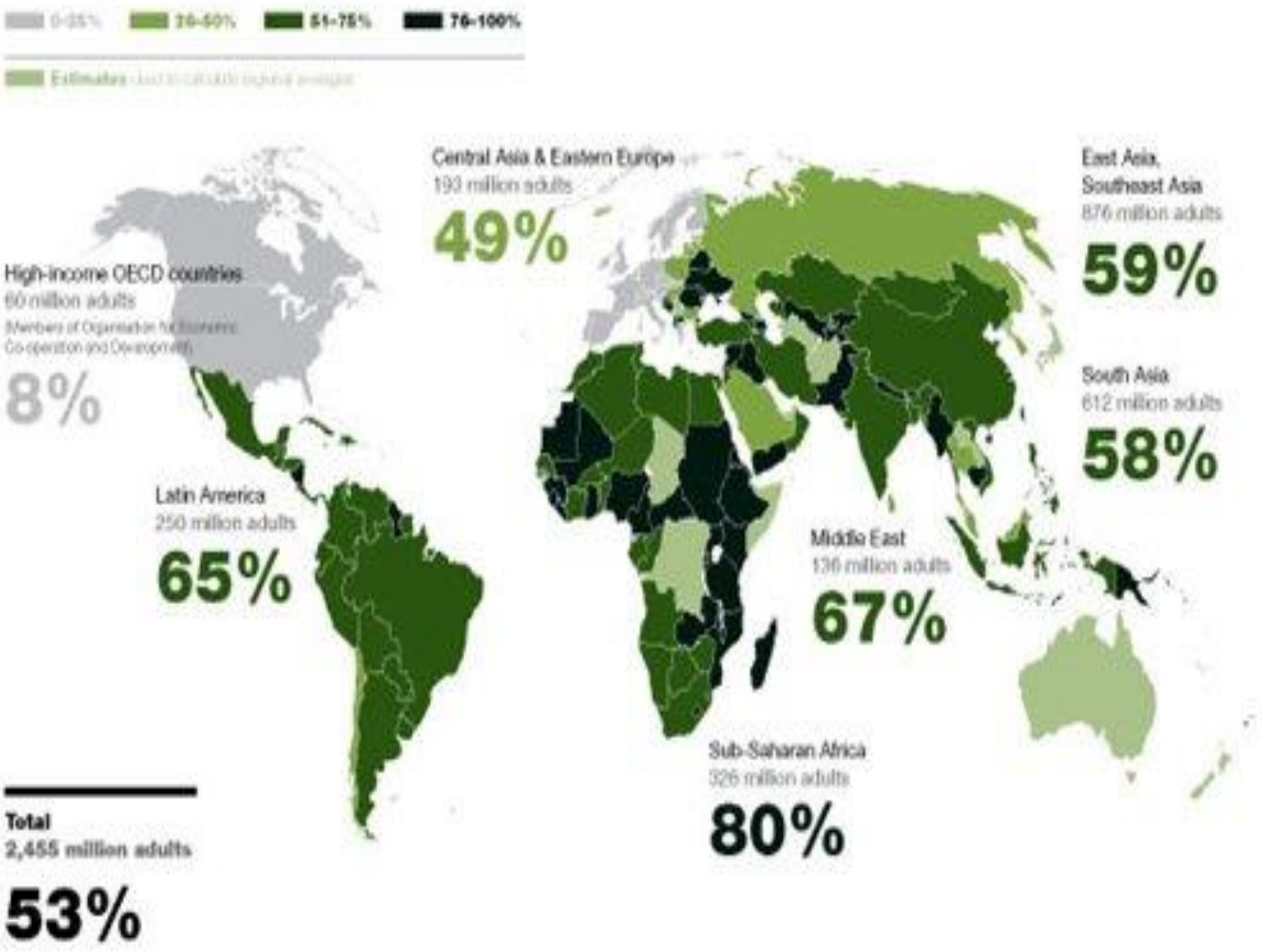
926 Di Castri *et al* 2015 http://gsma.com/mobilefordevelopment/wp-content/uploads/2015/10/Proportional-risk-based-AMLCFT-regimes-for-mobile-money.pdf.

927 Thomas Reuters 2015 https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/expert-talk/financial-inclusion-initiatives-money-launderers-playground-expert-talk.pdf.

928 Section 21 of *FICA* 38 of 2001.

**Annexure 2.1.**

**Diagram 1: Percentage of total adult population who do not use formal or semiformal services[929]**



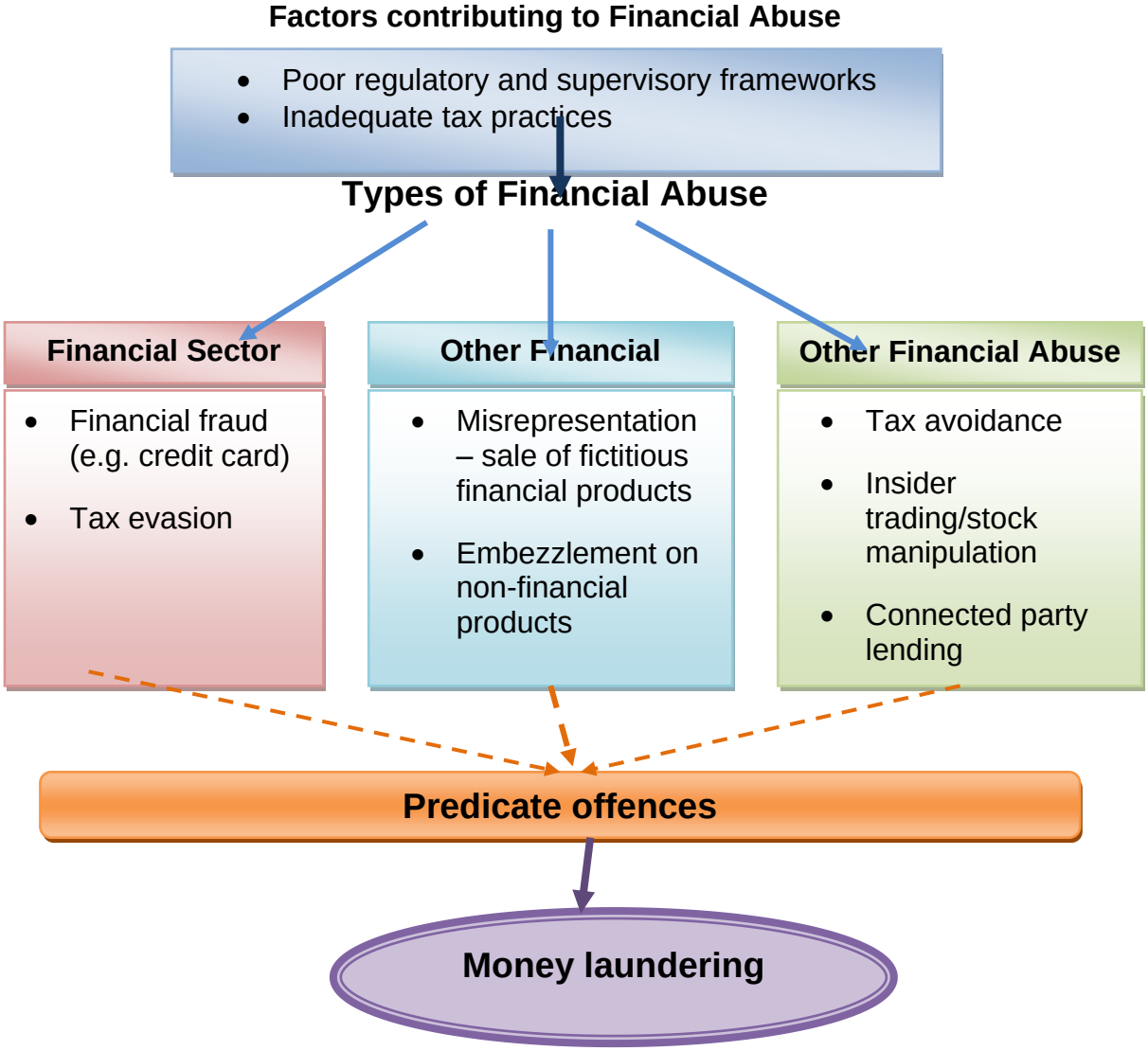

Key findings from the above and the report clearly illustrate that nearly half the world's adult population is unserved, of which 62% (2.2. billion) reside in Latin America, Africa, Asia and the Middle East. The report also highlighted that about 800 million individuals live on less than USD 5 per day.[930]

929 Chaia, Goland and Schiff 2010 http://mckinseyonsociety.com/downloads/reports/Economic-Development/Half_the_world_is_unbanked.pdf.

930 Chaia, Goland and Schiff 2010 http://mckinseyonsociety.com/downloads/reports/Economic-Development/Half_the_world_is_unbanked.pdf.

**Annexure 2.2.**

**Diagram 2: Concepts of Financial Abuse**[931]




[931] International Monetary Fund 2001 http://imf.org/external/np/ml/2001/eng/021201.pdf.

**Annexure 4.1.**

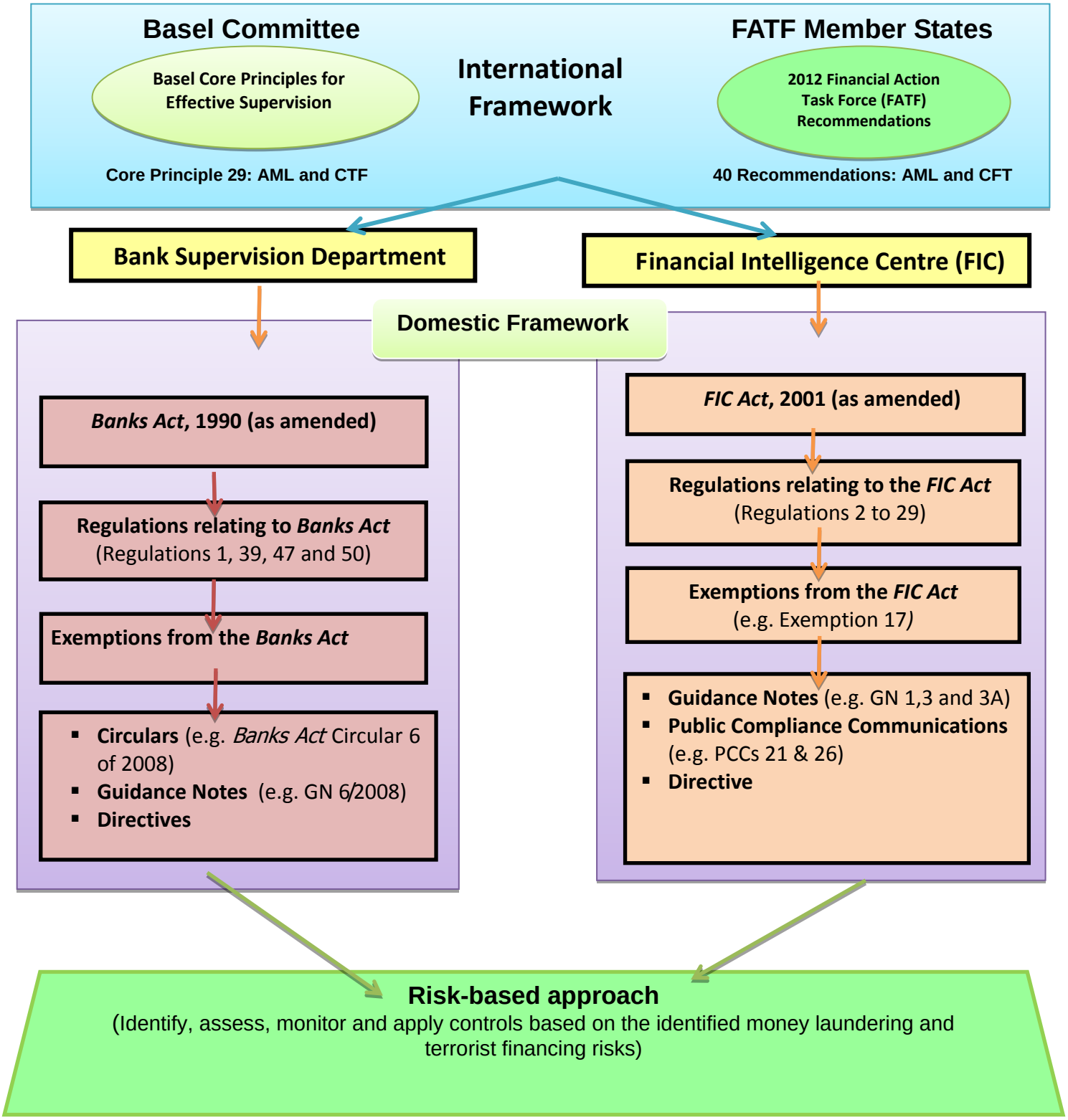
## Table 1: Regulatory methodologies[932]

| Methodologies | Advantages | Weaknesses |
|---|---|---|
| *Lex lata*<br><br>(Wait-and-see approach) | 1. Avoids rigid regulations that could hamper development of new technologies.<br>2. Maintains expertise in products or service and development.<br>3. Allows for monitoring of potential issues. | 1. Uneven playing field for existing financial institutions that have to adhere to rigid legislation compared to the retail market which is not regulated.<br>2. Lack of a clear legal framework may result in market entry being slow.<br>3. Risks of fraud, identity theft and unfair practices. |
| *Lex ferenda*<br><br>(Advance approach) | 1. Pre-empts the challenges of undesirable situations such as financial crime, reputational, AML/CFT risks.<br>2. Takes into account existing payment systems.<br>3. Recognises international organisations (i.e. FATF and Basel Committee), academic and market debates on the pros and cons of new innovative payment technologies. | 1. Requires a distinction between different role player (banks, cell phone operators, retailers) and the impact on the existing regulatory framework.<br>2. All information regarding risks and opportunities are not available in the inception phase of the new innovative payment products or services. |

[932] Mboweni 1999 http://bis.org/review/R9991013b.pdf; Mann *The Legal Aspect of Money: With Special Reference to comparative Private and Public International Law* 4th ed. 8; Delston and Walls 2009 *Case W. Res J.INT'L L.* 89-90 and Mann 2004 TLR 703 – 704.

**Annexure 5.1.**

## South Africa's regulatory framework



## Bibliography

### Literature


Aker and Mbiti 2010 *Journal of Economic Perspectives*

Aker J and Mbiti I "Mobile Phones and Economic Development in Africa" 2010 *Journal of Economic Perspectives* 207-232

Alexandre and Eisenhart 2013 *Washington Journal of Law, Technology and Art*

Alexandre C and Eisenhart LC "Mobile Money as an Engine of Financial Inclusion and Lynchpin of Financial Integrity" 2013 *Washington Journal of Law, Technology and Art* 285–301

Ali 2012 *Journal of Money Laundering Controls*

Ali l 2012 " ”Rule-based but risk-oriented” approach for combating money laundering in Chinese financial sectors" *Journal of Money Laundering Controls* 201

Al-Jabir 2012 *Journal of Electronic Commerce Research*

Al-Jabir 2012 "Mobile banking adoption: application of diffusion of innovation theory" *Journal of Electronic Commerce Research* 379-380

Benjamin *The Future of Global Currency: The Euro versus the Dollar*

Benjamin JC *The Future of Global Currency: The Euro versus the Dollar.* (Routledge New York 2011)

Booyens *Legal Perspective on the Risks Relating to Internet Banking*

Booyens A *A Legal Perspective on the Risks Relating to Internet Banking* (LLM dissertation University of Johannesburg 2014)

Carruthers and Espeland 1998 *American Behavior Scientist*

Carruthers BG and Espeland WN "Money, Meaning and Morality" 1998 *American Behavior Scientist* 1374-1375

Chaikin and Sharman *Corruption and Money Laundering: A Symbiotic Relationship*

Chaikin D and Sharman J *Corruption and Money Laundering: A Symbiotic Relationship* (Palgrave MacMillan New York 2009) 31-33

Chaix and Torre "Which economic model for mobile payments?"

Chaix L and Torre D "Which economic model for mobile payments?" *23rd European Regional Conference of the International Telecommunication Society* (1 – 4 July 2012 Vienna, Austria) 1-22

Chatain *et al Protecting Mobile Money against Financial Crime*

Chatain P *et al Protecting Mobile Money against Financial Crime* (The World Bank Washington DC 2011) xiii-xxx and 1

Chong and López-de-Silanes *Money Laundering and its Regulations*

Chong A and López-de-Silanes F *Money Laundering and its Regulations* (Inter-American Development Bank, Banco Interamericano de Desarrollo (BID) Research Department Working Paper 590, University of Amsterdam, Inter-American Development Bank and NBER, 2009) 11-13

De Koker 2004 *TSAR*

De Koker L "Client identification and money laundering control: Perspective on the Financial Intelligence Centre Act 38 of 2001" 2004 *TSAR* 715-741

De Koker 2006 *Journal of Financial Crime*

De Koker L "Money laundering control and suppression of financing of terrorism: Some thoughts on the impact of client due diligence measures on financial exclusion" 2006 *Journal of Financial Crime* 26-50

De Koker 2009 *Journal of Money Laundering Control*

De Koker L "The money laundering risks posed by low risk finance products in South Africa" 2009 Journal of Money Laundering Control 323-339

De Koker 2013 *Washington Journal of Law, Technology and Arts*

De Koker 2013 "The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework" *Washington Journal of Law, Technology and Arts* 167-169

De Koker *South African Money Laundering and Terror Financing Law*

De Koker L *South African Money Laundering and Terror Financing Law* (LexisNexis Group Durban 2015) 51

Delston and Walls 2009 *Case Western Reserve Journal of International Law*

Delston RS and Walls SC "Reaching beyond Banks: How to Target Trade-Base Money Laundering and Terrorist Financing Outside the Financial Sector" 2009 *Case Western Reserve Journal of International Law* 85–118

Demetriades 2016 *Journal of Money Laundering Control* 80.

Demetriades G " "Is the person who he claims to be?" Old fashioned due diligence may give the correct answer!" 2016 *Journal of Money Laundering Control* 79-91

Demombynes and Thegeya 2012 *World Bank Policy Research Working Paper No 5988*

Demombynes G and Thegeya "A Kenya's Mobile Revolution and the Promise of Mobile Savings" 2012 World Bank Policy Research Working Paper No 5988

Du Toit 2009 *Tydskrif vir die Suid-Afrikaanse Reg (TSAR)*

Du Toit S "Die Dematerialisasie van Geld: In die Skadu van die Sakereg" 2009 *TSAR* 1-21

Ferguson 2008 *The Ascent of Money: A Financial History of the World*

Ferguson N *The Ascent of Money: A Financial History of the World* (The Penguin Press New York 2008)

Frederic *The Economics of Money, Banking and Financial Markets*

Frederic SM *The Economics of Money, Banking and Financial M*arkets 9th ed (Pearson Addison-Westley Boston 2010)

Fonte 2013 *Washington Journal of Law, Technology and Arts*

Fonte EF "Mobile Payment in the United States: How Disintermediation may Affect Delivery of Payment functions, Financial inclusion and Anti-Money Laundering Issues" 2013 *Washington Journal of Law, Technology and Arts* 419-456

Gillespie *et al* "Toward Electronic Money and Banking: The Role of Government"

Gillespie J *et al* "Toward Electronic Money and Banking: The Role of Government" Unpublished contribution delivered at the United States Department of the Treasury Conference (19 – 20 September 1996 Washington DC)

Gold 1997 *The American Journal of International Law*

Gold J "Interpretation: The IMF and International Law" 1997 *The American Journal of International Law* 405-407

Goode *Commercial Law*

*Goode Commercial Law 2nd ed* (Lexis Nexis Oxford 1995*)*

Goode and McKendrick *Goode on Commercial Law*

Goode R and McKendrick E *Goode on Commercial Law* 4th ed (Lexis Nexis London 2010)

Gramham, *et al* "Brussels terror attacks metro airport suspects live"

Gramham C, Rothwell J, Lawler D *et al* "Brussels terror attacks metro airport suspects live" *Telegraph* (26 March 2016)

Grotius *De Jures Belli* ii12.17

Grotius *De Jures Belli* ac Pric ii12.17

Huang *The Law and Regulation of Central Counterparties*

Huang J *The Law and Regulation of Central Counterparties* (Hart Publishing Oxford and Portland 2010)

Jun and Ai 2009 *Journal of Money Laundering Control*

Jun T and Ai L 2009 "The international standards of client due diligence and Chinese practice" *Journal of Money Laundering Control* 407-408

Jonathan & Camilo 2008 *Asian Journal of Communication*

Jonathan D & Camilo T "Mobile banking and economic development: Linking adoption, impact and use" 2008 *Asian Journal of Communication* 318-322

Kersop and du Toit 2015 *Potchefstroomse Electroniese Regsblad* 1615.

Kersop M and du Toit SF 2015 "Anti-money laundering regulations and the effective use of mobile money in South Africa – Part 1*" *Potchefstroomse Electroniese Regsblad* 1603-1627.

Kersop and du Toit 2015 *Potchefstroom Electronic Law Journal*

Kersop M and du Toit SF 2015 "Anti-Money Laundering Regulations and the Effective Use of Mobile Money in South Africa – part 2" *Potchefstroom Electronic Law Journal* 1637-1664

Keynes *The General Theory of Employment, Interest and Money*

Keynes JM *The General Theory of Employment, Interest and Money* (Harcourt-Brace-Jovanovich New York)

Khanna *Advanced Study in Mona and Banking: Theory and Policy Relevance in the Indian Economy*

Khanna P *Advanced Study in Mona and Banking: Theory and Policy Relevance in the Indian Economy* (Atlantic Publishers and Disturbers: New Delhi 2005) 16

Killick and Parody 2007 *Journal of Financial and Regulatory Compliance*

Killick and Parody 2007 "Implementation AML/CFT measures that address the risks and not tick boxes" *Journal of Financial and Regulatory* Compliance 210–215

Kleijnen *et al* 2004 *Journal of Financial Services Marketing*

Kleijnen M, Wetzels M and Ruyter K "consumer acceptance of wireless finance" 2004 *Journal of Financial Services Marketing* 205-208.

Kumar and Dutta 2015 *Economic and Political Weekly*

Kumar L and Dutta S 2015 "Role of Mobile Money in Replacing Cash – A Study Among Migrant Workers in South India" *Economic and Political Weekly* 38-40

Kocherlakota 1998 *Journal of Economic Theory*

Kocherlakota N "Money is Memory" 1998 *Journal of Economic Theory* 232-251

Lawack-Davids 2012 *JICLT*

Lawack-Davids VA "The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa" 2012 *JICLT* 318–327

Lawack 2013 *Washington Journal of Law, Technology and* Arts

Lawack VA 2013 "Mobile Money, Financial Inclusion and Financial Integrity: The South African Case" *Washington Journal of Law, Technology and* Art 324-338

Lawack 2013 *Washington Journal of Law, Technology and Arts*

Lawack VA "Mobile Money, Financial Inclusion and Financial Integrity: The South African Case" 2013 *Washington Journal of Law, Technology and Arts* 318-344

Malan, Pretorius and Du Toit *Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law*

Malan FR, Pretorius JT and Du Toit SF *Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law* 5th ed (Lexis Nexis Durban 2009)

Mankiw *Macroeconomics*

Mankiw NG *Macroeconomics* 7th ed (Worth Publishers New York 2010)

Mankiw *Principles of Economics*

Mankiw NG *Principles of Economics* (Harcourt College Publishers Florida 2014)

Mann 2004 *Texas Law Review*

Mann RJ "Regulating Internet Payment Intermediaries" 2004 *Texas Law Review* 681-716

Mann *The Legal Aspects of Money*

Mann FA *The Legal Aspect of Money: With Special Reference to comparative Private and Public International Law* 4th ed (University Press Oxford 1982) 8

Mann *The Legal Aspects of Money*

Mann FA *The Legal Aspects of Money* 5th ed (University Press Oxford 1992)

Masciandaro 1998 *Journal of Money Laundering Control* 49-58

Masciandaro D 1998 "Money Laundering Regulation: The Micro Economics" *Journal of Money Laundering Control* 49-58

McEachern *Economics: A Contemporary Introduction*

McEachern WA *Economics: A Contemporary Introduction* 8th ed (Southwest Cengage Learning Mason 2009) 622

Meikle 1994 *Journal for Ancient Philosophy*

Meikle S "Phornesis" 1994 *Journal for Ancient Philosophy* 26-44

Mehrling 2000 *Journal of Post Keynesian Economics*

Mehrling P "Modern Money: Fiat or Credit?" 2000 *Journal of Post Keynesian Economics* 397–406

Merlonghi 2010 *Journal of Money Laundering Control*

Merlonghi G "Fighting financial crime in the age of electronic money: opportunities and limitations" 2010 *Journal of Money Laundering Control* 202 – 214

Maurer 2012 *Banking and Finance Law Review*

Maurer B "Regulation as Retrospective Ethnography: Mobile Money and the Art of Cash" 2012 *Banking and Finance Law Review* 299-313

Motsi 2016 *Financial Regulations International* 8

Motsi I "Between Scylla and Charybdis: Lessons from comparative analysis of the regulation of Bitcoin in the US and UK" 2016 *Financial Regulations International* 8-16

Murgia Telegraph

Murgia M "How to protect yourself from SIM-swaps scams" Telegraph (28 September 2015) 1

Nassbaum 1937 *Michigan Law Review*

Nussbaum A "Basic Monetary Conceptions in Law" 1937 *Michigan Law Review* 865-907

Nussbaum *Money in the Law: National and International*

Nussbaum A *Money in the Law: National and International* (The Foundantion Press Inc Brooklyn 1950)

Okeahalam 2003 *Journal of Banking Regulation*

Okeahalam CC 2003 "Regulation of the Payments System of South Africa" *Journal of Banking Regulation* 338-348

Pinguelo and Muller 2011 *Virginia Journal of Law and Technologies*

Pinguelo M and Muller BW 2011 "Virtual Crimes, Real Damages: A primer on Cybercrimes in the United Sates and Efforts to Combat Cyber Crime" *Virginia Journal of Law and Technologies* 117-188

Phillips 2014 *Western New England Law Review*

Phillips AS "Bank-created money, monetary sovereignty and the federal deficit: Toward a new paradigm in the government-spending debate" 2014 *Western New England Law Review* 221-260

Popa 2012 *Metalurgia International*

Popa C "Money laundering using the internet and electronic payments" 2012 *Metalurgia International* 219-220

Rachagan and Kasipillai 2013 *International Company and Commercial Law Review*

Rachagan and Kasipillai "Money laundering and tax crimes in an emerging economy" 2013 *International Company and Commercial Law Review* 278-289

Saksenberg, Sptiz and Meyer *FICA Training Manual*

Saksenberg D, Sptiz B and Meyer C 2008 *FICA Training Manual* (LexisNexis Durban 2008) 38-39

Schäfer HB 2002 *German Working Papers in Law and Economics*

Schäfer HB "Legal Rules and Standards" 2002 *German Working Papers in Law and Economics* 1-2

Schumper *History of Economic Analysis*

Schumper J A *History of Economic Analysis* (Routledge Oxford 1952) 62-63

Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*

Schott PA *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (The World Bank Washington DC 2006)

Smith *Financial Mail*

Smith N "Twin Peaks Regulations: Climbing Lessons" *Financial Mail* (2 April 2015) 1

Souto 2013 *Journal of Money Laundering Control*

Souto MA "Money Laundering New Technologies, FATF and Spanish Penal Reform" 2013 *Journal of Money Laundering Control* 266-268

Stokes 2012 *Information and Communications Technology Law*

Stokes R "Virtual money laundering: the case of Bitcoin and the Linden dollar" 2012 *Information and Communications Technology Law* 224-227

Stokes 2013 *Banking and Financial Service Policy Report*

Stokes R "Anti-Money Laundering Regulations and Emerging Payment Technologies" 2013 *Banking and Financial Service Policy Report* 2-6

The European Parliament and Council 2005 *Official Journal of the European Union*

The European Parliament and Council "Directive 2005/60/EF of the European parliament and the Council: On the prevention of the use of financial systems for the Purpose of money laundering and terrorist financing" 2005 *Official Journal of the European Union,* paragraph 5

The International Bank for Reconstruction and Development, The World Bank and The International Monetary Fund *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*

The International Bank for Reconstruction and Development, The World Bank and The International Monetary Fund *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (The World Bank Washington DC 2006) I1–I6

Tiwari and Buse *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector*

Tiwari A and Buse S *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector* (Hamburg University Press Hamburg 2008)

Trautman 2014 *Richmond Journal of Law and Technologies*

Trautman L "Virtual Currencies: Bitcoin and What Now After Liberty Reserve, Silk Road and MT.Gox?" 2014 *Richmond Journal of Law and Technologies* 1-108

Unger and van Waarden 2009 *Review of Law and Economics*

Unger B and van Waarden F "How to Dodge Drowning in Data? – Rule- and Risk-Based Anti-Money Laundering Policies Compared" 2009 *Review of Law and Economics*

Unger The Gravity Model for Measuring Money Laundering and Tax Evasion 1-5

Unger B The Gravity Model for Measuring Money Laundering and Tax Evasion Workshop on Macroeconomic and Policy Implication of Underground Economy and Tax Evasion (5-6 February 2009 at Bocconi University, Milan, Italy) 1-17

Vaughan *Early lessons from the deployment of M-PESA, Vodafone's own mobile transactions service* contribution from Coyle *The transformational potential of m-transactions*

Vaughan P "Early lessons from the deployment of M-PESA, Vodafone's own mobile transactions service" 2007 contribution from Coyle D *The transformational potential of m-transactions* (Vodafone Group London) 6-9

Vlcek 2011 *Development Policy Review*

Vlcek W 2011 "Global Anti-Money Laundering Standards and Development Economies: The Regulation of Mobile Money" *Development Policy Review* 415-431

Von Hagen and Welker *Money as God? The Monetization of the Market aand it Impact on Religion, Policy, Law and Ethics*

Von Hagen J and Welker *M Money as God? The Monetization of the Market and it Impact on Religion, Policy, Law and Ethics* (Cambridge University Press Cambridge 2014)

Webb 2010 *Journal of Banking Regulations*

Webb RH Webb RH "Legal issues in Mobile Banking" 2010 *Journal of Banking Regulations* 129-145

Winn and de Koker 2013 *Washington Journal of Law, Technology and Arts*

Winn JK and de Koker L "Introduction to Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference Special Issue" 2013 *Washington Journal of Law, Technology and Arts* 155-164

White and Duram *America Goes Green: An Encyclopaedia of Eco-Friendly Culture in the United States*

White KK and Duram LA *America Goes Green: An Encyclopaedia of Eco-Friendly Culture in the United States* (ABC-CLIO Santa Barbara 2013) 389-390

White 1997 *Technological Change, Financial Innovation and Financial Regulation: The Challenges for Public Policy in the USA*

White LJ 1997 *Technological Change, Financial Innovation and Financial Regulation: The Challenges for Public Policy in the USA* (Warton Financial Institution Centre, University of Pennsylvania) 97

Zagaris and MacDonald 1992 *George Washington Journal of Law and Economics*

Zagaris B and MacDonald S "Money Laundering, Financial Fraud and Technology: The Perils of an Instantaneous Economy" 1992 *George Washington Journal of Law and Economics* 61-92

***Case Law***

*Columbus Joint Venture v ABSA Bank Ltd* 2002 (1) SA 90 (SCA)

*Energy Measurements (Pty) Ltd v First National Bank of South Africa Ltd* 2001 (3) SA 132 (W)

*Estate Agency Affairs Board v Auction Alliance (Pty) Ltd and Others (CCT 94/13) 2014 (ZACC 3)*

*Estate Agency Affairs Board v Auction Alliance (Pty) Ltd and Others 2014 (3) SA 106 (CC)*

*Estate Agency Affairs Board v Auction Alliance (Pty) Ltd and Others 2014 (4) BCLR 373 (CC)*

*Indac Electronics (Pty) Ltd v Volkskas Bank Ltd* 2001 (3) SA 132 (W)

*KwaMashu Bakery Ltd v Standard Bank of South Africa Ltd* 1995 (1) SA 377 (D)

*Moss v Hancock* (1899) 2 QB 111 116

*Miller v Race* (1758) 1 Burr 452

*Powell and another v ABSA Bank Ltd t/a Volkskas Bank* 1998 (2) SA 807 (SE)

*Spratt v Hobhouse* (1827) 4 Bing 179

*Sylla and Others v Minster of the Department of Finance and Another* (08/38696) [2011] SAGPJHC 200

*Uganda v Sserunkuma and 8 others* [2015] UGHCACD 5

*USA v Liberty Reserve S.A. and 7 others* [2013] CRIM 368 (United States District Court, Southern District of New York)

**Legislation**

*Banks Act* 94 of 1990

*Constitution of the Republic of South Africa* 108 of 1996

*Currency and Exchanges Act* 9 of 1933

*Deposit-taking Institutions Act 94 of 1990*

*Electronic Communications Act* 36 of 2005

*Exchange Control Regulations* 1961

*Financial Intelligence Centre Act* 38 of 2001

*Financial Intelligence Centre Amendment Bill*

*Financial Sector Regulation Bill*

*Independent Communications Authority of South Africa Act* 13 of 2000

*Interpretation Act* 33 of 1957

*National Payment System Act* 78 of 1998

*Preventions and Combating of Corrupt Activities Act* 12 of 2004 *Prevention of Organised Crime Act* 121 of 1998

*Promotion of Personal Information* Act 4 of 2013

*Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004

*Protection of Personal Information Act* 4 of 2013

*South African Reserve Bank Act* 90 of 1989 *Telecommunications Act* 103 of 1996

*Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002

## International instruments

*Financial Action Task Force Forty Recommendations*

*Basel Committee on Banking Supervision Core Principles*

*International Convention for the Suppression of Counterfeiting Currency* Convention of 1929 (section 2)

*United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 20 December 1988*

United Nations 1999 *International Convention on the Suppression of the Financing of Terrorism, New York, 9 December 1999*

*United Nations Convention against Transitional Organised Crime and the Protocols Thereof (Palermo Convention),* 15 November 2000, General Assembly Resolution 55/25

## Government publications

GN R.1111, in GG Extraordinary 123, of 1 December 1961of 1 December 1961

GN R.445 in GG 35430 of 8 June 2012

GN R1596 and GN 24176 of 20 Dec 2002

GN 715 in GG 27803 of 18 July 2005

GN 78 in GG 33309 of 25 June 2010

GN1104 of 1 December 2010

GN R.445 in Government Gazette No. 354030 of 8 June 2012

GN 4 in GG7068 of 26 November 2013

GN 461 in GG. 38844 of 5 June 2015

## Unpublished Presentations

Department: National Treasury and the Financial Intelligence Centre "*Financial Intelligence Centre Amendment Bill*, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation on 20 April 2016

Department: National Treasury and the Financial Intelligence Centre "*Financial Intelligence Centre Amendment Bill*, 2016: Contentious Policy Issues, Resolutions and Implementation Briefing of the Standing Committee on Finance" presentation 20 April 2016

## Internet

Aglietta 2002 http://goo.gl/RTOse

Aglietta M 2002 *Whence and Shither Money? In Organisational for Economic Co-operation and Development (OECD) – The Future of Money* http://goo.gl/RTOse accessed 28 December 2015

Ahumud unknown date http://academia.edu/5321031/Literature_Review_Risk_Based_Approach_to_AML_and_CTF

Ahumud R unknown date *Literature Review of the Risk-Based Approach to AML and CFT* http://academia.edu/5321031/Literature_Review_Risk_Based_Approach_to_AML_and_CTF accessed 25 May 2016

Alexander, Mas and Radcliffe 2010 http://www.ssrn.com/abstract=1664644

Alexander C, Mas I and Radcliffe D 2010 *Regulating New Banking Models that can Bring Financial Services to All* http://ssrn.com/abstract=1664644 accessed 15 December 2014

Alexander 2001 http://microcreditsummit.org/uploads/resource/document/alexandrec_branchless_banking_52485.pdf

Alexander C 2001 *What can Branchless Banking do to Advance the Field, and What can it Not Do? From Mobile Banking to point of Service - Mobile Banking to Point of Service Microcredit Summit, Valladolid, Spain.* http://microcreditsummit.org/uploads/resource/document/alexandrec_branchless_banking_52485.pdf accessed 10 August 2014

Ali *et al* 2014 http://bankofengland.co.uk/publications/Documents/quaterlybulitin/2014/qp14q301.pdf

Ali, R, Barrdear, J, Clews, R and Southgate, J 2014 *The economics of digital currencies.* http://bankofengland.co.uk/publications/Documents/quaterlybulitin/2014/qp14q301.pdf accessed 10 August 2014

Anon 2014 http://itnewsafrica.com/2014/06/police-bring-down-tigo-call-credit-fraud-ring/

Anon 2014 *Police bring down Tigo call credit fraud ring* http://itnewsafrica.com/2014/06/police-bring-down-tigo-call-credit-fraud-ring/ accessed 13 January 2016

Bank for International Settlements 1988 http://bis.org/pub/bcbsc137.pdf

Bank for International Settlements 1988 *Statement on Prevention of Criminal Use of the Banking system for the Purpose of Money Laundering* http://bis.org/pub/bcbsc137.pdf accessed 21 March 2016

Bank for International Settlements 2001 http://bis.org/pub/bcbs85.pdf

Bank for International Settlements 2001 *Client Due Diligence for Banks* http://bis.org/pub/bcbs85.pdf

Bank for International Settlements 2012 http://bis.org/publ/bcbs213.pdf

Bank for International Settlements 2012 *Core Principle of Effective Banking Supervision* http://bis.org/publ/bcbs213.pdf accessed 2 February 2016

Bank for International Settlements 2015 http://www.bis.org/bcbs/about.htm

Bank for International Settlements 2015 *Basel Committee* http://bis.org/bcbs/about.htm accessed 19 February 2016

Bank for International Settlements 2016 http://bis.org/bcbs/publ/d353.pdf

Bank for International Settlements 2016 *Basel Committee on Banking Supervision: Sound management of risks related to money laundering and financing of terrorism (amended version which included guidance on account opening)* http://bis.org/bcbs/publ/d353.pdf accessed 10 February 2016

Bankrate 2015 http://bankrate.com/finance/savings/could-bank-hackers-steal-your-money-1.aspx

Bankrate 2015 *Could online hackers steal your cash?* http://bankrate.com/finance/savings/could-bank-hackers-steal-your-money-1.aspx accessed 5 January 2015

Bångers and Söderberg 2008 http://spidercenter.org/polopoly_fs/1.163645.1390316332!/menu/standard/file/Spider%20ICT4D%20Series%202%20Mobile%20banking%20-%20financial%20services%20for%20the%20unbanked.pdf

Bångers L and Söderberg B 2008 *Mobile Banking – Financial Services for the Unbanked* http://spidercenter.org/polopoly_fs/1.163645.1390316332!/menu/standard/file/Spider%20ICT4D%20Series%202%20Mobile%20banking%20-%20financial%20services%20for%20the%20unbanked.pdf accessed 3 January 2015

Bank for International Settlements 2012 http://bis.org/publ/bcbs230.pdf

Bank for International Settlements 2012 *Basel Committee on Banking Supervision*: *Core Principles for Effective Banking Supervision* http://bis.org/publ/bcbs230.pdf 28 February 2016

Basel Committee on Banking Supervision 1998 https://bis.org/publ/bcbx35.pdf accessed

Basel Committee on Banking Supervision 1998 *Risk Management for Electronic Banking and Electronic Money Activities* https://bis.org/publ/bcbx35.pdf accessed 10 August 2014

Basel Committee on Banking Supervision March 2012 http://bis.org/publ/bcbs213.pdf

Basel Committee on Banking Supervision March *2012 Consultative Document: Core Principles for Effective Banking Supervision* http://bis.org/publ/bcbs213.pdf accessed 5 January 2015

Basel Committee on Banking Supervision 2014 http://bis.org/press/p140115.htm

Basel Committee on Banking Supervision 2014 *Sound management of risks related to money laundering and financing of terrorism (Bank for International Settlements Basel)* http://bis.org/press/p140115.htm accessed 15 December 2014

BBC 2016 http://bbc.com/news/world-europe-35899353

BBC 2016 *Brussels attacks: Suspect's DNA at Paris attacks sites* http://bbc.com/news/world-europe-35899353 accessed 21 March 2016

Bester *et al.* 2010 http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf

Bester H, Hougaard C and Chamberlain D 2010 *Reviewing the policy framework for money transfers* http://cenfri.org/documents/Remittances/2010/Regulatory%20framework%20for%20money%20transfers_South%20Africa_discussion%20doc_250110.pdf accessed 15 December 2016

Bitcoin magazine 2014 https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507

Bitcoin magazine 2014 *Digital vs Virtual Currencies* https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507 accessed 2 April 2016

Blackstone *1765* http://press-pubs.uchicago.edu/founders/documents/a1_8_5s1.html

Blackstone W date unknown *Commentaries on the Laws of England: A Facsimile of the First Edition of 1765 – 1769. "The Founders' Constitution", Article 1, section 8, clause 5* http://press-pubs.uchicago.edu/founders/documents/a1_8_5s1.html accessed 3 January 2015

Burhouse, Chu, Goodstein *et al*. 2013 https://fdic.gov/householdsurvey/2013report.pdf

Burhouse S, Chu K, Goodstein R et al. 2013 *FDIC 2013 National Survey of Unbanked and Underbanked Households* https://fdic.gov/householdsurvey/2013report.pdf accessed 29 September 2015

Buckley *et al* 2014 http://clmr.usw.edu.au/taxonomy/team/77

Buckley R *et al* 2014 *Regulation of Mobile Money* http://clmr.usw.edu.au/taxonomy/team/77 accessed 3 January 2015

Carse 1999 http://bis.org/review/r991012c.pdf

Carse D 1999 *The Regulatory Framework of E-Banking* http://bis.org/review/r991012c.pdf accessed 25 January 2016

Cassara date unknown http://sas.com/en_us/insights/articles/risk-fraud/mobile-payments-smurfs-emerging-threats.html

Cassara JA date unknown *Mobile payments, smurfs and emerging threats*" SAS Institute Inc http://sas.com/en_us/insights/articles/risk-fraud/mobile-payments-smurfs-emerging-threats.html accessed 20 March 2015

Cassara June 2015 http://mobilepaymentstoday.com/articles/out-of-africa-aml-compliance-for-mobile-payments/

Cassara JA June 2015 *Out of Africa: AML compliance for mobile payments* http://mobilepaymentstoday.com/articles/out-of-africa-aml-compliance-for-mobile-payments/ accessed 20 March 2015

Centre for Global Development 2016 http://cgdev.org/sites/default/files/CGD-Policy-Paper-Gelb-KYC-Financial-Inclusion.pdf

Centre for Global Development 2016 *Balancing Financial Integrity with Financial Inclusion: Risk-Based approach to "Know-Your-Client"* http://cgdev.org/sites/default/files/CGD-Policy-Paper-Gelb-KYC-Financial-Inclusion.pdf accessed 10 February 2016

Chaia, Goland and Schiff 2010 http://mckinsey.com/insights/financial_services/counting_the_worlds_unbanked

Chaia A, Goland T and Schiff R 2010 Counting the world's unbanked http://mckinsey.com/insights/financial_services/counting_the_worlds_unbanked accessed 15 April 2015

Chaix and Torre 2011 http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf

Chaix L and Torre D 2011 *Four models for mobile payments* http://hp.gredeg.cnrs.fr/Dominique_Torre/workpap/chaix_torre_gdr2011_17mars.pdf accessed 25 May 2016

Chatain *et al* 2008 http://siteresources.worldbank.org/INTAML/Resources/WP146_web.pdg

Chatain P *et al* 2008 *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing 146* http://siteresources.worldbank.org/INTAML/Resources/WP146_web.pdg accessed 24 April 2015

Chiu and Wong 2014 http://bostonfed.org/payments2014/papers/Chiu_Wong.pdf

Chiu J and Wong T 2014 On the Essentiality of Electronic Money http://bostonfed.org/payments2014/papers/Chiu_Wong.pdf accessed 3 January 2015

Chriten, Lyman and Rosenberg 2003 http://info.worldbank.org/etools/docs/library/83619/cgap_paper.pdf

Chriten RP, Lyman TR and Rosenberg R 2003 *Guiding Principles of Regulation and Supervision of Microfinance. Consensus Guideline.* http://info.worldbank.org/etools/docs/library/83619/cgap_paper.pdf accessed 3 January 2015

Cluley 2015 http://hotforsecurity.com/blog/hackers-steal-5-million-from-ryanairs-bank-account-11744.html

Cluley G 2015 *Hackers steal $5 million from Ryanair's bank account* http://hotforsecurity.com/blog/hackers-steal-5-million-from-ryanairs-bank-account-11744.html accessed 22 September 2015

CNNMoney (New York) 14 May 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/

CNNMoney (New York) 14 May 2015 *Hackers are draining bank accounts via the Starbucks app* http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/ accessed 22 September 2015

Consultative Group to Assist the Poor (CGAP) 2014 http://cgap.org/publications/bitcoin-vs-electronic-money

Consultative Group to Assist the Poor (CGAP) 2014 *Bitcoin vs Electronic Money* http://cgap.org/publications/bitcoin-vs-electronic-money accessed 10 February 2016

Costanzo 2007 http://2.econ.uu.nl/users/unger/papers/Costanzo.pdf

Costanzo P 2007 *Rule-based vs. Risk-based approaches to control the 3rd EU Anti-Money Laundering Directive* http://2.econ.uu.nl/users/unger/papers/Costanzo.pdf accessed 15 January 2015

Di Castri *et al.* 2015 http://gsma.com/mobilefordevelopment/wp-content/uploads/2015/10/Proportional-risk-based-AMLCFT-regimes-for-mobile-money.pdf.

Di Castri S, Grossman J and Sihin R 2015 *Proportional risk-based AML/CFT regimes for mobile money: A framework for assessing risk factors and mitigation measures* http://gsma.com/mobilefordevelopment/wp-content/uploads/2015/10/Proportional-risk-based-AMLCFT-regimes-for-mobile-money.pdf accessed 20 December 2016

De Koker 2008 http://finmark.org.za/wp-content/uploads/pubs/Rep_ML_Riskmanagement_prodserv_SA_May08.pdf

De Koker L 2008 *Money laundering and terrorist financing risk management of low risk financial products and services in South Africa" The Centre for Financial Regulations and Inclusion* http://finmark.org.za/wp-content/uploads/pubs/Rep_ML_Riskmanagement_prodserv_SA_May08.pdf accessed 15 January 2015

Demirgüç-Kunt, Beck, and Honohan 2008 Washington: World Bank http://go.worldbank.org/HNKL9ZHO50

Demirgüç-Kunt A, Beck T, and Honohan P 2008 *Finance for All? Policies and Pitfalls in Expanding Access. World Bank Policy Research Report.* Washington: World Bank http://go.worldbank.org/HNKL9ZHO50 accessed 3 January 2015

Demombynes and Thegeya. March 2012 http://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5988

DemombynesG and Thegeya A March 2012 K*enya's Mobile Revolution and the Promise of Mobile Savings. World Bank Policy Research Working Paper, No. 5988* http://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5988 accessed 3 July 2015

Department of Justice 2013 http://justice.gov/criminal/pr/speeches/2013/crm-speech-131118.html

Department of Justice 2013 *Acting Assistant Attorney General M Raman testifies before the Senate Committee on Homeland Security and Governmental Affairs.* http://justice.gov/criminal/pr/speeches/2013/crm-speech-131118.html accessed 13 August 2015

Department of Justice 2013 http://justice.gov/opa/pr/2013/Octobe/13-crm-1128.html

Department of Justice 2013 *Indictment Unsealed and "Wanted" Posters Issued to Fugitives changed with Multimillion Dollar Cyber Fraud Scheme* http://justice.gov/opa/pr/2013/Octobe/13-crm-1128.html accessed 13 August 2015

Dias and McKee 2010 http://cgap.org/publications/protecting-branchless-banking-consumers

Dias D and McKee K 2010 *Protecting Branchless Banking Clients: Policy Objectives and Regulatory Options* http://cgap.org/publications/protecting-branchless-banking-consumers accessed 15 December 2014

Du Toit 2013 http://dspace.nwu.ac.za/bitstream/handle/10394/10197/Du_Toit_SF.pdf?sequence=1

Du Toit 2013 *Die juridiese aard van geld: skuiwende matrikse en paradigmas* http://dspace.nwu.ac.za/bitstream/handle/10394/10197/Du_Toit_SF.pdf?sequence=1 accessed 3 January 2015

Egmont Group 2013 http://egmontgroup.org/library/download/290

Egmont Group 2013 Egmont Group of Financial Intelligence Units Principles for Information Exchange between Financial Intelligence Units http://egmontgroup.org/library/download/290 accessed 24 February 2016

Ely 1996 http://cato.org/moneyconf/14mc-2.html

Ely B 1996 *Electronic Money and Monetary Policy: Separating Fact from Fiction. The Future of Money in the Information Age, CATO Institute's 14th Annual Monetary Conference 1996*. http://cato.org/moneyconf/14mc-2.html accessed 15 December 2014

Ericsson 2015 http://ericsson.com/ericsson-mobility-report

Ericsson 2015 *Ericsson Mobility Report 2015 – on the pulse of the networked society* http://ericsson.com/ericsson-mobility-report accessed 22 September 2015

Ernst and Young 2013 http://ey.com/Publication/vwLUAssets/The_evolution_of_borderless_financial_crime/$File/1310-1152512_FinancialCrimeMngt_Broch_v6.pdf

Ernst and Young 2013 *Financial crime management: The evolution of borderless financial crime* http://ey.com/Publication/vwLUAssets/The_evolution_of_borderless_financial_crime/$File/1310-1152512_FinancialCrimeMngt_Broch_v6.pdf accessed 22 September 2015

European Central Bank 2012 http://ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Central Bank 2012 *Virtual Currency Schemes* http://ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf accessed 5 January 2015

Eurofi 2014 https://eurofi.net/wp-content/uploads/2014/09/Electronic-Payment-services-WEB.pdf

Eurofi 2014 The regulatory challenges posed by electronic financial and payment services https://eurofi.net/wp-content/uploads/2014/09/Electronic-Payment-services-WEB.pdf accessed 28 June 2016

European Parliament 2009 http://europarl.europa.eu/document/activities/cont/200911/20091119ATT64822/20091119ATT64822EN.pdf

European Parliament 2009 *Defining and Measuring Systemic Risk* http://europarl.europa.eu/document/activities/cont/200911/20091119ATT64822/20091119ATT64822EN.pdf accessed 15 March 2016

Eyewitness news 2016 http://ewn.co.za/2016/05/23/Standard-Bank-confirms-R300m-lost-in-credit-card-scam

Eyewitness news 2016 *Standard Bank confirms R300m lost in credit card scam* http://ewn.co.za/2016/05/23/Standard-Bank-confirms-R300m-lost-in-credit-card-scam accessed 28 June 2016

Feinson unknown http://aau.org/sites/default/files/urg/docs/nis_overview_country-%20cases.pdf

Feinson S unknown *National Innovation Systems: Overview and Country Cases* http://aau.org/sites/default/files/urg/docs/nis_overview_country-%20cases.pdf accessed 5 February 2016

Financial Actions Task Force 2003 – 2004 https://imolin.org/pdf/imolin/FATF_Typologies_Rpt_2003-04.pdf

Financial Actions Task Force 2003 – 2004 Money laundering and terrorist financing typology 2004 -2003 https://imolin.org/pdf/imolin/FATF_Typologies_Rpt_2003-04.pdf accessed 25 January 2016

Financial Actions Task Force October 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf

Financial Actions Task Force October 2006 *Report on new payment Methods* http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf accessed 13 August 2015

Financial Actions Task Force 2006 http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20 New%20Payment%20Methods.pdf

Financial Actions Task Force 2006 *Report on New Payment Methods* http://fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf accessed 10 January 2016

Financial Action Task Force 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

Financial Action Task Force 2012 *Financial Action Task Force Recommendations of 2012* http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf accessed 10 September 2016

Financial Action Task Force Recommendation February 2012 http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Financial Action Task Force Recommendation February 2012 *FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* http://fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf accessed 25 September 2015

Financial Action Task Force June 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf accessed

Financial Action Task Force June 2013 *Guidance for Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services* http://fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf accessed 10 August 2014

Financial Action Task Force 2013 http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

Financial Action Task Force 2013 *Prepaid cards, mobile payments and internet-based payments* http://fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf accessed 13 August 2015

Financial Action Task Force June 2014 http://fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Financial Action Task Force June 2014 *Report Virtual Currencies: Key Definitions and Potential AML/CFT Risks* http://fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf accessed 5 January 2015

Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf

Financial Action Task Force 2015 *Guidance for Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisor and the Financial Sector and Law Enforcement* http://fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf accessed 19 January 2016

Financial Action Task Force 2015 http://fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf

Financial Action Task Force 2015 *Australia Mutual Evaluation Report* http://fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf accessed 25 September 2015

Financial Intelligence Centre 2004 https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf

Financial Intelligence Centre 2004 *Guidance note 1: General guidance concerning identification of clients* https://fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/16.Guidance%20concerning%20identification%20of%20clients.pdf accessed 15 January 2015

Financial Intelligence Centre 2014 https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/AP140213%20PCC26%20Single%20Client%20View.pdf

Financial Intelligence Centre 2014 *Public Compliance Communication No. 26 (PCC26) – Single client view* https://fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/AP140213%20PCC26%20Single%20Client%20View.pdf accessed 15 September 2015

Financial Services Board 2013 https://fsb.co.za/Departments/twinpeaks/Documents/Twin%20Peaks%2001%20Feb%202013%20Final.pdf

Financial Services Board 2013 *Implementing a twin peaks model of financial regulation in South Africa* https://fsb.co.za/Departments/twinpeaks/Documents/Twin%20Peaks%2001%20Feb%202013%20Final.pdf accessed 2 February 2016

Financial Transaction and Report Analysis Centre of Canada 2014 http://fintrac-canafe.gc.ca/fintrac-canafe/definitions/terrorist-terroriste-eng.asp

Financial Transaction and Report Analysis Centre of Canada 2014 *Terrorist* http://fintrac-canafe.gc.ca/fintrac-canafe/definitions/terrorist-terroriste-eng.asp accessed 5 January 2015

FinCen 2013 https://fincen.gov/news_room/testimony/html/20131119.html

FinCen 2013 *What is virtual currency?* https://fincen.gov/news_room/testimony/html/20131119.html accessed 5 January 2015

FinMark Trust 2009 http://bankablefrontier.com

FinMark Trust 2009 *The Mzansi Bank Account Initiative in South Africa Report* Commissioned by Bankable Frontier Associates LLC http://bankablefrontier.com accessed 8 January 2014.

FinMark Trust Compliance and Risk Resources 2015 http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf

FinMark Trust Compliance and Risk Resources 2015 *AML/CFT and Financial Inclusion in SADC: Contribution of Anti-Money Laundering and Combating the Financing of Terrorism Legislation in Various Southern African Development Community (SADC) countries* http://finmark.org.za/wp-content/uploads/2016/01/Microsoft-Word-10.-South-Africa-Rep_AML_Country_SouthAfrica_20152.pdf accessed 25 April 2016

Fung, Molico and Stuber 2014 http://banqueducanada.ca/wp-content/uploads/2014/04/dp2014-2.pdf

Fung B, Molico M and Stuber G 2014 *Electronic Money and Payments: Recent development and Issues Bank of Canada* http://banqueducanada.ca/wp-content/uploads/2014/04/dp2014-2.pdf accessed 15 September 2015

Gastrow 1998 https://issafrica.org/publications/monographs/monograph-28-organised-crime-in-south-africa-an-assessment-of-its-nature-and-origins-by-peter-gastrow.

Gastrow P 1998 *Organised crime in South Africa: An assessment of its nature and origins. ISS Monograh Series No. 28. Institute for Security Studies.* https://issafrica.org/publications/monographs/monograph-28-organised-crime-in-south-africa-an-assessment-of-its-nature-and-origins-by-peter-gastrow accessed 15 January 2013

Gates January 2015 http://social.yourstory.com/2015/01/quotes-bill-gates-mobile-banking

Gates B January 2015 *Banking is necessary, banks are not.* http://social.yourstory.com/2015/01/quotes-bill-gates-mobile-banking accessed 3 July 2015

Gardner 2014 http://bbc.com/news/world-europe-30789123

Gardner F 2014 *Paris Attacks: Were gunmen aided by terror network?* http://bbc.com/news/world-europe-30789123 accessed 18 January 2015

Geva and Kianieff 2005 http://goo.gl/QfR4y

Geva B and Kianieff M 2005 *Reimagining E-Money: Its Conceptual Unity with other Retail Payment Systems* http://goo.gl/QfR4y accessed 28 December 2015

Gianviti 2004 http://imf.org/external/np/leg/sem/2004/cdmfl/eng/gianvi.pdf

Gianviti F 2004 *Current Legal Aspects of Monetary Sovereignty* http://imf.org/external/np/leg/sem/2004/cdmfl/eng/gianvi.pdf accessed 15 December 2014

Global Partnership for Financial Inclusion 2010 http://gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf

Global Partnership for Financial Inclusion 2010 *G20 Principle of Innovative Financial Inclusion* http://gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf accessed 3 July 2015

Global Partnership for Financial Inclusion September 2014 https://g20.org/wp-content/uploads/2014/12/2014_g20_financial_inclusion_action_plan.pdf

Global Partnership for Financial Inclusion September 2014 *2014 Financial Inclusion Action Plan* https://g20.org/wp-content/uploads/2014/12/2014_g20_financial_inclusion_action_plan.pdf accessed 15 September 2015

Golder and Williams 2004 https://corrigan.austlii.edu.agu

Golder B and Williams G 2004 *What is "Terrorism? Problem of Legal Definition"* https://corrigan.austlii.edu.agu accessed 20 February 2016

Greenacre 2014 http://clmr.unsw.ed.au/article/risk/material-risk/fure-mobile-banking-part-one

Greenacre J 2014 *The Future of Mobile Banking – Part One* http://clmr.unsw.ed.au/article/risk/material-risk/fure-mobile-banking-part-one accessed 16 January 2015

Grimmelamann 2014 http://ssrn.com/abstract=2358627

Grimmelamann J, 2014 *Anarchy, Status Updates and Utopia, 34 Place L Rev.* http://ssrn.com/abstract=2358627 accessed 8 August 2015

Gross et al. 2012

http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf

Gross MB, Hogarth JM and Schmeiser MD 2012 *Use of Financial Services by the Unbanked and Underbanked and the Potential for Mobile Financial Services Adoption.*

http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf accessed 15 September 2015

GSMA 2006 http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/Philippines-Case-Study-v-X21-21.pdf

GSMA 2006 *Mobile Money in the Philippines – The Market, the Models and Regulation* http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/Philippines-Case-Study-v-X21-21.pdf accessed 15 September 2015

GSMA Association 2015 http://gsmamobileeconomy.com/

GSMA Association 2015 *The Mobile Economy* http://gsmamobileeconomy.com/ accessed 8 August 2015

Gross, Hogarth and Schmeiser 2012 http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf

Gross MB, Hogarth JM and Schmeiser MD 2012 *Use of Financial Services by the Unbanked and Underbanked and the Potential for Mobile Financial Services Adoption.* http://federalreserve.gov/Pubs/Bulletin/2012/pdf/mobile_financial_services_201209.pdf accessed 15 September 2015

Groupe Special Mobile Association (GSMA) 2012 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/03/MMU_Results-from-the-2012-Global-Mobile-Money-Adoption-Survey.pdf

Groupe Special Mobile Association (GSMA) 2012 *Findings on Mobile Money for the Unbanked: State of the Industry – Results from the 2012 Global Mobile Money Adoption Survey* http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/03/MMU_Results-from-the-2012-Global-Mobile-Money-Adoption-Survey.pdf accessed 15 December 2014

Guardian Data Systems 2014 http://guardiandatasystems.com/open-vs-closed-loop-payment-processing/ accessed

Guardian Data Systems 2014 *Open vs Closed Loop Payment Systems* http://guardiandatasystems.com/open-vs-closed-loop-payment-processing/ accessed 5 January 2015

Howden 2014 http://theguardian.com/world/interactive/2013/oct/04/westgate-mall-attacks-kenya-terror

Howden D 2014 *Terror in Westgate Mall: The full story of the attacks that devastated Kenya* http://theguardian.com/world/interactive/2013/oct/04/westgate-mall-attacks-kenya-terror accessed 18 January 2015

Innes 1913 http://community-exchange.org/docs/what%20is%20money.htm

Innes AM 1913 *What is Money?* http://community-exchange.org/docs/what%20is%20money.htm accessed 15 January 2015

International Monetary Fund 2001 https://imf.org/external/np/ml/2001/eng/021201.pdf

International Monetary Fund 2001 *Financial System Abuse, Financial Crime and Money Laundering— Background Paper* https://imf.org/external/np/ml/2001/eng/021201.pdf accessed 10 August 2014

International Organization for Standardization (ISO) 2009 http://iso.org/iso/iso31000

International Organization for Standardization (ISO) 2009 *Risk Management* http://iso.org/iso/iso31000 accessed 10 April 2016

International Peace Institute 2010 https://ciaonet.org/attachments/17631/uploads

International Peace Institute 2010 Transnational Organized Crime and Palermo Convention: A Reality Check https://ciaonet.org/attachments/17631/uploads accessed 12 February 2016

Interpol 2015 http://interpol.int/Crime-areas/Financial-crime/Money-laundering

Interpol 2015 *Money Laundering* http://interpol.int/Crime-areas/Financial-crime/Money-laundering accessed 10 January 2015

Investopedia 2015 http://investopedia.com/terms/u/unbanked.asp

Investopedia 2015 *Definition of Unbanked* http://investopedia.com/terms/u/unbanked.asp accessed 15 January 2015

Investopedia 2015 http://investopedia.com/terms/f/fiatmoney.asp

Investopedia 2015 http://investopedia.com/terms/f/fiatmoney.asp
Investopedia 2015 *Fiat Money Definition* http://www.investopedia.com/terms/f/fiatmoney.asp accessed 15 January 2015

IT Web Security 2016 http://itweb.co.za/index.php?option=com_content&view=article&id=151192

IT Web Security 2016 *Vodacom security solution targets small business* http://itweb.co.za/index.php?option=com_content&view=article&id=151192 accessed 5 April 2016

Isern and de Koker 2009 http://cgap.org/publications/amlcft-strengthening-financial-inclusion-and-integrity

Isern J and de Koker L 2009 *AML/CFT: Strengthening Financial Inclusion and Integrity* CGAP http://cgap.org/publications/amlcft-strengthening-financial-inclusion-and-integrity

Ivatury and Pickens 2006 https://cgap.org/sites/default/files/CGAP-Mobile-Phone-Banking-and-Low-Income-Clients-Evidence-from-South-Africa-Jan-2006.pdf

Ivatury G and Pickens M 2006 *Mobile phone banking and low-income clients: Evidence from South Africa.* Washington, DC: Consultative group to assist the poor (CGAP) and the United Nations Foundation https://cgap.org/sites/default/files/CGAP-Mobile-Phone-Banking-and-Low-Income-Clients-Evidence-from-South-Africa-Jan-2006.pdf accessed 15 September 2015

Jenkins 2008 http://hks.harvard.edu/m-rcbg/CSRI/publications/report_30_MOBILEMONEY.pdf

Jenkins B 2008 *Developing Mobile Money Ecosystem, Washington DEC:IFCe and Harward Kennedy school* http://hks.harvard.edu/m-rcbg/CSRI/publications/report_30_MOBILEMONEY.pdf accessed 15 September 2015

Justice Michael Kirby 2007 https://cnet.com/news/judge-on-privacy-computer-code-trumps-the-law/

Justice Michael Kirby 2007 *Judge of the High Court of Australia, as reported in L Tung 2007 Judges: computer code is more potent than the law ZDNet* https://cnet.com/news/judge-on-privacy-computer-code-trumps-the-law/ accessed 18 December 2016

Juta Law 2015 https://jutalaw.co.za

Juta Law 2015 "Twin Peaks in South Africa" https://jutalaw.co.za accessed 1 April 2016

Kaspersky Lab 2015 http://kaspersky.com/about/news/virus/2015/Kaspersky-Lab-mobile-banking-threats-among-the-top-10-malicious-financial-programs-for-the-first-time

Kaspersky Lab 2015 *Kaspersky Lab: mobile banking among the top 10 malicious financial program for the first time* http://kaspersky.com/about/news/virus/2015/Kaspersky-Lab-mobile-banking-threats-among-the-top-10-malicious-financial-programs-for-the-first-time access on 5 April 2016

Kaspersky Lab 2015 https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

Kaspersky Lab 2015 *Kapersky Security Bulletin 2015: overall Statistics for 2015* https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

Kellermann 2006 http://wds.workdbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_2006042114035/Rendered/PDF/359050rev0Mone1nCyberspace01

Kellermann T 2006 *Money Laundering in Cyberspace.* The World Bank: Financial Sector Working Paper http:/wds.workdbank.org/external/default/WDSContentServer/WDSP/IB/2006/04/21/000012009_2006042114035/Rendered/PDF/359050rev0Mone1nCyberspace01 accessed 5 February 2016

Kendall and Machoka 2011 http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/ssrnid1830704.pdf.

Kendall J and Machoka P 2011 *An Emerging Platform: From Money Transfer System to Mobile Money Ecosystem* http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/ssrnid1830704.pdf accessed 18 December 2016

Klein in Chatain *et al* 2008 http://siteresources.worldbank.org/INTAML/Resources/WP146_web.pdg

Klein M in Chatain P *et al* 2008 *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing 146* http://siteresources.worldbank.org/INTAML/Resources/WP146_web.pdg accessed 18 August 2015

Klein and Mayer 2013 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/ibrdmbankingregulation27-1.pdf.

Klein and Mayer 2013 *Mobile Banking and Financial Inclusions: The Regulatory Lessons* http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/ibrdmbankingregulation27-1.pdf accessed 2 April 2016

KPMG 2013 https://kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Financial-Services/Documents/KPMG%20Twin%20peaks.pdf.

KPMG 2013 *Financial Services: Twin Peaks* https://kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Financial-Services/Documents/KPMG%20Twin%20peaks.pdf accessed 20 February 2016

Kumar and Dutta July 2015 http:/epw.in/system/files/pdf/2015_50/28/Role_of_Mobile_Money_in_Replacing_Cash.pdf

Kumar L and Dutta S July 2015 *Role of Mobile Money in Replacing Cash – A Study Among Migrant Workers in South India* Economic and Political Weekly 41 http:/epw.in/system/files/pdf/2015_50/28/Role_of_Mobile_Money_in_Replacing_Cash.pdf accessed 29 August 2015

Lassignardie and Brown 2013

http://capgemini.com/resource-file-access/resource/pdf/wpr_2013.pdf

Lassignardie J and Brown K 2013 *World Payment Report* http://capgemini.com/resource-file-access/resource/pdf/wpr_2013.pdf accessed 18 November 2013

Luo, Zhang and Shim 2010 http://unm.edu/~xinluo/papers/DSS2010_MB.pdf

Luo X, Zhang J and Shim JP 2010 *Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. Decision Support Systems* 222–234 http://unm.edu/~xinluo/papers/DSS2010_MB.pdf accessed 18 August 2015

Lyman, Consultative Group to Assist the Poor (CGAP) 2008 http://cgap.org/sites/default/files/CGAP-Focus-Note-Regulating-Transformational-Branchless-Banking-Mobile-Phones-and-Other-Technology-to-Increase-Access-to-Finance-Jan-2008.pdf

Lyman T, Consultative Group to Assist the Poor (CGAP) 2008 *Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to finance* http://cgap.org/sites/default/files/CGAP-Focus-Note-Regulating-Transformational-Branchless-Banking-Mobile-Phones-and-Other-Technology-to-Increase-Access-to-Finance-Jan-2008.pdf accessed 15 December 2014

Mail&Guardian 2014 http://mg.co.za/article/2015-10-14-net1-the-company-that-runs-the-social-grant-payment-system

Mail&Guardian 2015 Net1 – the company that runs the social grant payment system http://mg.co.za/article/2015-10-14-net1-the-company-that-runs-the-social-grant-payment-system accessed 5 June 2016

McAfee unknown date http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf

McAfee unknown date *Digital laundering: An analysis of online currencies and their use in cybercrime* http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf accessed 15 February 2016.

Mbiti and Weil 2001 http://nber.org/papers/w17129.pdf

Mbiti I and Weil DN 2001 *Mobile Banking: The Impact of M-Pesa in Kenya* http://nber.org/papers/w17129.pdf accessed 8 February 2016

Mboweni 1999 http://bis.org/review/r991012c.pdf

Mboweni T 1999 *E-money and its impact on the central bank's operations* http://bis.org/review/r991012c.pdf accessed 25 January 2016

Mcdermid 2015 http://reuters.com/article/2015/10/05/us-usa-bitcoin-auction-idUSKCN0RZ1SP20151005

Mcdermid R 2015 *U.S. to hold final auction of bitcoins from Silk Road case* Reuters http://reuters.com/article/2015/10/05/us-usa-bitcoin-auction-idUSKCN0RZ1SP20151005 accessed 29 August 2015

Merritt 2010 http://frbatlanta.org/-/media/documents/rprf/rprf.../wp0810.pdf

Merritt C 2010 *Mobile Money Transfer Services: The next phase in Evolution in Person-to-Person payments* Federal Reserve Bank of Atlanta, Retail Payments Risk Forum White Paper http://frbatlanta.org/-/media/documents/rprf/rprf.../wp0810.pdf accessed 15 January 2015

Meyer June 2013 http://qz.com/94570/how-mobile-payments-might-be-the-global-money-laundering-machine-criminals-have-dreamed-about/

Meyer J June 2013 *How mobile payments might be the global money-laundering mechine criminals have dreamed about* http://qz.com/94570/how-mobile-payments-might-be-the-global-money-laundering-machine-criminals-have-dreamed-about/ accessed 15 January 2015

Miller et al 2016 http://arxiv.org/pdf/1602.05048.pdf

Miller K, Kennedy, E and Dubrawski, A 2016 *Do Public Events Attract Sex Trafficking Activities?* http://arxiv.org/pdf/1602.05048.pdf accessed 18 April 2016

Minnaar 1999 http://9iacc.org/papers/day4/ws5/dnld/d4ws5_aminnaar.pdf.

Minnaar 1999 *A Symbiotic Relationship? Organised Crime and Corruption in South Africa*. 9th International Anti-corruption Conference, Durban http://9iacc.org/papers/day4/ws5/dnld/d4ws5_aminnaar.pdf accessed 20 January 2014

Morawczvnski 2015 http://cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion

Morawczvnski O 2015 *Fraud in Uganda: How millions were lost to internal collusion* http://cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion accessed 29 August 2015

Murgia 2015 http://telegraph.co.uk/technology/internet-security/11896024/How-to-protect-yourself-from-SIM-swap-scams.html.

Murgia M 2015 *How to protect yourself from SIM-swap scams* http://telegraph.co.uk/technology/internet-security/11896024/How-to-protect-yourself-from-SIM-swap-scams.html accessed 20 February 2016

Nakamoto 2008 http://cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf

Nakamoto S 2008 Bitcoin: A Peer-to-Peer Electronic Cash System http://cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf accessed 22 June 2015

National Treasury 2011 http://treasury.gov.za/documents/national%20budget/2011/A%20safer%20financial%20sector%20to%20serve%20South%20Africa%20better.pdf

National Treasury 2011 *A Safer Financial Sector to Serve South Africa Better* http://treasury.gov.za/documents/national%20budget/2011/A%20safer%20financial%20sector%20to%20serve%20South%20Africa%20better.pdf accessed 28 January 2016

National Treasury 2011 http://gov.za/2011-budget-speech-minister-finance-pravin-gordhan

National Treasury 2011 *2011 Budget speech by Minster of Finance Pravin Gordhan* http://gov.za/2011-budget-speech-minister-finance-pravin-gordhan accessed 28 February 2016

National Treasury 2014 https://jutalaw.co.za/media/filestore/2015/03/2014_12_12_Response_document.pdf

National Treasury 2014 *Twin Peaks in South Africa: Responses and Explanatory document* https://jutalaw.co.za/media/filestore/2015/03/2014_12_12_Response_document.pdf accessed 28 January 2016

Net1 2012 http://net1.com/legal/terms-and-conditions-for-the-use-of-the-sassa-card-and-sassa-account/

Net1 2012 Terms and Conditions for the use of the SAASA Card and SASSA Account http://net1.com/legal/terms-and-conditions-for-the-use-of-the-sassa-card-and-sassa-account/ accessed 20 June 2016

Organisation for Economic Co-operative and Development 2002 http://oecd.org/futures/35391062.pdf

Organisation for Economic Co-operative and Development 2002 *Future of Money.* http://oecd.org/futures/35391062.pdf accessed 10 August 2014

Parker CGAP 2014 http://cgap.org/publications/bitcoin-vs-electronic-money

Parker SR CGAP 2014 *Bitcoin vs Electronic Money* http://cgap.org/publications/bitcoin-vs-electronic-money accessed 15 January 2015

Pénicaud February 2013 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/03/MMU_Results-from-the-2012-Global-Mobile-Money-Adoption-Survey.pdf

Pénicaud C February 2013 *State of the Industry – Results from the 2012 Global Mobile Money Adoption Survey* GSMA http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/03/MMU_Results-from-the-2012-Global-Mobile-Money-Adoption-Survey.pdf accessed 15 January 2015

Pikens, Poreous and Rotman 2009 http://cgap.org/sites/default/files/CGAP-Focus-Note-Scenarios-for-Branchless-Banking-in-2020-Oct-2009.pdf

Pikens M, Poreous D and Rotman S October 2009 *Scenarios for Branchless Banking in 2020* http://cgap.org/sites/default/files/CGAP-Focus-Note-Scenarios-for-Branchless-Banking-in-2020-Oct-2009.pdf accessed 16 January 2015

Pousttchi and Schurig 2012 http://doi.ieeecomputersociety.org/10.1109/HICSS.2004.1265440

Pousttchi and Schurig 2012 Assessment of today's mobilize banking applications from the view of customer requirements http://doi.ieeecomputersociety.org/10.1109/HICSS.2004.1265440 accessed 31 January 2015

PwC' February 2014 http://pwc.co.za/en_ZA/za/assets/pdf/global-economic-crime-survey-2014.pdf

PwC' February 2014 *Global Economic Grime Survey "Confronting the changing face of economic crime* http://pwc.co.za/en_ZA/za/assets/pdf/global-economic-crime-survey-2014.pdf accessed 16 January 2015

Reaves *et al* 2015 http://cise.ufl.edu/~traynor/papers/reaves-usenix15a.pdf

Reaves B *et al* 2015 *Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World* http://cise.ufl.edu/~traynor/papers/reaves-usenix15a.pdf accessed 2 September 2015

Reuters 2016 http://reuters.com/article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB

Reuters 2016 Japan an alluring target for Standard Bank ATM thieves http://reuters.com/article/us-standard-bk-grp-fraud-japan-idUSKCN0YF1IB accessed 20 November 2016

Samani, Paget and Hart 2014 http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf

Samani R, Paget F and Hart M 2014 *Digital Laundry: An analysis of online currencies, and their use in cybercrime* http://mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf accessed 29 August 2015

Saul 2008 https://ssrn.com

Saul B 2008 Defining "Terrorism" to Protect Human Rights" https://ssrn.com accessed 15 February 2016

Scott 2013 http://research.stlouisfed.org/pageone-economics/uploads/newsletter/2013/PageOne0313_Money_Trade_Barter_Inflation.pdf

Scott AW 2013 *Money and Inflation: A Functional Relationship* http://research.stlouisfed.org/pageone-economics/uploads/newsletter/2013/PageOne0313_Money_Trade_Barter_Inflation.pdf accessed 16 January 2015

Smith 2015 http://financialmail.co.za/moneyinvesting/2015/04/02/twin-peaks-regulation-climbing-lessons

Smith N 2015 *Twin Peaks Regulations: Climbing Lessons* http://financialmail.co.za/moneyinvesting/2015/04/02/twin-peaks-regulation-climbing-lessons accessed 22 January 2016

Solin and Zerzan 2010 http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/amlfinal35.pdf

Solin M and Zerzan A 2010 *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks* http://gsma.com/mobilefordevelopment/wp-content/uploads/2013/09/amlfinal35.pdf accessed 26 July 2014

South African Reserve Bank National Payment System Department December 2014 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf

South African Reserve Bank National Payment System Department December 2014 *Position Paper on Virtual currencies* http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf accessed 16 January 2015

South African Reserve Bank National Payment System Department November 2009 http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf

South African Reserve Bank National Payment System Department November 2009 *Position Paper on Electronic Money* http://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf accessed 16 January 2015

Sulivan 2015 http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/

Sulivan B 2015 *Hackers are draining bank accounts via the Starbucks app* http://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/ accessed 29 August 2015

Thacker and Wright 2012 http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/bn_116_building_business_models_for_mobile_money.pdf

Thacker KUM and Wright GAN 2012 *Building Business Models for Mobile Money* http://gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/bn_116_building_business_models_for_mobile_money.pdf accessed 15 January 2015

Telegraph 2016 http://telegraph.co.uk/news/worldnews/europe/belgium/12204399/Brussels-terror-attacks-metro-airport-suspects-live.html

Telegraph 2016 *Brussels terror attacks metro airport suspects live* http://telegraph.co.uk/news/worldnews/europe/belgium/12204399/Brussels-terror-attacks-metro-airport-suspects-live.html accessed 25 January 2016

The Bank of International Settlements 2009 http://legislation.gov.uk/uksi/2011/99/schedule/4/part/2/made

The Bank of International Settlements 2009 *Electronic Money Directive 2009/110/EC* http://legislation.gov.uk/uksi/2011/99/schedule/4/part/2/made accessed 5 August 2014

The Economists 2008 http://economist.com/node/11465558?story_id=11465558

The Economists 2008 *Halfway There: How to promote the spread of mobile phones among the world's poorest* http://economist.com/node/11465558?story_id=11465558 accessed 29 August 2015

The European Commission February 2006 http://ec.europa.eu/internal_market/bank/docs/e-money/evaluation_en.pdf

The European Commission February 2006 *Evaluation of the E-Money Directive 2000/46/EC* http://ec.europa.eu/internal_market/bank/docs/e-money/evaluation_en.pdf accessed 26 July 2014

The South African Reserve Bank National Payment System Department 2009 http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf

The South African Reserve Bank National Payment System Department 2009 www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/PP2009_01.pdf accessed 15 January 2015

The South African Reserve Bank 2015 https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem%28NPS%29/Documents/Overview/Vision2015.pdf

The South African Reserve Bank 2015 *National Payment System Framework and Strategy: Vision 2015 South African Reserve Bank's Payment System* https://resbank.co.za/RegulationAndSupervision/NationalPaymentSystem%28NPS%29/Documents/Overview/Vision2015.pdf accessed 15 January 2015

The Statistics Portal 2015 http://tatista.com/statistics/284203/mena-mobile-phone-internet-user-penetration/

The Statistics Portal 2015 *Mobile phone internet user penetration in Middle East and Africa from 2012 to 2017* http://statista.com/statistics/284203/mena-mobile-phone-internet-user-penetration/ accessed 29 August 2015

The United States of America Act 2001 https://gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

The United States of America Act 2001 *USA Patriot Act* https://gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf accessed 25 January 2016

The World Bank 2013 http://worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank

The World Bank 2013 *Developing Countries to Receive Over USD 410 Billion in Remittances in 2013, say World Bank* http://worldbank.org/en/news/press-release/2013/10/02/developing-countries-remittances-2013-world-bank accessed 15 October 2015

Thomas Reuters 2015 https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/expert-talk/financial-inclusion-initiatives-money-launderers-playground-expert-talk.pdf

Thomas Reuters 2015 *Financial inclusion initiatives: Money launders playground* https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/expert-talk/financial-inclusion-initiatives-money-launderers-playground-expert-talk.pdf accessed 27 November 2015

Traynor and Butler 2015 http://theguardian.com/global-development-professionals-network/2015/sep/24/mobile-money-apps-security-flaws-study-reveals

Traynor P and Butler K 2015 *Mobile money in developing countries: study reveals security flaws in apps* The Guardian http://theguardian.com/global-development-professionals-network/2015/sep/24/mobile-money-apps-security-flaws-study-reveals accessed 2 September 2015

Tubbs B 2014 http://itweb.co.za/index.php?option=com_content&view=article&id=136282&t ITWeb telecoms

Tubbs B 2014 *Land grab' in mobile payment space* ITWeb http://itweb.co.za/index.php?option=com_content&view=article&id=136282&t ITWeb telecoms accessed 2 September 2015

Unknown 1929 International Convention for the Suppression of Counterfeiting Currency of 1929 http://*paclii.org/pits/en/treaty_database/1929/3.rtf*

Unknown 1929 International Convention for the Suppression of Counterfeiting Currency of 1929 http://*paclii.org/pits/en/treaty_database/1929/3.rtf* accessed 26 September 2016

Unknown unknown date http://investopedia.com/terms/l/laissezfaire.asp

Unknown unknown date *Definition of Laissez-faire* http://investopedia.com/terms/l/laissezfaire.asp accessed 10 February 2016

United Nations 1988 https://unodc.org/pdf/convention_1988_en.pdf

United Nations 1988 *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* https://unodc.org/pdf/convention_1988_en.pdf accessed 25 January 2016

United Nations 1999 https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf

United Nations 1999 *International Convention on the Suppression of the Financing of Terrorism* https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf accessed 25 January 2016

*United Nations* 2003 and 2004 http://un.com

United Nations 2003 and 2004*United Nations Security Council Resolution 1516 (2003) and 1530 (2004)* http://un.com accessed 12 April 2012

United Nations Treaty Collection unknown date https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en

United Nations Treaty Collection unknown date *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substance, Vienna 20 December 1988* https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en accessed 25 January 2016

United Nations Office on Drugs and Crime 2008 https://unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf,

United Nations Office on Drugs and Crime 2008 *Toolkit to Combate Trafficking of Persons* https://unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_3-5.pdf accessed 29 September 2016

U.S. Government Accountability Office 2009 http://defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf

U.S. Government Accountability Office, Statement for the Record to the Sub-Committee on Terrorism and Homeland Security, Sen. Cybersecurity. Continued efforts are needed to protect information systems form evolving treats 3 n. 3 (2009), available at http://defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf accessed 17 September 2015

Villasenor 2013 http://brookings.edu/research/papers/2013/09/16-smartphones-mobile-money-developing-countries-villasenor

Villasenor J 2013 *Issues in Technology Innovations: Smartphones for the Unbanked: How Mobile Money Will Drive Digital Inclusion in Developing Countries September 2013* http://brookings.edu/research/papers/2013/09/16-smartphones-mobile-money-developing-countries-villasenor accessed 29 July 2014.

Vodacom unknown date http://vodacom.co.za/vodacom/services/financial-solutions/m-pesa

Vodacom unknown date *M-pesa* http://vodacom.co.za/vodacom/services/financial-solutions/m-pesa accessed 18 April 2016

Writer 2016 http://itweb.co.za/index.php?option=com_content&view=article&id=153515:Mobile-international-remittances-to-exceed-25bn-by-2018

Writer S 2016 Mobile international remittances to exceed $25bn by 2018 http://itweb.co.za/index.php?option=com_content&view=article&id=153515:Mobile-international-remittances-to-exceed-25bn-by-2018 accessed 20 June 2016

Weber 2013 http://theweek.com/articles/464499/great-atm-heist-how-thieves-brazenly-stole-45-million-few-hours

Weber P 2013 The *great ATM heist: How thieves brazenly stole $45 million in a few hours* http://theweek.com/articles/464499/great-atm-heist-how-thieves-brazenly-stole-45-million-few-hours accessed 15 January 2015

WebFinance Inc., Invertor Words 2015 http://investorwords.com/2587/intrinsic_value.html

WebFinance Inc., Invertor Words 2015 What is Intrinsic Value? http://investorwords.com/2587/intrinsic_value.html accessed 15 January 2015

Working Group of the European Payment Systems 1994 http://ecb.europa.eu/pub/pdf/other/prepaidcards1994en.pdf?9fc7b56c72b0b1a42eb60ab5f97fb7d3

Working Group of the European Payment Systems 1994 *Prepaid Cards: Report to the Council of the European Monetary Institute* http://ecb.europa.eu/pub/pdf/other/prepaidcards1994en.pdf?9fc7b56c72b0b1a42eb60ab5f97fb7d3 accessed 10 February 2016

Wolfsberg Group 2002 http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_(2002).pdf.

Wolfsberg Group 2002 *Wolfsberg Statement on the Suppression of the Financing of Terrorism* http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_(2002).pdf accessed 23 March 2016

Wolfsberg Group 2011 http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf

Wolfsberg Group 2011 *Guidance on Prepaid and Stored Value Cards* http://wolfsberg-principles.com/pdf/standards/Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14,_2011.pdf accessed 2 February 2016

World Bank 2008

http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf

World Bank 2008 *Mobile Money Methodology for Assessing Money Laundering* http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf accessed 11 January 2013

World Bank 2015

http://worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report

World Bank 2015 *Massive Drop in Numbers of Unbanked, says New Report* http://worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report accessed 15 August 2016

Wray 2010 http://e1.newcastle.edu.au/coffee/pubs/workshops/12_2001/carlson.pdf

Wray LR 2010 *Understanding Modern Money Workshop: Understanding Unemployment in Australia, Japan and the USA*. http://e1.newcastle.edu.au/coffee/pubs/workshops/12_2001/carlson.pdf accessed 16 January 2014

# List of Abbreviations

| | |
|---|---|
| ATMs | Automated teller machine |
| *Banks Act* | *The Banks Act* 94 of 1990 |
| CDD | Client due diligence |
| FATF | Financial Action Task Force |
| *FIC Act* | *The Financial Intelligence Centre Act* 38 of 2001 |
| FIC | Financial Intelligence Centre |
| FinSurv | Financial Surveillance Department |
| e-banking | Electronic banking |
| EDD | Enhanced due diligence |
| e-money | Electronic money |
| EPC | European Parliament and the Council |
| GG | Government Gazette |
| GN | Government Notice |
| GSMA | *Groupe Speciale* Mobile Association |
| KYC | Know-your-client |
| m-banking | Mobile banking |
| ML | Money laundering |
| Regulations | *Money Laundering and Terrorist Financing Control Regulations* |
| MNOs | Mobile-network operators |
| m-money | Mobile money |
| *NPS Act* | *National Payment Systems Act* 78 of 1998 |
| OECD | Organisation for Economic Co-operation and Development |
| *POCA* | *Prevention of Organised Crime* Act 121 of 1998 |
| *POCDATARA* | *The Protection of Constitutional Democracy against Terrorist and Related Activities Act* 33 of 2004 |

| | |
|---|---|
| RBA | Risk-based approach |
| *SARB Act* | *South African Reserve Bank Act* 90 of 1989 |
| TLR | Texas Law Review |
| TF | Terrorist financing |
| TSAR | Tydskrif vir die Suid-Afrikaanse Reg |
| Wolfsberg Group | Wolfsberg Group of International Financial Institutions |