Anti-money laundering regulations and the effective use of mobile money in South Africa

M Kersop

21119392

Mini-Dissertation submitted in partial fulfillment of the requirements for the degree *Magister Legum* in

Import and Export Law

at the Potchefstroom Campus of the North-West University

Supervisor: Prof SF du Toit

2014

INDEX

Abstract		iii
Opsomming		iv
List of abbreviations		v
1	Introduction and problem statement	1
1.1	Demarcation and scope	8
2	Mobile money	9
2.1	Introduction	9
2.2	What is mobile money?	9
2.2.1	A brief history of mobile money	12
2.2.2	Nature and characteristics of mobile money	13
2.2.3	Different mobile money business models today	16
2.2.3.1	The operator-centric model	16
2.2.3.2	The bank-centric model	17
2.2.3.3	The peer-to-peer model	18
2.2.3.4	The collaboration model	18
2.3	Regulation of mobile money in South Africa, with specific focus on AML measures	19
2.4	Conclusion	22
3	Money laundering and the anti-money laundering framework in South Africa	22
3.1	Introduction	22
3.2	What is money laundering?	23
3.3	Anti-money laundering measures in South Africa	25
3.3.1	The *Financial Action Task Force Recommendations*	26
3.3.2	*Prevention of Organised Crime Act* 121 of 1998	27
3.3.3	*Financial Intelligence Centre Act* 38 of 2001	29
3.3.4	The establishment and verification of identities of clients as an AML measure	32
3.4	Conclusion	38
4	Mobile money, money laundering and the risk-based approach	39
4.1	Introduction	39

4.2	Financial integrity risks linked to mobile money: perceptions versus reality	39
4.2.1	Perceived financial integrity risks of mobile financial services	40
4.2.1.1	Unknown identity	40
4.2.1.2	False identification	40
4.2.1.3	Smurfing	40
4.2.1.4	Transaction Speed	41
4.2.1.5	Pooling and delegation	41
4.2.1.6	Lack of regulation	41
4.2.2	Proven financial integrity risks of mobile financial services	42
4.2.2.1	Anonymity	42
4.2.2.2	Elusiveness	43
4.2.2.3	Rapidity	43
4.2.2.4	Poor oversight	44
4.3	Customer due diligence, mobile money and the risk-based approach	46
4.3.1	Simplified customer due diligence, mobile money and the FATF	49
4.3.2	Mitigating measures which facilitate the application of simplified customer due diligence	52
4.4	South Africa and the risk-based approach in terms of customer due diligence	54
4.5	Conclusion	56
5	Conclusion and recommendations	56
Reference list		60

ABSTRACT

Mobile financial services, specifically mobile money, has the potential to expand access to financial services to millions of unbanked people in South Africa. As such, it looks very promising in terms of financial inclusion. However, concerns exist that mobile money can be detrimental to financial integrity since there are several proven risk factors linked to mobile financial services. These risk factors make mobile money very susceptible to money laundering. The potential for abuse and the need for appropriate controls is therefore something which cannot be ignored.

While the South African legislator has made provision for comprehensive anti-money laundering preventative measures by means of the *Financial Intelligence Centre Act* 38 of 2001, there exists no South African legislation explicitly concerned with mobile money. It is therefore difficult to determine what the regulatory stance is in terms of mobile money in South Africa. The Financial Action Task Force (FATF) is, however, currently focusing attention on the effect which mobile money may have on financial integrity. The latest *FATF Recommendations* make provision for several anti-money laundering controls which are specifically applicable to mobile money, including controls regarding money or value transfer services and new technologies.

While it is always difficult to balance financial integrity and financial inclusion, the risk-based approach makes it possible for governments to implement effective anti-money laundering measures, thereby preserving financial integrity, without the need to compromise on financial inclusion objectives. The fact that South Africa has not fully adopted a risk-based approach is a problem which needs to be addressed if mobile money is to deliver on its promises for financial inclusion, without being detrimental to financial integrity.

Keywords: mobile money – financial inclusion – financial integrity – risk-based approach

OPSOMMING

Mobiele finansiële dienste, spesifiek mobiele geld, beskik oor die potensiaal om toegang tot finansiële dienste aan miljoene mense sonder bankrekenings in Suid-Afrika uit te brei. As sulks lyk dit baie belowend in terme van finansiële insluiting. Daar bestaan egter kommer dat mobiele geld nadeling vir finansiële integriteit kan wees, aangesien daar verskeie bewese risiko-faktore bestaan wat verband hou met mobiele finansiële dienste. Hierdie risiko-faktore maak mobiele geld baie vatbaar vir geldwassery. Die potensiaal vir misbruik en die behoefte aan die nodige kontrole is dus iets wat nie geïgnoreer kan word nie.

Terwyl die Suid-Afrikaanse wetgewer voorsiening gemaak het vir omvattende voorkomende maatreëls ten einde geldwassery te bekamp, deur middel van die *Financial Intelligence Centre Act* 38 van 2001, bestaan daar geen Suid-Afrikaanse wetgewing wat uitdruklik met mobiele geld gemoeid is nie. Dit is dus moeilik om te bepaal wat die regulerende standpunt in terme van mobiele geld in Suid-Afrika is. Die *Financial Action Task Force* (FATF) fokus egter tans aandag op die uitwerking wat mobiele geld op finansiële integriteit kan hê. Die nuutste *FATF Recommendations* maak voorsiening vir anti-geldwassery kontroles wat spesifiek van toepassing is op mobiele geld, insluitend beheermaatreëls ten opsigte van geld- of waarde-oordragdienste en nuwe tegnologie.

Ten spyte van die feit dat dit moeilik is om ‘n balans tussen finansiële integriteit en finansiële insluiting te handhaaf, maak die risiko-gebaseerde benadering dit moontlik vir regerings om effektiewe anti-geldwassery maatreëls te implementeer en sodoende finansiële integriteit te behou, sonder om finansiële insluitingsdoelwitte hoef prys te gee. Die feit dat Suid-Afrika nog nie ‘n ten volle risiko-gebaseerde benadering aangeneem het nie, is 'n probleem wat aangespreek moet word ten einde die effektiewe gebruik van mobiele geld vir finansiële insluiting te verseker, sonder om nadelige gevolge vir finansiële integriteit in te hou.

Sleutelwoorde: mobiele geld – finansiële insluiting – finansiële integriteit – die risiko-gebaseerde benadering

LIST OF ABBREVIATIONS

AML	Anti-money laundering
ATM	Automated teller machine
CDD	Customer due diligence
CFT	Countering the financing of terrorism
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	*Financial Intelligence Centre Act* 38 of 2001
JICLT	*Journal of International Commercial Law and Technology*
MNO	Mobile network operator
MVTS	Money or value transfer services
NPPS	New payment products and services
POCA	*Prevention of Organised Crime Act* 121 of 1998
SMS	Short message service
WJLTA	*Washington Journal of Law, Technology & Arts*
WAP	Wireless application protocol

1 Introduction and problem statement

Mobile technology[1] affects the lives of billions of people worldwide[2] and has transformed the way in which not only communication, but also business transactions, take place.[3] It is a valuable medium and crucial piece of infrastructure which supports a number of economic sectors.[4] In terms of financial services,[5] the development of mobile technology has shown unique opportunities and allowed almost three billion people without bank accounts to gain access to financial services.[6] This is a significant achievement, since sparse availability of financial services is one of the most prominent restrictions on economic development.[7] While this is a worldwide phenomenon, it is particularly true for rural areas in Sub-Saharan Africa,[8] where low-income individuals have restricted access to traditional financial systems.[9] Exclusion from the financial system is also one of the most substantial obstacles preventing the eradication of poverty.[10] A recent report from the World Bank indicates that limited access to financial services keeps economic inequality alive and could also give rise to continuous disincentives for working and saving.[11]

---

1 The term "mobile technology" will be used as the collective term for mobile phones and mobile services. However, "mobile phones" and "mobile services" will also be referred to throughout this dissertation, if deemed necessary by the context.

2 World Bank's Working Paper number 146, entitled *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing,* hereinafter referred to simply as World Bank Working Paper no.146 xiii, 1.

3 Jobodwana *JICLT* 287; World Bank Working Paper no.146 xiii.

4 Such as commerce, health insurance, banking and agriculture, among others. See Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 57.

5 The term "financial services" will be used as a collective term for facilities such as savings accounts and money transfers generally provided by banks, credit unions, and finance companies. See BusinessDictionary.com 2014 http://www.businessdictionary.com in this regard.

6 World Bank Working Paper no.146 1.

7 Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 58.

8 Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 58.

9 A financial system can be described as a system that allows the transfer of money between investors and borrowers. It comprises a set of closely interconnected financial institutions, markets, instruments, services, practices, and transactions. See O'Sullivan and Sheffrin *Economics: Principles in Action* 551; Gurusamy *Financial Services and Systems* 3 in this regard. Factors that prevent access to financial systems include high service costs, geographic inaccessibility of bank branches and ATMs, and negative perceptions of financial service providers.

10 The reason for this being that the lack of financial instruments such as accounts places a limitation on the ability of businesses and consumers to save, repay debts and manage risk. See Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 58 in this regard.

11 World Bank Working Paper no.146 7-8.

Financial inclusion, which can be defined as "ensuring access to appropriate financial products and services at an affordable cost in a fair and transparent manner",[12] has therefore become an increasingly important international policy initiative in the fight against poverty.[13]

Financial inclusion, in other words, entails providing financially excluded individuals[14] such as low-income, rural and undocumented persons who often have no other option than making do with cash and physical assets,[15] with access to a sufficient variety of convenient, secure and inexpensive financial services.[16] Financial inclusion also entails providing individuals who only have access to rudimentary financial services with a more extensive variety of financial services.[17]

Increased financial inclusion can be achieved by means of mobile money, which enables the storage of monetary value on a mobile phone.[18] This stored value can be used to make payments and/or purchases or it can be sent to other mobile money users who can then store it on their own mobile phones and utilise it for payments and purchases if the user so wishes.[19] Mobile money can also be redeemed for cash[20] and cash can be converted into mobile money by depositing it into a mobile money account.[21] Mobile money is thus at the crossroads of mobile technology and financial services[22] and as such, it is a financial inclusion initiative which presents a

12 Financial inclusion is sometimes also simply defined as providing access to financial services for all. See *FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* 17, hereinafter referred to as *FATF Guidance: AML and Financial Inclusion.* References to this source will be in terms of paragraph numbers.

13 De Koker 2011 *Journal of Financial Crime* 362.

14 *FATF Guidance: AML and Financial Inclusion* 17. "Financial exclusion" will be used as an opposite of "financial inclusion", i.e. individuals who fall outside of a financial system and are in need of financial inclusion, are currently financially excluded.

15 Alexandre and Eisenhart 2013 *WJLTA* 288; Jenkins "Developing Mobile Money Ecosystems" 5. Dealing with cash has inherent risks and costs which are excluded or at least mitigated by financial inclusion.

16 *FATF Guidance: AML and Financial Inclusion* 17.

17 *FATF Guidance: AML and Financial Inclusion* 17.

18 World Bank Working Paper no.146 74; Alexandre and Eisenhart 2013 *WJLTA* 287. A more comprehensive definition of mobile money can be found in Chapter 2, where the concept of mobile money is explored in greater detail.

19 World Bank Working Paper no.146 27; Alexandre and Eisenhart 2013 *WJLTA* 287; Lawack 2013 *WJLTA* 319; GSMA 2013 https://mobiledevelopmentintelligence.com.

20 World Bank Working Paper no.146 27, 74; Alexandre and Eisenhart 2013 *WJLTA* 287; Lawack 2013 *WJLTA* 319; GSMA 2013 https://mobiledevelopmentintelligence.com.

21 Alexandre and Eisenhart 2013 *WJLTA* 288; Lawack 2013 *WJLTA* 319.

22 Alexandre and Eisenhart 2013 *WJLTA* 288.

uniquely sustainable, accessible solution to the problem that is financial exclusion.[23] The reason why mobile money is so uniquely positioned to drive change[24] in terms of financial inclusion, is because the mobile phone is the most widely adopted form of modern technology in history.[25] In 2006, the mobile phone became the first communications technology to have more users in third world countries than in first world countries.[26] Today, mobile technology is readily obtainable by low-income individuals and remote populations[27] and almost half the world owns a mobile phone.[28] When comparing this vast amount of people who have access to mobile phones with the amount of people who do not have bank accounts, it becomes clear that there is a large overlap between these two groups worldwide: more than one billion individuals in developing markets have access to a mobile phone, but not to a bank account.[29] Mobile technology offers novel alternatives to access financial services,[30] with the potential of mobile financial services being contained in the delivery platform.[31] Mobile technology is not subject to the restraints of infrastructure and expensiveness that have customarily prevented banks and other financial institutions from being accessible to the poor.[32] It is for this reason that banks, mobile network operators (MNOs), and other non-bank institutions[33] have developed methods to harness mobile technology in a manner which has effectively brought financial services within the grasp of unbanked,[34] low-income individuals

23 GSMA 2013 https://mobiledevelopmentintelligence.com.
24 GSMA 2013 https://mobiledevelopmentintelligence.com.
25 GSMA 2013 https://mobiledevelopmentintelligence.com.
26 In 2006, more than 60 percent of all mobile phone subscribers were situated in developing countries. See World Bank Working Paper no.146 8 in this regard.
27 World Bank Working Paper no.146 xiii.
28 World Bank Working Paper no.146 vii.
29 GSMA 2013 https://mobiledevelopmentintelligence.com; Jenkins "Developing Mobile Money Ecosystems" 5; *G20 Principles for Innovative Financial Inclusion*.
30 World Bank Working Paper no.146 xiii.
31 World Bank Working Paper no.146 vii; Jenkins "Developing Mobile Money Ecosystems" 5.
32 World Bank Working Paper no.146 vii.
33 Such as airtime sales agents, retailers and utility companies. See Jenkins "Developing Mobile Money Ecosystems" 7 in this regard.
34 This includes micro-entrepreneurs, low-income earners and the poor, according to Schoombee 2004 *South African Journal of Economics* 581. According to Coetzee, characteristics of the unbanked in South Africa are that they typically do not have any form of transactional account, tend to be less well educated, reside in rural areas and townships, are mostly black or coloured, and lack a steady cash flow. A large proportion of the unbanked have no formal evidence of any form of credit history and are not banking product literate. See Coetzee 2009 *South African Journal of Economic and Management Sciences* 450. According to Lawack, "the unbanked" refers to individuals who do not have bank accounts and who do their "banking" through informal means. See Lawack 2013 *WJLTA* 317 in this regard.

worldwide[35] – individuals who have historically been deprived of access to these services, but the majority of whom now have access to a mobile phone.[36]

What makes mobile money even more beneficial is the fact that mobile financial service systems can be integrated into pre-existing mobile network technology, which results in less infrastructural strain than traditional banking.[37] This is especially true in cases where extensive prepaid mobile phone systems[38] are already in place and can be utilised for mobile money.[39] Mobile financial services are likely to expand as market penetration of mobile technology increases. Indeed, mobile financial services have already developed to include services such as mobile finance,[40] mobile banking[41] and mobile payments.[42]

No other form of financial service offers the intrinsic mobility comparable to that of mobile financial services,[43] and incentives for the escalating availability of mobile financial services may include the dire need for financial services exhibited by unbanked individuals, political drive to make access to financial services attainable by individuals residing in rural areas,[44] and the necessity to remove geographical barriers to financial inclusion.[45]

---

35 World Bank Working Paper no.146 vii, 1.
36 GSMA 2013 https://mobiledevelopmentintelligence.com.
37 World Bank Working Paper no.146 8 -9; Jenkins "Developing Mobile Money Ecosystems" 5.
38 In the mobile phone industry, "prepaid" refers to a type of mobile phone account that requires the purchase of call credit before services can be used. A prepaid client of an MNO would, for example, purchase a R50 prepaid token from a retailer which could then be used to fund an account with, allowing the owner of the account to use R50 worth of voice minutes, text messages, or data. See Anon 2013 http://www.mobileburn.com in this regard.
39 World Bank Working Paper no.146 8 -9.
40 Which includes credit, insurance and savings. See Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 57.
41 Which can be divided into transactional and informational mobile banking. See Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 57.
42 Which includes person-to-person, government-to-person and business-to-business payments. See Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 57.
43 Features which contribute to this marked mobility include low infrastructural requirements; competitive advantages like low costs, increased convenience, and small transactions amounts; security features; and the ability to make cross-border remittances. See World Bank Working Paper no.146 8 in this regard.
44 Rural population refers to people living in rural areas as defined by national statistical offices. It is calculated as the difference between total population and urban population. Population is based on the de facto definition of population, which counts all residents regardless of legal status or citizenship – except for refugees not permanently settled in the country of asylum, who are generally considered part of the population of the country of origin. See Anon 2013 www.tradingeconomics.com in this regard.
45 World Bank Working Paper no.146 8-9.

Mobile money is currently experiencing a revival in South Africa. An example of this is the recent re-launch of M-PESA.[46] A large drive in the development of mobile money in South Africa is the objective of implementing policies which further financial inclusion while observing anti-money laundering (AML) and countering the financing of terrorism (CFT) standards.[47] It is submitted that the recent development in mobile money can also be contributed, at least in part, to the increasing market penetration level of mobile connections in South Africa.[48] The market penetration for mobile connections in South Africa was 133% in 2013,[49] amounting to more than 70 million connections.[50] This was the 4th highest market penetration figure in Africa for 2013. Another reason for the recent revival of mobile money in South Africa could be the fact that South Africa still has a reasonably large rural population, with an estimated 37.13% of the population being rural in 2013.[51] As mentioned previously, mobile money is specifically suitable to be implemented in areas where strong prepaid infrastructures exist. South Africa is in a favourable position in this respect, having a large number of prepaid connections: 83.78% of the total number of mobile phone connections in South Africa were prepaid in 2013.[52] South Africa is also a developing economy with a large sector of unbanked individuals and as such, the increasing amount of new payment products and services (NPPS)[53] using mobile

46 M-PESA was originally launched in South Africa in 2010 after the great success it achieved in Kenya, but did not achieve the same level of success in South Africa. See Goldstuck 2014 http://mg.co.za in this regard.

47 World Bank Working Paper no.146 4.

48 Lawack 2013 *WJLTA* 317.

49 GSMA 2013 https://mobiledevelopmentintelligence.com.

50 GSMA 2013 https://mobiledevelopmentintelligence.com.

51 The last time a formal measurement of urban vs rural population was conducted in South Africa, was in 2010 when it was found that 38.30% of the country's population was rural. See Anon 2012 www.southafrica.info; Anon 2013 www.tradingeconomics.com and GSMA 2013 https://mobiledevelopmentintelligence.com in this regard.

52 GSMA 2013 https://mobiledevelopmentintelligence.com

53 NPPS are new and innovative payment products and services that offer an alternative to traditional financial services. NPPS include a variety of products and services that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations. NPPS include, inter alia, prepaid cards, mobile payment services, and Internet-based payment services. The FATF makes specific provision for the regulation of NPPS. See *FATF Guidance for a Risk-Based Approach (2013): Prepaid Cards, Mobile Payments and Internet-Based Payment Services* 3, hereinafter simply referred to as *FATF Guidance for a Risk-Based Approach.* References to last-mentioned source will be in terms of paragraph numbers.

technology to expand access to the financial system holds great promise for financial inclusion.[54] However, the majority of these initiatives are yet to reach scale.[55]

It is submitted that this can be partly attributed to challenges which have surfaced with respect to the effective application of AML/CFT measures to NPPS – specifically to mobile financial services.[56] Concerns have been raised about potential exploitation of mobile technology for illegal means.[57] As already mentioned, mobile phones are used by billions of people around the world. This includes criminals and terrorists.[58] Mobile money thus has inherent financial integrity[59] risks namely the risk of money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction.[60] Concerns also exist that mobile money can be additionally detrimental to financial integrity as it increases the speed of transactions.[61] Regulation of mobile money, especially when issued by mobile operators, is also a source of apprehension.[62] While it is clear that mobile financial services can enhance the lives of many people in developing countries, the potential for abuse and the need for appropriate controls is something which cannot be ignored.[63]

In this regard, the Financial Action Task Force (FATF) is presently placing focus on the consequences that mobile money could possibly hold for financial integrity. South Africa is one of the 36 members of the FATF[64] – an inter-governmental body which develops and advances policies aimed at safeguarding the global financial

54 GSMA 2013 https://mobiledevelopmentintelligence.com; *FATF Guidance: AML and Financial Inclusion* 30; *FATF Guidance for a Risk-Based Approach* 3.

55 GSMA 2013 https://mobiledevelopmentintelligence.com; *FATF Guidance: AML and Financial Inclusion* 30.

56 These challenges are created by the rapid development, increased functionality, and growing use of NPPS globally and governments and private sector institutions have equally daunting tasks in ensuring that NPPS are not misused for money laundering and terrorist financing purposes. See *FATF Guidance: AML and Financial Inclusion* 30; *FATF Guidance for a Risk-Based Approach* 3 in this regard.

57 World Bank Working Paper no.146 2.

58 World Bank Working Paper no.146 2.

59 "Financial integrity" is the integrity of the financial system (see fn 9 above for an explanation of what a financial system is). Financial integrity is an interest which must be protected against certain threats or risks which will be mentioned in the main text. See Van Duyne *Criminal Finance and Organising Crime in Europe* 75 in this regard.

60 Winn and De Koker 2013 *WJLTA* 156; World Bank Working Paper no.146 2. Money laundering will be discussed in more detail in Chapter 3.

61 Alexandre and Eisenhart 2013 *WJLTA* 287.

62 Alexandre and Eisenhart 2013 *WJLTA* 287.

63 De Koker 2013 *WJLTA* 195.

64 South Africa joined the FATF in 2003 and held the presidency in 2005/6.

system from financial integrity risks.[65] The *FATF Recommendations*[66] are observed by more than 180 countries, and are universally acknowledged as the international standard for AML/CFT.[67] The FATF's primary mandate is to see to it that financial integrity risks are addressed effectively. This includes the responsibility of ensuring that including more people in the financial system does not come at the expense of weakening effective AML/CFT measures. The FATF does, however, concede that a so-called "overly cautious approach" to AML/CFT measures can inadvertently lead to the exclusion of legitimate individuals from the financial system.[68] AML/CFT measures should therefore be designed in such a way that it does not prevent unbanked and financially excluded persons from having access to formal financial services.[69]

South Africa has been hailed as one of the foremost jurisdictions as far as financial inclusion is concerned, but while a supportive framework for mobile money has been developed, this framework is not fully inclusive.[70] It would seem that while the market penetration level of mobile phones in South Africa is ever-increasing,[71] the regulatory framework for mobile financial services is, as Lawack[72] puts it, "still not entirely conducive to greater financial inclusion."

From the above it is clear that mobile money presents great prospects for increased financial inclusion, since mobile phones are likely to become a common tool in performing financial transactions to a global extent in the not too distant future.[73] However, since it is a daunting task to find an equilibrium between financial integrity and financial inclusion, the expansion of access to financial services to impoverished South Africans could be hindered if rigid AML/CFT measures are not amended to make provision for wider financial inclusion. The question therefore is: how can the preservation of financial integrity and the promotion of financial inclusion be

65 Guidance Note 3A as issued by the South African FIC in 2013; FIC 2013 https://www.fic.gov.za/DownloadContent/NEWS/ PRESSRELEASE/FIC%20Annual% 20 Report %202012-13.pdf.
66 The *FATF Recommendations* will be discussed in detail in Chapter 3.
67 *FATF Recommendations* 7.
68 *FATF Guidance for a Risk-Based Approach* 2.
69 *FATF Guidance for a Risk-Based Approach* 3.
70 Winn and De Koker 2013 *WJLTA* 161.
71 Lawack 2013 *WJLTA* 317.
72 Lawack 2013 *WJLTA* 317.
73 World Bank Working Paper no.146 xiii.

balanced in such a way that mobile money can be utilised and developed effectively, thereby promoting financial inclusion, without being detrimental to financial integrity? In order to do this, it is necessary to investigate what actual threats mobile money holds for financial integrity and to what extent the potential of financial inclusion which mobile money holds is inhibited by AML regulations which are aimed at protecting financial integrity.

The purpose of this dissertation will thus be to determine to what extent current AML regulations in South Africa make provision for the effective use of mobile money. This will be done by firstly examining the concept of mobile money and how it is regulated in South Africa. Thereafter, attention will be turned to money laundering and the current AML framework in South Africa. Finally, mobile money will be viewed in the light of the actual and perceived money laundering risks it poses and how this can be managed effectively. This analysis will be done with reference to instruments from the FATF, such as the *FATF Recommendations*, as well as South African legislation.

1.1 Demarcation of scope of dissertation

The scope of this dissertation will be narrowed down extensively due to space constraints. Firstly, it must be noted that while money laundering and the financing of terrorism and proliferation usually go hand in hand,[74] for purposes of this dissertation focus will fall only on money laundering and not on the financing of terrorism. Reference will thus only be made to money laundering and not to financing of terrorism.

As far as mobile money is concerned, attention will be focused on mobile money as an independent method of payment or transfer only, and not on extended mobile financial service products such as mobile securities account services or mobile banking.[75] Furthermore, the discussion of the regulation of mobile money will mostly

74 As is evident from instruments such as that of the FATF and in academic works involving the topic of threats to financial integrity.

75 Chapter 2 will contain a discussion of different categories of mobile financial services in order to provide appropriate context for the discussion of mobile money which will follow in the same chapter.

be limited to the aspect of AML measures and not general regulation of mobile money.[76] The scope of AML measures which will be discussed will be narrowed down to AML preventative measures,[77] and even more specifically to customer due diligence (CDD)[78] only, with specific focus on the establishment and verification of identities of clients as AML measure.

2 Mobile Money

2.1 Introduction

The focus of this chapter will be the nature, history and regulation of mobile money. In the first part of the discussion, the World Bank's Working Paper number 146 (*Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing*) will be used as a point of departure to illustrate that mobile money is just one of several forms of mobile financial services. Mobile money as such will then be explored with reference to the nature, history and regulation thereof. It will become clear throughout this chapter that mobile money is an important tool for aiding financial inclusion.

2.2 What is mobile money?

Mobile money services is one of four main mobile financial services, the other three being mobile financial information services, mobile bank and securities accounts services, and mobile payment services.[79] These services often work in parallel and in some circumstances one service operates as a basis for the others.[80] The more a specific mobile financial service model deviates from traditional financial service

76 General regulation will be discussed as far as it is pertinent to making certain determinations regarding mobile money, such as whether mobile money providers are financial service providers or not, in as far as it is has bearing on AML measures which are applicable to it or not.

77 Reference throughout this dissertation to "AML measures" will mean "AML preventative measures", unless context indicates otherwise.

78 Customer due diligence (CDD) is also referred to as "know your customer (KYC)". For purposes of uniformity, the term CDD will be used throughout this dissertation.

79 World Bank Working Paper no.146 xiii.

80 World Bank Working Paper no.146 xiii.

models, the more its accompanying risks, but also its likelihood for furthering financial inclusion, increases.[81]

Mobile financial services differ from other electronic financial services because the technology which is used for the former is flexible and usually easily accessible.[82] Mobile financial services are provided by means of platforms such as short message service (SMS) or application standards such as wireless application protocol (WAP), which are unique to mobile phones.[83]

Each of the mobile financial services previously mentioned, excluding mobile money services, will be briefly discussed in order to place mobile money into the perspective of the bigger framework of mobile financial services. This will be followed by an extensive discussion of mobile money services.

Mobile financial information services is the most frequently used mobile financial service. It enables clients to observe personal account data such as their "account balance statements, transaction history records, receipts and confirmations for credit/debit card transactions, and credit limit alerts" as well as general financial information such as exchange rates and stock quotes.[84] All this is done without performing transactions.[85]

Mobile bank and securities account services give already existing bank and securities account holders the option to initiate transactions by means of their mobile phones.[86] Mobile bank account services are similar to transactions performed via other electronic means of banking such as automated teller machines (ATMs) or online banking.[87] Mobile securities account services are used for trading securities from a client's already existing securities account,[88] by means of mobile phone. These services are widespread, since it evolved from mobile financial information

81 World Bank Working Paper no.146 xiii.
82 Compared to, for example, "Internet" or "online" banking, which requires an Internet connection and a computer. See World Bank Working Paper no.146 8.
83 World Bank Working Paper no.146 8-9.
84 World Bank Working Paper no.146 20.
85 World Bank Working Paper no.146 20.
86 World Bank Working Paper no.146 21.
87 World Bank Working Paper no.146 21.
88 World Bank Working Paper no.146 21.

services after clients displayed a need therefor.[89] Examples of these services include transfers,[90] settlement of balances,[91] securities' transactions,[92] and foreign exchange operations.[93] South African banks have utilised mobile phones as a mechanism to provide branchless banking to lower-income individuals who do not have the means to obtain a traditional bank account, thereby expanding access to financial services.[94]

Mobile payment services afford individuals without bank or securities accounts the opportunity to make payments[95] by means of mobile phones. Mobile payment services are distinctly different from mobile bank and securities account services despite the fact that transactions may be processed by a bank, with the distinction lying in the fact that mobile payment services are not dependent of an account with a traditional financial institution.[96] As such, mobile payment services can be carried out through non-bank entities, which is indeed often the case.[97] As payment systems[98] advance with new technologies, mobile payments are likely to enjoy increased popularity since it is not subject to the same restrictions as bank-based services or mobile bank and securities account services.[99] It should be noted that while mobile money (which will be discussed momentarily) also makes provision for mobile payments, mobile payment services entail payments exclusively and do not include other services such as, for example, transfers between individuals.

89 World Bank Working Paper no.146 21. Since mobile financial information services is the most frequently used mobile financial service, it stands to reason that the service which developed from it due to client demand would gain popularity on a large scale.
90 Including person-to-person and person-to-business transfers. See World Bank Working Paper no.146 21.
91 Such as bill and credit card balances. See World Bank Working Paper no.146 22.
92 Such as stock transactions. See World Bank Working Paper no.146 22.
93 World Bank Working Paper no.146 22.
94 World Bank Working Paper no.146 22.
95 This includes payment of goods (i.e. purchases at retail stores) and utility and other bills.
96 *FATF Guidance for a Risk-Based Approach* 11. See also World Bank Working Paper no.146 26.
97 Such as a credit card company.
98 A payment system is defined by s1 of the *National Payment System Act* 78 of 1998 as "a system that enables payments to be effected or facilitates the circulation of money and includes any instruments and procedures that relate to the system."
99 For example, a user's mobile phone can be used to make payments at a merchant's point of sale terminal or as a payment instrument akin to debit cards. See World Bank Working Paper no.146 26.

This then brings the discussion to mobile money services. While the concept of mobile money was briefly explained in Chapter 1, it will now be revisited in greater detail.

2.2.1 A brief history of mobile money

Mobile money as we know it today exists thanks to a so-called "evolutionary process" which commenced with the expansion of mobile technology across the globe almost two decades ago.[100]

This process can be divided into stages. The first of these two stages can be associated with the inherent abilities of mobile phones in terms of data communication, which piqued the interest of banks and lead them to launch mobile information services, after which the variety of services gradually started expanding to also include mobile banking and securities accounts, as previously discussed.[101] These services collectively became known as "mobile banking."[102]

The second stage can be associated with the increased expansion of mobile technology which coincided with the advent of electronic money. This motivated experimentation with electronic money products of which the ability to initiate transactions through mobile phones were a fundamental design aspect. This stage also gave rise to the distribution network of agents[103] that function on a prepaid model. [104] Non-banking institutions played an increasingly greater role because of this, seeing as mobile money products and services are generally linked to prepaid accounts.[105] MNOs in particular have been successful providers of mobile money services.[106] Mobile financial services which are designed to facilitate an assortment of financial transactions by means of mobile phone[107] have seen the light of day in

100 *FATF Guidance for a Risk-Based Approach* 11.
101 Under par 3.1. See also *FATF Guidance for a Risk-Based Approach* 11 in this regard.
102 *FATF Guidance for a Risk-Based Approach* 11.
103 These agents are usually third parties or an entity who works for the mobile phone operator or bank. See Aker and Mbiti 2010 *Journal of Economic Perspectives* 220-221 in this regard.
104 *FATF Guidance for a Risk-Based Approach* 11.
105 *FATF Guidance for a Risk-Based Approach* 11.
106 *FATF Guidance for a Risk-Based Approach* 11.
107 Including transmitting airtime, paying bills, and transferring money between individuals. See Aker and Mbiti 2010 *Journal of Economic Perspectives* 220 in this regard.

several emerging markets[108] since 2005.[109] There are currently even a small amount of mobile money services in developing countries that make provision for international money transfers.[110]

Today, mobile money services are enabled by traditional financial service providers[111] and non-bank financial service providers[112] alike,[113] together with several different types of service providers as crucial partners[114] depending on the business model and technology which is employed.[115] Mobile money is an ever-expanding service, and as such, it is continually furthering financial inclusion.[116]

2.2.2 Nature and characteristics of mobile money

Mobile money services make provision for the use of mobile money or "m-money,"[117] which is a form of electronic currency,[118] or electronic money,[119] the value of which is

---

108 Defined by BusinessDictionary.com 2014 http://www.businessdictionary.com as "new market structures arising from digitalization, deregulation, globalization, and open-standards, that are shifting the balance of economic power from the sellers to the buyers. In such markets information is freely and widely available, and is almost instantly accessible. To compete in these scenarios, a firm must adopt new processes based information technologies, and must keep a close watch on the price, quality, and convenience trends." See also Khanna and Palepu 2010 http://www.forbes.com in this regard.

109 Aker and Mbiti 2010 *Journal of Economic Perspectives* 220-221.

110 Aker and Mbiti 2010 *Journal of Economic Perspectives* 220-221.

111 Such as banks, as defined by s 1 of the *Banks Act* 94 of 1990.

112 *FATF Guidance for a Risk-Based Approach* 13. These non-bank financial service providers are labelled by the FATF as money or value transfer services (MVTS) and will be discussed more extensively under par 2.3 below.

113 *FATF Guidance for a Risk-Based Approach* 13.

114 These partners include MNOs, and may include mobile telephone equipment manufacturers, telecommunications industry standards setting groups, payment networks, and software developers. See *FATF Guidance for a Risk-Based Approach* 13.

115 The different mobile money service business models will be discussed under par 2.2.3 below. In terms of technology used, business models use a range of approaches to facilitate mobile payments including text messaging, mobile Internet access, near field communication (NFC), programmed subscriber identity module (SIM) cards and unstructured supplementary service data (USSD). See *FATF Guidance for a Risk-Based Approach* 13 for more detail in this regard.

116 As discussed in Chapter 1. See also *FATF Guidance for a Risk-Based Approach* 12, 86 in this regard.

117 For the sake of convenience and clarity, the term "mobile money" will be used throughout this dissertation, rather than "m-money". Reference will also be made to "mobile payment systems" or "mobile payment services", since this is the terminology of choice used by the FATF in the *FATF Guidance For A Risk-Based Approach*.

118 Alexandre and Eisenhart 2013 *WJLTA* 288; World Bank Working Paper no.146 27.

119 According to the South African Reserve Bank, electronic money is 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. See the South African Reserve Bank's Position Paper on Electronic Money (2009) 3 in this regard. According to

either stored on a mobile phone, or linked to a mobile phone account which clients obtain once they have been registered for mobile money services.[120] Cash is thus converted into mobile money by depositing it into a mobile money account.[121] This stored value can be used to make payments and/or purchases[122] or it can be sent to other mobile money users[123] who can then store it on their own mobile phones and in turn use it to make payments or transfers.[124] Mobile money can also be converted into cash by means of a "withdrawal".[125] All of the above can be performed with minimal effort and expense[126] through a network of local transfer agents.[127] Mobile money comprises a primary account in its own right[128] and no prior existence of a bank account is necessary for mobile money services to be activated.[129] As such,

---

the World Bank, electronic money is a stored-value or prepaid product in which a record of the funds or value available to the client for multipurpose use, including transfers to other users and conversion to and from cash, is stored on an electronic device in the client's possession. Common uses are phone credits and airtime as tender that users can trade for other goods and services. See World Bank Working Paper no. 146 73 in this regard.

120 World Bank Working Paper no.146 27. 74; Alexandre and Eisenhart 2013 *WJLTA* 287; Aker and Mbiti 2010 *Journal of Economic Perspectives* 220-221.

121 Alexandre and Eisenhart 2013 *WJLTA* 287, 288; Lawack 2013 *WJLTA* 319; World Bank Working Paper no.146 27, 74; GSMA 2013 https://mobiledevelopmentintelligence.com https://mobiledevelopmentintelligence.com.

122 Which is either an over-the-counter service where an agent performs the transaction, or a so-called mobile wallet service where the client performs the transaction (see par 2.2.3.1 below for more detail regarding mobile wallets). Bill payments and payments of goods are included under the functionality of payment. Clients use the payment service primarily to pay utility bills. See GSMA 2013 https://mobiledevelopmentintelligence.com in this regard.

123 I.e. a mobile transfer of funds to a beneficiary takes place. This entails the transferring of cash from person-to-person via so called mobile wallets or "m-wallets". Transfers can be recurrent, which function as income support for the recipient, or used to send lump sums. See GSMA 2013 https://mobiledevelopmentintelligence.com https://mobiledevelopmentintelligence.com in this regard.

124 World Bank Working Paper no.146 27; Alexandre and Eisenhart 2013 *WJLTA* 287; Lawack 2013 *WJLTA* 319; GSMA 2013 https://mobiledevelopmentintelligence.com https://mobiledevelopmentintelligence.com.

125 World Bank Working Paper no.146 27. The withdrawal will be done via a local agent. See fn 127 below in this regard.

126 In general, each transaction will be subject to a transaction fee. See Aker and Mbiti 2010 *Journal of Economic Perspectives* 220-221. While this may seem counter-intuitive in the endeavour of providing affordable financial services to low-income individuals, it has been proven that clients are more willing to pay on a per transaction basis if they know that this will meet their needs, rather than having a "free" account which has various strict limitations and are ultimately of very little use, if any, to the client. See Alexandre and Eisenhart 2013 *WJLTA* 294-296 for more detail in this regard.

127 Alexandre and Eisenhart 2013 *WJLTA* 288; Lawack 2013 *WJLTA* 319. As previously stated, an agent is usually a third party or someone who works for the mobile phone operator or bank. The word "agent" in this sense should be construed as having the meaning of "distributor" and will usually be a retail outlet of sorts. See Aker and Mbiti 2010 *Journal of Economic Perspectives* 220 – 221 and *FATF Guidance for a Risk-Based Approach* 20 in this regard.

128 Lawack 2013 *WJLTA* 319; World Bank Working Paper no.146 74.

129 Alexandre and Eisenhart 2013 *WJLTA* 288; Lawack 2013 *WJLTA* 319. While not prevalent in South Africa, it is in fact possible for mobile money services to function completely independently of the banking system. In such instances, individuals can communicate directly with each other

mobile money makes it possible for clients to be financially linked by means of nothing more than a mobile phone.

An added benefit of mobile money is that it is exceptionally suitable for non-proximity situations,[130] given the fact that it provides a platform for transactions to be effected by means of a technological medium which is unsurpassed in terms of mobility.[131] Mobile money is therefore accessible to all mobile phone users and can be especially valuable to unbanked individuals since for many clients, such a mobile money account will be the first account they have ever held.[132]

While it is abundantly clear that mobile money services hold great financial inclusion potential, there are also other benefits linked to it. It could have an "overall positive impact on the economy" due to increased transaction speed and movement of money.[133] Mobile money could also eventually reduce dependency on cash, as well as the amount of cash in the economy within which it is utilised.[134] Payments by means of mobile money can furthermore contribute to promoting transparency[135] since electronic transactions are easier to trace than their cash counterparts.[136] As mentioned in Chapter 1, mobile money also plays an important role in supporting other economic sectors,[137] especially in emerging markets.[138]

---

regarding payments and receipts and an accounting system for recording debits and credits operates autonomously, with no requirement for payments to be channelled through a central clearing system (See the *National Payment System Act* 78 of 1998 with regard to clearing systems). This holds many advantages, such as the fact that payment is immediate and not subject to the delays of clearing systems; and it allows for participants to receive immediate records of transactions that enhance trust in the conduct of the parties to a transaction and the organisation facilitating the transaction. See Klein and Mayer *Mobile banking and financial inclusion: The regulatory lessons* 12 in this regard.

130 In terms of clients being geographically far-removed from both banks and their beneficiaries.

131 Alexandre and Eisenhart 2013 *WJLTA* 288-289.

132 Alexandre and Eisenhart 2013 *WJLTA* 288; Lawack 2013 *WJLTA* 319.

133 World Bank Working Paper no.146 27.

134 Winn and De Koker 2013 *WJLTA* 159; World Bank Working Paper no.146 27.

135 And, as such, combating corruption.

136 Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 57.

137 Such as commerce, health insurance, and agricultural banking, among others. See Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 57 in this regard.

138 Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012* 57.

From the aforementioned, it is clear that mobile money influences the advancement of financial services on several different levels.[139]

2.2.3 Different mobile money business models today

In order to address regulatory issues in terms of mobile money development and advancement, it is necessary to understand that the nature and operation of mobile money differs substantially from business model to business model, based on factors such as the service provider which has the primary function and the technical platform which is used.

As previously mentioned,[140] several different service providers can be involved in providing mobile money services.[141] This includes banks, MNOs, agents, and electronic money issuers.[142] These service providers have different functions in different mobile money service business models[143] and one service provider may be responsible for more than one function.[144] The different business models of mobile money services will be discussed accordingly.[145]

2.2.3.1 The operator-centric model

139 Alexandre and Eisenhart 2013 *WJLTA* 288.
140 Under par 2.2.1 above.
141 *FATF Guidance for a Risk-Based Approach* 20.
142 MNOs provide the technical platform to allow access to the funds through a mobile phone whereas distributors sell, or arrange for the issuance of funds on behalf of the issuer to clients. The electronic money issuer obviously issues electronic money, of which a definition has already been provided at the onset of this chapter but which is described by *FATF Guidance for a Risk-Based Approach* 20 as "a record of funds or value available to a client stored on a payment device such as chip on a prepaid card, mobile phones or on computer systems as a non-traditional account with a banking or non-banking entity." See *FATF Guidance for a Risk-Based Approach* 20; Aker and Mbiti 2010 *Journal of Economic Perspectives* 220-221; Alexandre and Eisenhart 2013 *WJLTA* 287 in this regard.
143 *FATF Guidance for a Risk-Based Approach* 20.
144 *FATF Guidance for a Risk-Based Approach* 20.
145 This description is not exhaustive and does not describe any particular scheme, although reference to South African mobile money providers will be made where applicable in order to serve as concrete examples.

In the operator-centric model, an MNO acts autonomously in providing a mobile money service.[146] This is often done by means of a mobile wallet which operates separately from the client's mobile account.[147] The biggest challenge which MNOs face in terms of the operator-centric model is the fact that they are not connected to existing payment networks.[148] This model has been launched in emerging markets by pioneers in the mobile financial services industry, but payments in terms of this model are usually limited to transfers and so-called "airtime top-ups."[149] MNOs usually offer mobile financial services under the operator-centric model with the intention to add value to their existing core service, namely communication.[150] Client funds are normally retained in a prepaid account by the MNO itself or by a subsidiary.[151] Regardless of the fact that the MNO is the entity which bears the greatest financial risk and active responsibility of offering the service under this model, it is standard practice in several jurisdictions for a partner bank to be the formal holder of the licence for the service.[152]

2.2.3.2 The bank-centric model

This model entails that a bank is the entity which offers mobile financial services to clients, with MNOs merely playing an assisting role and addressing quality concerns by means of experience.[153] Under this model, clients become account holders of the bank by whom the mobile financial service is offered.[154] This must be distinguished from mobile banking,[155] however, since under a bank-centric mobile money services model the bank either designs new products to provide for the needs of the previously unbanked, or alternatively, provides electronic money that is not linked to

146 Chaix and Torre *Different models for mobile payments* 2010 Working Paper University of Nice Sophia-Antipolis (hereafter referred to as Chaix and Torre *Different models for mobile payments*) 4, 6.
147 I.e., the mobile account containing prepaid credit or so-called "airtime", as discussed in chapter 1.
148 Chaix and Torre *Different models for mobile payments* 4, 10-14.
149 Chaix and Torre *Different models for mobile payments* 4, 10-14.
150 *FATF Guidance for a Risk-Based Approach* 16.
151 *FATF Guidance for a Risk-Based Approach* 16.
152 *FATF Guidance for a Risk-Based Approach* 16.
153 Chaix and Torre *Different models for mobile payments* 4, 10-14.
154 *FATF Guidance for a Risk-Based Approach* 15.
155 I.e. the provision of traditional banking services through a mobile phone, as explained previously under par 2.2.

a bank account.[156] An MNO's function under this model is the mere provision of the mobile technology which facilitates the transactional messages.[157] At no stage does the MNO manage or hold the client's funds.[158] The MNO thus does not require a banking licence since the bank is the financial service provider.[159]

2.2.3.3 The peer-to-peer model

The peer-to-peer model entails that a mobile financial service provider operates independently from financial institutions and MNOs in providing mobile money.[160] Since this model is not prevalent in South Africa, it will not be discussed further.

2.2.3.4 The collaboration model

Several mobile financial services have been deployed by financial institutions and MNOs who have joined forces to establish agent networks to extend to geographical regions where financial exclusion is rife.[161] This is known as the collaboration model since it involves collaboration among banks, MNOs, and a third party connecting the bank and MNO.[162] In such instances, MNO or other retail outlets offer services such as registering clients, taking deposits, and paying out cash to complete mobile money transactions.[163] This model seems like the most viable model since it allows each partner to retain focus on their own separate skills, which makes it much easier to implement than any of the previously-mentioned business models.[164] An example of this in South Africa is the recently re-launched M-PESA, a collaborative effort between Nedbank as bank and Vodacom as MNO.[165]

Although the above business models and the terminology that accompanies it may differ from jurisdiction to jurisdiction, it is assumed that in most mobile money

156 *FATF Guidance for a Risk-Based Approach* 15.
157 *FATF Guidance for a Risk-Based Approach* 15.
158 *FATF Guidance for a Risk-Based Approach* 15.
159 *FATF Guidance for a Risk-Based Approach* 15.
160 Chaix and Torre *Different models for mobile payments* 4, 17.
161 *FATF Guidance for a Risk-Based Approach* 17.
162 Chaix and Torre *Different models for mobile payments* 4, 17.
163 *FATF Guidance for a Risk-Based Approach* 17.
164 Chaix and Torre *Different models for mobile payments* 17.
165 Goldstuck 2014 http://mg.co.za.

business models, the agent acts on behalf of a financial institution.[166] The latter is accountable for the business relationship with the client. The agent is merely authorised by the financial institution to act on behalf of and under the control of the financial institution, thereby enabling the agent to deal with clients. The agent can also act on behalf of an MNO who is authorised to issue electronic money.[167]

The question which now remains is the following: are mobile money service providers subject to AML regulations?

2.3 Regulation of mobile money in South Africa, with specific focus on AML measures

All mobile financial service providers in South Africa are required to hold a banking licence,[168] and should, as such, adopt the standards of the South African Reserve Bank.[169] This legal requirement has had the practical effect that MNOs become, in part, a division of a financial institution. MTN, for example, partially became a division of Standard Bank for purposes of offering MTN MobileMoney.[170]

This would suggest that mobile money providers are indeed accountable institutions.[171] However, since South Africa has no legal provisions expressly concerned with mobile money,[172] refuge will be sought in the *FATF Recommendations*, which include any natural or legal person who conducts money

166 *FATF Guidance: AML and Financial Inclusion* 118; Interpretive Note 1 to Recommendation 17.
167 *FATF Guidance: AML and Financial Inclusion* 118.
168 The Reserve Bank is responsible for bank regulation and supervision in South Africa. The purpose is to achieve a sound, efficient banking system in the interest of the depositors of banks and the economy as a whole. This function is performed by issuing banking licences to banking institutions, and monitoring their activities in terms of either the *Banks Act* 94 of 1990, or the *Mutual Banks Act* 124 of 1993 and the Regulations relating thereto. See South African Reserve Bank 2011 https://www.resbank.co.za for more information in this regard.
169 These standards include: financial background and strength, governance, client protection, safety and soundness of the system, background information on shareholders and managers; and business model. See World Bank Working Paper no.146 35.
170 World Bank Working Paper no.146 35. According to *Standard Bank of South Africa Ltd v 3MFuture Africa (Pty) Ltd* 2013 JDR 2748 (SCA), MTN and Standard Bank are equal owners of MTN MobileMoney. Incidentally, this is the only South African case law to date which contains the phrase “mobile money.”
171 As per Schedule 1 of FICA, which will be discussed in extensive detail in Chapter 3.
172 It is submitted by Alexandre and Eisenhart that in terms of the “mobile” element, there is no need for specific “mobile money” regulation per se but instead for rules on electronic money that also apply to mobile money services. See Alexandre and Eisenhart 2013 *WJLTA* 297 In this regard.

or value transfer services (MVTS) as a business for or on behalf of a client in the definition of "financial institutions."[173] "MVTS", in turn, are defined as

> financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods.[174]

As such, mobile money providers fall within the scope of the FATF's definition of "financial institution" by virtue of the fact that they perform MVTS, and should therefore be subject to the AML measures imposed by the *FATF Recommendations* in general.[175] FATF Recommendation 14 furthermore makes specific provision for MVTS by stating that providers of MVTS and their agents should be licensed or registered,[176] and should show compliance with the relevant AML measures contained in the *FATF Recommendations*.[177] FATF Recommendation 26 emphasises the fact that all financial service providers must be subject to regulation and supervision and specifically states that businesses providing MVTS should be licensed or registered, and "subject to effective systems for monitoring and ensuring compliance with national requirements to combat [money laundering]."[178] Although Recommendation 26 does not make specific mention of mobile financial services,[179] it can be assumed that mobile financial service providers should be monitored, especially in the case where mobile money services are offered under a model other than the bank-centric business model, since poor oversight is a major risk factor in such instances,[180] as will be seen in Chapter 4.

Of specific interest for purposes of this dissertation, is the question of CDD. The "holding and management of an account" on behalf of a client is a circumstance

173 *FATF Methodology* Glossary 131-132.
174 *FATF Methodology* Glossary 134.
175 *FATF Guidance for a Risk-Based Approach* 3, 34, 123.
176 Agents need not be registered if the MVTS provider maintains a current list of its agents, which is accessible by competent authorities in the countries in which the MVTS provider and its agents operate. See FATF Recommendation 14 in this regard.
177 FATF Recommendation 14.
178 FATF Recommendation 26.
179 It is submitted by the author that since mobile money services have been analysed to be a form of MVTS, it is indeed included under FATF Recommendation 26.
180 World Bank Working Paper no.146 40.

which, according to FATF Recommendation 10, necessitates the performing of CDD measures.[181] As was seen, mobile money services entail the creation of an account and as such, mobile money service providers "typically establish business relationships" with clients as envisaged by Recommendation 10[182] – hence, CDD measures should be performed by mobile money service providers. The World Bank is also of the opinion that mobile money service providers should observe CDD measures similar to other financial institutions, including verification of clients' identity when establishing business relations.[183]

The fact that multiple service providers are involved in providing mobile money services[184] may, however, pose a problem for regulators in determining where "appropriate responsibility" for AML measures should be placed.[185] The decision regarding which entity be kept responsible for imposing AML measures will be guided by the business model of the mobile money service. Under the bank-centric model, the decision is easy: the bank should be subject to AML measures, seeing as it is a financial institution in any event.[186] Under the operator-centric model, the MNO is the financial institution for purposes of the *FATF Recommendations*,[187] and should accordingly be obligated to observe AML measures.

Where there is more than one entity involved in the provision of mobile money (such as in the case of the collaboration model) and there is uncertainty as to which entity constitutes the actual provider, the following factors could aid in determining the appropriate entity:[188]

- the entity which visibly provides the service;
- the entity which manages client relationships;
- the entity which holds client funds; and

181 FATF Recommendation 10. The reason for this is that the holding and managing of an account represents the establishment of a business relationship.
182 *FATF Guidance for a Risk-Based Approach* 94.
183 World Bank Working Paper no.146 36.
184 As discussed under par 2.2.3 above.
185 *FATF Guidance for a Risk-Based Approach* 20.
186 As per Schedule 1 of FICA. See also *FATF Guidance for a Risk-Based Approach* 125.
187 *FATF Guidance for a Risk-Based Approach* 126.
188 *FATF Guidance for a Risk-Based Approach* 118.

- the entity against which clients have a claim to their funds.[189]

Agents typically interact directly with clients, and are optimally suited to enforce AML preventative measures, such as CDD, on behalf of the provider. The FATF views agents as mere extensions of the financial services provider, and as a result, the CDD conducted by agents is considered to be conducted by the financial institution.[190]

2.4 Conclusion

The conclusion which can be drawn from the above is that mobile money is a powerful tool towards financial inclusion and the development and strengthening of the economy. While no specific provision is made for mobile money in the South African legislative context, it can be assumed with reasonable safety that mobile money service providers are accountable institutions for purposes of the FICA.[191] Furthermore, the FATF makes express provision, in several different measures, for the regulation of mobile money as far as AML measures are concerned.[192] With this in mind, the next chapter will focus on the regulation of money laundering in South Africa.

3 Money laundering and the anti-money laundering framework in South Africa

3.1 Introduction

This chapter will deal with financial integrity in the sense that money laundering, the financial integrity risk which forms the focus of this dissertation, and the measures

189 *FATF Guidance for a Risk-Based Approach* 118. These factors were also used by the FATF in determining that the MNO is the financial institution for purposes of the operator-centric model. See *FATF Guidance for a Risk-Based Approach* 126 in this regard.

190 *FATF Guidance for a Risk-Based Approach* 127; *FATF Guidance: AML and Financial Inclusion* 119. In this regard, "agents" or distributors are also acting as "agents" in the legal sense of the word, i.e. as an entity with agency to act on behalf of a person (natural or juristic), in this case the financial services provider.

191 World Bank Working Paper no.146 35. FICA and "accountable institutions" will be discussed extensively in Chapter 3.

192 Such as *FATF Guidance: AML and Financial Inclusion* and *FATF Guidance for a Risk-Based Approach.*

aimed at ensuring financial integrity by combating money laundering will be discussed. The concept of money laundering will be discussed as a point of departure after which applicable South African AML measures will be discussed within the broader framework of AML measures on both international and national level. The chapter will be concluded with specific focus on customer due diligence as AML measure and the impact it has on financial inclusion, with reference to mobile money.

3.2 What is money laundering?

Money laundering is, in simple terms, the "conversion of criminal incomes into assets that cannot be traced back to the underlying crime."[193] In other words, it entails the concealing of the nature, source, location or movement of the proceeds of crime so as to obscure the unlawfulness thereof in order for it to be used without arousing suspicion.[194] "Proceeds of crime" includes any asset, cash or otherwise, which is acquired by means of the commission of any criminal offence.[195] The objective of money laundering is thus to conceal the proceeds of crime in order for the offender to circumvent prosecution[196] whilst being able to utilise as much of the said proceeds of crime as possible.[197]

Money laundering is conventionally divided into three stages, namely placement, layering, and integration. Placement is the first stage in the process and comprises the displacement of funds obtained by means of illegal activities to a location or in a form that is less suspicious to law enforcement authorities and more expedient to the criminal offender. Once that has been done, the proceeds are channelled into financial institutions or the retail economy. The second phase is layering. This entails the severance of proceeds from the unlawful origin by making use of several intricate financial transactions (such as wire transfers or monetary instruments) to

193 Reuter and Truman *Chasing Dirty Money* 1.
194 Reuter and Truman *Chasing Dirty Money* 25.
195 Typical criminal activities in which money laundering is involved include theft, robbery, fraud, abduction, extortion, drug dealing, tax evasion, and the like. See Reuter and Truman *Chasing Dirty Money* 25 in this regard.
196 Prosecution in terms of the predicate crime, the definition of which will be discussed shortly.
197 Financial Intelligence Centre Guidance Note 3A, hereinafter only referred to as Guidance Note 3A.

obscure the audit trail and conceal the proceeds, usually by passing such proceeds through various institutions and jurisdictions in order to disguise the origin thereof. The final stage in the process is incorporation into an economy, during which unlawful proceeds are converted into seemingly lawful business earnings by means of ordinary financial or commercial operations.[198] Money laundering is criminalised in South Africa by the *Prevention of Organised Crime Act* 121 of 1998, the details of which will be discussed later in this chapter. Typical money laundering methods which are pertinent to this dissertation will now be briefly discussed.[199]

Structuring, also known as "smurfing", entails the splitting of a large financial transaction into several smaller transactions.[200] This is typically done by dividing cash deposits into amounts below a minimum limit above which banks are required to report financial transactions, known as threshold amounts.[201] Couriers or so-called "smurfs" then make these deposits into several different bank accounts, often at different banks.[202] This is done in order to avoid detection by authorities.[203]

Electronic funds transfers (EFTs) and its old-fashioned counterpart, wire transfers, are also prime tools for laundering money. It entails the transferring of control of funds form one institution[204] to another by sending a notification electronically (in the case of EFT) or by means of cable (in the case of wire transfers).[205] Such transfers are especially popular in the layering stage since funds can be transferred through various different institutions in different jurisdictions in order to obscure the trail to the origin of the funds.[206] Transfers can also be made from several different bank

198 Reuter and Truman *Chasing Dirty Money* 25. Evidence proposes that money laundering is generally not practiced as a separate activity by professionals, but is usually part of the underlying offense, which is known as the "predicate crime," or involves ad hoc assistance. Such assistance is criminalised in South Africa by s5 of the *Prevention of Organised Crime Act* 121 of 1998 (hereinafter referred to as POCA), as will be discussed later. See also Reuter and Truman *Chasing Dirty Money* 4-5 in this regard.

199 This discussion will be limited to two methods only: structuring or "smurfing" and the use of EFTs. The reason for this specific demarcation will become apparent in Chapter 4 where it will be explained how and why these two methods of money laundering are of specific pertinence when dealing with mobile money and the regulation thereof.

200 Reuter and Truman *Chasing Dirty Money* 30; World Bank Working Paper no.146 12.

201 Reuter and Truman *Chasing Dirty Money* 30, World Bank Working Paper no.146 12.

202 Reuter and Truman *Chasing Dirty Money* 30; World Bank Working Paper no.146 12.

203 Reuter and Truman *Chasing Dirty Money* 30; World Bank Working Paper no.146 12.

204 Usually a bank.

205 Reuter and Truman *Chasing Dirty Money* 30.

206 Reuter and Truman *Chasing Dirty Money* 30.

accounts, into which deposits have been made by "smurfing", to a single collecting account, which will usually be located abroad in an offshore financial centre.[207]

3.3 Anti-money laundering measures in South Africa

The South African legislator has made provision for comprehensive AML regulation in two acts: the *Prevention of Organised Crime Act* 121 of 1998 (POCA) and the *Financial Intelligence Centre Act* 38 of 2001 (FICA). POCA is the main legislative measure in terms of demarcating conduct that constitutes money laundering offences, but it does not provide for the measures which should be implemented in order to suppress and detect money laundering. These measures are provided for in FICA, which is the primary legislative instrument concerned with prescribing AML measures.[208] In other words, POCA outlines activities that constitute money laundering offences,[209] while FICA prescribes the measures to be implemented to suppress and detect money laundering.[210]

Anti-money laundering regimes have two pillars: prevention[211] and enforcement.[212] For purposes of the present dissertation focus will fall on the prevention pillar, with specific focus on customer due diligence[213] as preventative measure in terms of the *Financial Action Task Force Recommendations*[214] and the above-mentioned South African legislation.

---

207 Reuter and Truman *Chasing Dirty Money* 30.
208 Lawack 2013 *WJLTA* 331.
209 Lawack 2013 *WJLTA* 331.
210 See Lawack 2013 *WJLTA* 331. Focus in this regard will fall primarily on FICA.
211 This pillar comprises the following measures: customer due diligence, reporting, regulation and supervision, and sanctions. See Reuter and Truman *Chasing Dirty Money* 4.
212 This pillar includes measures such as a list of predicate crimes, investigation, prosecution and punishment, and confiscation. See Reuter and Truman *Chasing Dirty Money* 4.
213 As mentioned under par 1 above. According to the World Bank, customer due diligence entails the following: "Processes that include verifying a customer's identity and assessing the risks associated with that customer which enable the financial institution or another entity to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious." See World Bank Working Paper no. 146 73 in this regard.
214 Hereinafter referred to simply as the *FATF Recommendations*. For ease of reference and to avoid confusion, reference to the instrument as such will be *FATF Recommendations* (plural, italicised) and will be done in terms of page numbers of the document, whereas reference to a specific Recommendation will be done in terms of the number of the Recommendation in question, e.g., FATF Recommendation 1 (singular unless more than one Recommendation is mentioned, not italicised).

3.3.1 *The* Financial Action Task Force Recommendations

The Financial Action Task Force (FATF) is the intergovernmental global AML and counter-terrorist financing (CTF) standard-setting body.[215] It describes itself as follows:

> The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. *The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard*.[216]

The FATF thus develops guidance and best practices[217] to assist jurisdictions in the application of international AML standards, mainly by improving a country's existing AML regime.[218] The *FATF Recommendations* set out a comprehensive and consistent framework of measures which jurisdictions are advised to implement in order to combat money laundering.[219] It is therefore advisable that authorities as well as private sector institutions apply the *FATF Recommendations* as far as it may be relevant.[220]

As was seen in Chapter 1, South Africa is a member of FATF[221] and as such, the South African Financial Intelligence Centre (FIC) regularly publishes FATF policies. It should be noted that such policies are neither legislative instruments nor formal guidance issued under FICA.[222] However, FICA was amended in 2008 by the *Financial Intelligence Centre Amendment Act* 11 of 2008 which addressed, *inter alia*, some of the supervisory concerns raised in the FATF mutual evaluation of South

215 De Koker 2013 *WJLTA* 165.
216 *FATF Recommendations* preamble, own emphasis added. As mentioned in Chapter 1, the focus of this dissertation will fall on anti-money laundering only and not on counter-terrorist financing.
217 In the form of the *FATF Recommendations*.
218 FIC 2008 https://www.fic.gov.za.
219 *FATF Recommendations* 7.
220 *FATF Recommendations* 7; FIC 2008 https://www.fic.gov.za.
221 World Bank Working Paper no.146 4; FIC Annual report 2012-2013; FIC 2008 https://www.fic.gov.za.
222 *Financial Intelligence Centre Act* 38 of 2001. See FIC 2008 https://www.fic.gov.za in this regard.

Africa in 2008.[223] This is a clear indicator that the *FATF Recommendations* do carry weight and have a large influence on South Africa's AML policies. Guidance Note 3A, issued by the FIC in 2013, reiterates this by stating that the *FATF Recommendations* form the contextual basis for the implementation of FICA and that international standards such as the *FATF Recommendations* provide the minimum requirements with which countries must comply.[224]

The relevant provisions of POCA and FICA will accordingly be discussed with reference to the *FATF Recommendations* and, where applicable, in terms of its compliance with the *FATF Recommendations* as described in the *FATF Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems*.[225]

3.3.2 Prevention of Organised Crime Act *121 of 1998*

According to FATF Recommendation 3, money laundering should be criminalised on the basis of the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (1988) (Vienna Convention) and the *United Nations*

223 Lawack 2013 *WJLTA* 331. The FATF Mutual Evaluation was based on the laws, regulations and other materials supplied by South Africa, and information obtained by the evaluation team during its onsite visit to South Africa from 4-15 August 2008, and subsequently. During the evaluation, the team met with officials and representatives of all relevant South African government agencies and the private sector. For more information, see the *FATF GAFI Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism, South Africa* of 29 February 2009, hereafter referred to as *FATF GAFI MER*.

224 Guidance Note 3A paragraph 24.

225 *The FATF Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems* (hereafter referred to as the *FATF Methodology*) prescribes how countries should go about in assessing technical compliance with the *FATF Recommendations* and the effectiveness of AML/CFT systems. The key points in this regard is that all requirements for financial institutions should be introduced either in law (any legislation issued or approved through a parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for noncompliance, as well as judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country) or enforceable means (regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority) and that sanctions for non-compliance should be effective, proportionate and dissuasive. It should also be clear that these sanctions will be applied in the event of non-compliance by a financial institution. For a complete list of factors to be taken into account when assessing whether a document or mechanism has requirements that amount to enforceable means, see the *FATF Methodology* 123 and the note on the Legal Basis of Requirements on Financial Institutions and DNFBPS contained in the *FATF Recommendations.*

Convention against Transnational Organised Crime (2000) (Palermo Convention).[226] As a point of departure, it should be noted that South Africa has ratified both the Vienna Convention and the Palermo Convention.[227]

Furthermore, according to FATF Recommendation 3, money laundering should be applied to all serious offences, with a vision to include the widest range of predicate offences.[228] As previously mentioned, POCA is the primary piece of South African legislation in terms of outlining activities that constitute offences relating to money laundering.[229] This is also confirmed in FICA, which defines 'money laundering' or 'money laundering activity' as

> an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of section 64 of this Act *or section 4, 5 or 6 of the* Prevention of Organised Crime Act *121 of 1998.*[230]

POCA criminalises money laundering in conformity with the requirements of the Vienna Convention and the Palermo Convention,[231] and as such it is compliant with the first part of FATF Recommendation number 3.

POCA makes provision for the conversion or transfer, concealment or disguise, possession, and acquisition of property[232] and criminalises the act of money laundering as follows:[233]

> Any person who knows or ought reasonably to have known that property is or forms part of the proceeds of *unlawful activities* and—
>
> *(a)* enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether such agreement, arrangement or transaction is legally enforceable or not; or
>
> (*b*) performs any other act in connection with such property, whether it is performed independently or in concert with any other person,
>
> which has or is likely to have the effect—

226 FATF Recommendation 3.
227 United Nations 2014 https://treaties.un.org, *FATF GAFI MER* par 34.
228 FATF Recommendation 3.
229 Lawack 2013 *WJLTA* 331.
230 S 1 *Financial Intelligence Centre Act* 38 of 2001, own emphasis added.
231 Lawack 2013 *WJLTA* 330.
232 Lawack 2013 *WJLTA* 330
233 POCA s4, own emphasis added.

(i) of *concealing or disguising the nature, source, location, disposition or movement of the said property* or the ownership thereof or any interest which anyone may have in respect thereof;

(ii) of *enabling or assisting any person who has committed or commits an offence*, whether in the Republic or elsewhere—

(*aa*) to avoid prosecution; or

(*bb*) to *remove or diminish any property acquired* directly, or indirectly, *as a result of the commission of an offence*,

shall be guilty of an offence.

Sections 5 and 6 of POCA furthermore provide that assisting another to benefit from proceeds of unlawful activities,[234] as well as the acquisition, possession or use of proceeds of unlawful activities,[235] constitute offences.

As can be seen, proceeds from "unlawful activities"[236] are included in all these sections, clearly meeting the requirement set out in the second part of FATF Recommendation 3, namely that the crime of money laundering should be applied to all serious offences, with a view to including the widest range of predicate offences.[237]

The fact that money laundering is a serious offence under South African law can be inferred from the maximum sentences one can incur for being convicted thereof: either a fine of up to R100 million, or imprisonment for up to 30 years.[238]

3.3.3 Financial Intelligence Centre Act *38 of 2001*[239]

As mentioned previously,[240] South African legislation not only proscribes conduct that constitutes money laundering, but also makes provision for various control

234 POCA s5.
235 POCA s6.
236 According to s1 of POCA, unlawful activity means "any conduct which constitutes a crime or which contravenes any law whether such conduct occurred before or after the commencement of this Act and whether such conduct occurred in the Republic or elsewhere."
237 FATF Recommendation 3.
238 POCA s8(1).
239 As will be seen, FICA should be read together with its regulations as well as the exemptions in terms of those regulations. The regulations, exemptions and other measures which can be implemented under FICA (such as Guidance Notes) will accordingly all be discussed under the current heading in an integrated manner.
240 Under paragraph 2.3.

measures which have the objective of enabling the suppression, detection and investigation of money laundering.[241] These control measures can be found in FICA, which is the principal source of legislation concerned with outlining AML measures.[242] These measures are based on three basic principles[243] of money laundering detection and investigation, namely that intermediaries in the financial system[244] must know whom they are doing business with, record must be kept of transactions through the financial system, and transactions which could possibly involve money laundering must be reported to investigating authorities.[245]

The control measures enacted by FICA include stipulations to the effect that institutions[246] need to establish and verify the identities of their clients,[247] keep certain records, report certain information and implement measures that will assist in compliance with FICA.[248] Section 77 of FICA also confers power upon the Minister of Finance[249] to make regulations in terms of the Act,[250] which will have legislative authority equal to that of FICA itself.[251] As a result, FICA is to be read together with the *Money Laundering and Terrorist Financing Control Regulations* (MLTFC Regulations),[252] as well as several exemptions in terms of the *Financial Intelligence Centre Act (Exemptions)*.[253] The application of these measures has led to the

241 Lawack 2013 *WJLTA* 331.
242 As mentioned previously. See Lawack 2013 *WJLTA* 331.
243 For purposes of the present discussion, only the first of these three principles will be of relevance.
244 The financial system can be described as the system that allows the transfer of money between investors and borrowers. It comprises a set of closely interconnected financial institutions, markets, instruments, services, practices, and transactions. See O'Sullivan and Sheffrin *Economics: Principles in Action* 551; Gurusamy *Financial Services and Systems* 3 in this regard.
245 FIC 2008 https://www.fic.gov.za.
246 Most of the obligations imposed by FICA are applicable to "accountable institutions". These are institutions that fall within any one of the categories of institutions listed in Schedule 1 to FICA. For purposes of the present chapter, focus will fall purely on specific control measures. These control measures will be placed in the context of mobile money in Chapter 4.
247 As mentioned in Chapter 1, this is the specific AML measure which will be scrutinised in this dissertation. Whilst the FATF prefers to use the term "customer", FICA makes use of the term "client". The term "client" will forthwith be used for the sake of uniformity and in accordance with national legislation, unless instruments such as the *FATF Recommendations* are directly quoted and the word "customer" appears in the excerpt used, or if reference to CDD (customer due diligence) is made.
248 Guidance Note 3A.
249 S 1 of FICA.
250 *Financial Intelligence Centre Act* 38 of 2001.
251 According to s1 of FICA, any reference in the Act to the Act will include any regulations under the Act in terms of s77.
252 Reg R1595 in GG 24176 of 20 December 2002.
253 The Exemptions are to be found in the Schedule to Reg R1595 in GG 24176 of 20 December 2002 and in Reg R1353 and R1354 in GG 27011 of 19 November 2004.

implementation of comprehensive AML policies and preventative measures in South Africa.[254]

Besides enacting AML regulations, FICA also established the FIC as the institution tasked with the collection, analysis and disclosure of data to aid the detection, prevention and deterrence of money laundering in South Africa.[255] Section 4(c) of FICA authorises the FIC to issue guidance regarding various matters concerned with compliance in terms of the obligations imposed by FICA.[256] The MLTFC Regulations[257] also make provision for guidance notes under Regulation 28(1):[258]

> The Centre may issue guidance notes concerning–
> (a) the verification of identities;
> (b) reporting of suspicious and unusual transactions; and
> (c) any other obligations imposed on accountable institutions under the Act.
> (2) Guidance notes referred to in subregulation (1) may differ for different accountable institutions or persons, or categories of accountable institutions or persons and different categories of transactions.

The establishment of the FIC in terms of section 2 of FICA and the powers it has in terms of Regulation 28(1)[259] illustrates compliance with FATF Recommendation 2, which states that "countries should have national AML/CFT policies […] which should be regularly reviewed, and *should designate an authority* […] *that is responsible for such policies*."[260]

It should be noted the only form of guidance officially recognised in terms of FICA and the Regulations, is that guidance which is imparted by the FIC.[261] As such, guidance provided by the FIC is authoritative in nature. An accountable institution *must apply guidance issued by the* FIC, or demonstrate an equivalent level of compliance with the relevant obligations under FICA.[262] Enforcement action may stem from non-compliance with FICA where an accountable institution does not

254 Lawack 2013 *WJLTA* 331.
255 See ss 2, 3 and 4 of FICA.
256 S 4 of FICA; Guidance Note 3A.
257 Reg R1595 in GG 24176 of 20 December 2002.
258 Reg R1595 in GG 24176 of 20 December 2002.
259 Reg R1595 in GG 24176 of 20 December 2002.
260 FATF Recommendation 2, own emphasis added.
261 Reg R1595 in GG 24176 of 20 December 2002.
262 Guidance Note 3A paragraph 2, own emphasis added.

follow guidance issued by the FIC and cannot demonstrate compliance with the legal obligation to which the guidance relates.[263]

Section 21 of FICA[264] specifically deals with control measures for money laundering, including the establishment and verification of clients' identities. Since this forms the focus of this dissertation, it will accordingly be discussed in greater detail.

3.3.4 The establishment and verification of identities of clients as an AML measure

According to FATF Recommendation 10, it should be illegal for financial institutions to keep anonymous accounts or accounts in obviously fictitious names.[265] Furthermore, financial institutions should be obliged to implement customer due diligence (CDD) measures when establishing business relations[266] – a principle which should be set out in law.[267]

The CDD measures which should be implemented include identification of the client and verification of such identity. Such verification should be done by making use of "reliable, independent source documents, data or information."[268] The purpose of CDD measures is to enable financial institutions to effectively identify, verify and monitor their clients and the transactions they enter into, in relation to the money laundering risks that they pose.[269]

Compliance with FATF Recommendation 10 can be found in section 21(1) of FICA, which states that

---

263 Guidance Note 3A paragraph 2.
264 Ss 21-45 of FICA.
265 FATF Recommendation 10.
266 FATF Recommendation 10(i), *FATF Guidance for a Risk-Based Approach* 93(a). This is not the only instance in which CDD measures should be taken. This is, however, the instance on which the focus of this dissertation will fall. See Recommendation 10(ii)-(iv) for other instances when CDD measures should be taken.
267 FATF Recommendation 10.
268 FATF Recommendation 10(a); *FATF Guidance: AML and Financial Inclusion* 65(a). This is not the only CDD measure which should be taken. This is, however, the CDD measure on which the focus of this dissertation will fall. See Recommendation 10(b)-(d) for other CDD measures.
269 *FATF Guidance for a Risk-Based Approach* 92; *FATF Guidance: AML and Financial Inclusion* 61.

> An accountable institution may not establish a business relationship or conclude a single transaction with a client unless the accountable institution has taken the prescribed steps-
> (a) to establish and verify the identity of the client;
> (b) if the client is acting on behalf of another person, to establish and verify-
> (i) the identity of that other person; and
> (ii) the client's authority to establish the business relationship or to conclude the single transaction on behalf of that other person; and
> (c) if another person is acting on behalf of the client, to establish and verify-
> (i) the identity of that other person; and
> (ii) that other person's authority to act on behalf of the client.

Guidance Note 3A reiterates this by stating that client identification and verification must be done "at the outset of the business relationship or single transaction."[270]

Regulation 3(1)[271] prescribes what such identification and verification of clients[272] should entail:

> An accountable institution must obtain from, or in respect of, a natural person who is a citizen of, or resident in, the Republic, that person's–
> (a) full names;
> (b) date of birth;
> (c) identity number;
> (d) income tax registration number, if such a number has been issued to that person; and
> (e) residential address.

If these regulations are applied to mobile money providers as accountable institutions and followed stringently, the opening of mobile money accounts will in certain instances be made impossible or difficult since the verification of this information can prove troublesome, especially with regard to residential address.[273] The verification of clients' addresses has indeed presented certain complications in

270 Guidance Note 3A par 10.

271 Reg R1595 in GG 24176 of 20 December 2002.

272 Reg 3(2) also provides for instances where a person wishing to establish a business relationship or conclude a single transaction with an accountable institution as contemplated in Reg 3(1) does not have the legal capacity to do so without another person's assistance. In such an instance, the person assisting the potential client must furnish the following particulars to the accountable institution: (a) his or her full names; (b) his or her date of birth; (c) his or her identity number; (d) his or her residential address; and (e) his or her contact particulars. This is in line with Interpretive Note 4 to FATF Recommendation 10, which states that "when performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person."

273 Alexandre and Eisenhart 2013 *WJLTA* 299. See also *FATF Guidance: AML and Financial Inclusion* 79.

South Africa, particularly in the case of low-income individuals.[274] Migrant labourers who live in informal settlements, for example, encounter substantial obstacles in accessing formal remittance services since they cannot readily verify their residential addresses in most instances.[275] Research done by the World Bank has also pointed out that a lack of verifying documentation is often one of the main reasons why people don't have accounts.[276] It is also the findings of the FATF that the client identity verification[277] stage is the most difficult and onerous part of the CDD process.[278] It is thus clear that arduous verification requirements can be counterproductive to financial inclusion.[279]

It is therefore a positive sign that the South African legislator was mindful of the fact that prospective clients who live in informal settlements and rural areas could encounter difficulties in verifying their residential addresses in conformity with the regulatory provisions.[280] An exception to the obligation to provide a residential address, amongst other things, was consequently created by means of the well-known Exemption 17.[281] Exemption 17 exempts certain financial institutions[282] from having to comply with selected provisions of section 21 of FICA and Regulations 3 and 4[283] when dealing with certain types of accounts,[284] to the effect that a customer's residential address does not need to be obtained or verified. Mobile money transfer businesses, however, do not fall under the scope of this exemption.[285] In other words, Exemption 17 is not applicable to financial institutions that provide mobile money transfers (i.e. remittance services) as their only

274 Lawack 2013 *WJLTA* 332.
275 Lawack 2013 *WJLTA* 339; *FATF Guidance: AML and Financial Inclusion* 23.
276 *FATF Guidance: AML and Financial Inclusion* 79.
277 Which, in South Africa, entails the verification of residential address in order to ensure that identity fraud has not been committed. See Lawack 2013 *WJLTA* 332 in this regard.
278 *FATF Guidance: AML and Financial Inclusion* 78.
279 *FATF Guidance: AML and Financial Inclusion* 78.
280 Lawack 2013 *WJLTA* 332.
281 Reg R1353 in GG 27011 of 19 November 2004.
282 These institutions are the following: a person who carries on the 'business of a bank' as defined in the *Banks Act* 94 of 1990, a mutual bank as defined in the *Mutual Banks Act* 124 of 1993, the Postbank referred to in section 51 of the *Postal Services Act* 124 of 1998, and the Ithala Development Finance Corporation Limited.
283 Reg R1595 in GG 24176 of 20 December 2002.
284 Lawack 2013 *WJLTA* 337. See Exemption 17(3)(a)-(d), contained in Reg R1353 in GG 27011 of 19 November 2004, for the types of accounts which are included under this exemption.
285 Lawack 2013 *WJLTA* 339.

business.[286] With that being said, attention is focused on the requirement of supplying and verifying a residential address once again.

According to Regulation 4(3), an accountable institution must verify the residential address referred to in Regulation 3(1)(e) or 3(2)(f) by comparing these details with "information which can reasonably be expected to achieve such verification and is obtained by reasonably practical means,"[287] taking into consideration any applicable guidance notes concerning the verification of identities.[288]

Guidance Note 3A, which was published by the FIC on 28 March 2013 and which is applicable to all accountable institutions under Schedule 1 of FICA[289] addresses, *inter alia,* the potential difficulty of complying with this regulation by dealing with several aspects which will consequently be discussed.

According to Guidance Note 3A, the most secure form of confirmation of a residential address would be for a staff member and/or agent of the accountable institution to visit the residential address provided by the natural person applying for an account, in order to confirm that the person indeed resides at the specified residential address.[290] Logic dictates that this is highly impractical and as such, it will be an adequate measure of verification in most cases to review an original document[291] that offers a reasonable confirmation of the information in question and to obtain a copy of such document.[292]

According to the FIC, accountable institutions had been applying a restrictive approach regarding which types of documentation will be accepted to verify the residential address of a client,[293] which had resulted in the frustration of the verification process (which ultimately led to the exacerbation of financial

286 Lawack 2013 *WJLTA* 338-339. The Banks Act Guidance Note 6/2008 issued by the Registrar of Banks has, however, brought mobile banking products within the framework of Exemption 17.
287 Reg 4(3) of R1595 in GG 24176 of 20 December 2002.
288 Reg 4(3) of R1595 in GG 24176 of 20 December 2002.
289 Preface to Guidance Note 3A.
290 Guidance Note 3A par 11.
291 Supplied by the person applying for the account.
292 Guidance Note 3A par 11.
293 Guidance Note 3A par 11.

exclusion).[294] The FIC accordingly took steps to mitigate this situation by providing guidance in paragraph 11 of Guidance Note 3A regarding which documents qualify as acceptable verification documentation.[295]

This paragraph includes a list of examples of documentation that may be used to verify the residential address of a natural person. This list is not exhaustive, and other documents may be used if circumstances deem it necessary.[296]

Documents which, according to paragraph 11 of Guidance Note 3A, may offer proof of the residential address of a person[297] include, *inter alia*,[298] the following:

- a utility bill;[299]
- a recent lease or rental agreement;
- municipal rates and taxes;
- telephone or cellular account;
- valid television licence;
- recent motor vehicle licence documentation; or
- a statement of account issued by a retail store that reflects the residential address of the person.[300]

Provision is furthermore made for instances where a utility bill does not identify the physical street address of the property owner because it is sent to a postal address. In this case, the utility bill will still be an acceptable form of verification provided the client's name and their erf number or stand number and township[301] details are contained therein. The client's physical address, erf number and township should then be documented by the institution, after which the institution should cross-

294 *FATF Guidance: AML and Financial Inclusion* 39.
295 Lawack 2013 *WJLTA* 338. This action taken by the FIC was in accordance with the *FATF Guidance: AML and Financial Inclusion*, which states in par 39 that regulators should provide further guidance when institutions overestimate money laundering risks or adopt overly-conservative control measures.
296 Decisions as to how residential addresses are to be verified should be based on an accountable institution's risk framework, according to Guidance Note 3A paragraph 11.
297 I.e. documents containing both the residential address and names of the person.
298 Only documents that would be applicable to an unbanked person will be included for purposes of this dissertation.
299 Including that of a telephone or cellular account, Eskom or a local authority.
300 Guidance Note 3A par 11.
301 The word "township" should be interpreted in the legal sense of the word in this instance, as opposed to the meaning it would have in terms of South African vernacular.

reference the township to the suburb in which the client resides. Details can also be verified by reference to the Deeds Office if there remains any doubt about the client's residential particulars.

If none of the above can be provided by the client, other ways to verify a client's address may be explored. The example expressly provided for by Guidance Note 3A is that of an affidavit from the client's employer or a person co-habiting with the client, stating the name, residential address, and identity number of both the client and the deponent of the affidavit together with particulars about the relationship between the client and the deponent of the affidavit and confirmation of the client's residential address.[302]

It should be noted that while Guidance Note 3A does offer considerable leniency to accountable institutions regarding the documents which may be used for residential address verification purposes, the FIC is still of the opinion that the address slips issued by the Department of Home Affairs which is found in the back cover of South African identity documents, do not constitute information that can "reasonably be expected to achieve verification of a person's current address."[303] The reason for this is that the FIC does not regard these address slips as independent source documents.[304] Furthermore, the information contained in an address slip may be outdated.[305]

The reasonable inference that can thus be drawn from the above is that the FIC's aim with paragraph 11 of Guidance Note 3A is to urge accountable institutions to accept as many secure forms of verification as possible (i.e. to promote financial inclusion) as long as it does not come at the expense of financial integrity. It would thus seem as if accountable institutions are encouraged to follow a risk-based

302 Guidance Note 3A par 11.

303 As per the requirement in Reg 4(3) of R1595 in GG 24176 of 20 December 2002. FATF Recommendation 10(a) requires financial institutions to verify the client's identity using reliable, independent source documents, data or information. This is also reiterated in *FATF Guidance: AML and Financial Inclusion* 77, which goes on to say that "when determining the degree of reliability and independence of such documentation, countries should take into account the potential risks of fraud and counterfeiting in a particular country. It is the responsibility of each country to determine what can constitute "reliable, independent source documents, data or information" under its AML regime."

304 Guidance Note 3A par 7.

305 Guidance Note 3A par 7.

approach[306] when establishing and verifying customer identity rather than a rigid, uniform approach.[307]

It is, however, clear that the obligation on financial institutions to obtain and verify residential addresses as part of CDD appears to have been the chosen safeguard against identity fraud[308] and that the South African legislator is not willing to do away with this safeguard lightly. The need for providing a residential address for purposes of aiding the identification of a client has, however, been questioned by esteemed academics such as de Koker.[309] Lawack submits that if an accountable institution can obtain a client's name, date of birth, and unique national identity number, it is unnecessary to obtain a residential address as well since it will not add significant value to the identification process, but will undoubtedly cause an unnecessary setback for clients who do not have formal addresses.[310] This is quite apparent from the practical difficulties that have been experienced up to date in South Africa in verifying the residential addresses of especially low-income individuals.[311]

3.4 Conclusion

From the above it is clear that South Africa has a reasonable extensive AML framework which, although it is on par with international standards such as the *FATF Recommendations*, makes provision for the unique South African socio-economic setup – to a certain extent. It would seem that an over-cautious approach to CDD could be what is hampering the widespread development and acceptance of mobile money as a tool for financial inclusion. The application of a risk-based approach and the benefits it can hold for the full development of the potential that mobile money holds, will be explored in the next chapter.

306 The notion of a risk-based approach will be discussed extensively in Chapter 4 of this dissertation.
307 Lawack 2013 *WJLTA* 338.
308 Lawack 2013 *WJLTA* 336.
309 Lawack 2013 *WJLTA* 336; De Koker 2004 *Journal of South African Law* 742.
310 Lawack 2013 *WJLTA* 336; De Koker 2004 *Journal of South African Law* 742.
311 Lawack 2013 *WJLTA* 336; De Koker 2004 *Journal of South African Law* 742.

4 Mobile money, money laundering and the risk-based approach

4.1 Introduction

The basic principle of criminology is the following: crime follows opportunity.[312] The patterns of crime involving technology have the capability to rapidly adapt as new advances in technology occur.[313] The expansion of mobile internet systems holds the potential of novel opportunities for criminals in general, but also specifically in the domain of mobile financial services.[314] This chapter will explore perceived versus actual financial integrity risks in terms of mobile financial services,[315] the way in which CDD serves to mitigate these risks, the negative impact that over-regulation can have on financial inclusion, as well as a possible solution to the problem of over-regulation. Finally, the South African legal position regarding CDD and over-regulation will be discussed briefly.

4.2 Financial integrity risks linked to mobile money: perceptions versus reality

Many regulators worldwide fear that mobile financial services hold serious financial integrity risks,[316] since mobile financial services in general are often perceived as presenting unique risks compared to their traditional counterparts. The six major financial integrity concerns in this regard, as identified by the World Bank, are unknown identity, false identification, smurfing, increased transaction speed, so-called phone "pooling"[317] and phone "delegation",[318] and lack of regulation of providers of mobile financial services.[319] The rationale behind each of these fears will now be briefly discussed.

---

312 Grabosky, Smith and Dempsey *Electronic Theft: Unlawful Acquisition in Cyberspace* 1.
313 Avina 2011 *Journal of Financial Crime* 286.
314 Avina 2011 *Journal of Financial Crime* 286.
315 World Bank Working Paper no.146 xiii. These financial integrity risks will be discussed mainly with reference to the World Bank Working Paper no.146.
316 World Bank Working Paper no.146 xiii, 2, 11.
317 I.e. when several individuals share a few mobile phones. This practice is prevalent in poorer communities. See Bank Working Paper no.146 12 in this regard.
318 As opposed to pooling, delegation is observed in more wealthy communities. This is the custom in terms of which an agent or "delegate" is appointed to operate a mobile phone on behalf of the owner thereof. See Bank Working Paper no.146 12 in this regard.
319 Alexandre and Eisenhart 2013 *WJLTA* 288; Bank Working Paper no.146 12.

4.2.1 Perceived financial integrity risks of mobile financial services

4.2.1.1 Unknown identity

For many regulators, the greatest financial integrity concern in terms of mobile financial services is a lack of information about the client's identity.[320] This is beneficial to money launderers since it could facilitate the conclusion of transactions without any name attached to it, thereby providing a guise for money launderers under which to operate.[321]

4.2.1.2 False identification

The use of counterfeit documentation by money launderers in order to avoid detection is considered a grave risk in terms of mobile financial services.[322] The conditions which must be complied with in order to obtain a mobile phone often differ greatly from the conditions which must be complied with before a bank account can be opened.[323] Money launderers make use of pseudonyms or third-party names and personal particulars.[324] Alternatively, a mobile phone which is already linked to a mobile money account may be supplied to money launderers by a third party who is supportive of their criminal activities.[325] Mobile phones may also be stolen for purposes of laundering money by means of it under a false identity.[326]

4.2.1.3 Smurfing

Mobile money seems to be very susceptible to smurfing because it enables a large amount of money that is being transferred to be hidden as smaller, more inconspicuous amounts.[327] Mobile financial services in general also seem to provide

320 World Bank Working Paper no.146 11.
321 World Bank Working Paper no.146 12.
322 World Bank Working Paper no.146 12.
323 World Bank Working Paper no.146 12.
324 Kellerman "Mobile Risk Management: E-finance in the Wireless Environment" 7; World Bank Working Paper no.146 12.
325 World Bank Working Paper no.146 12.
326 World Bank Working Paper no.146 12.
327 World Bank Working Paper no.146 12.

a very convenient tool for "layering" of funds by concealing the illegal origins thereof by means of intricate movements, especially since mobile financial services are considerably less expensive than traditional financial services.[328] Small transactions initiated from several different mobile money accounts might go unnoticed. Several different senders may also channel funds into a primary mobile money account,[329] very similar to the manner in which EFTs or wire transfers are utilised in money laundering operations.[330]

4.2.1.4 Transaction Speed

The fact that mobile financial services enable the rapid performance of transactions is perceived to be very beneficial to money launderers.[331] Mobile money offers a safe, convenient and quick manner of transferring money, not only to legitimate clients, but also to criminals.[332]

4.2.1.5 Pooling and delegation

Pooling and delegation share the same perceived financial integrity risk, namely that a money launderer's identity can be easily obscured since the mobile phone which was used to commit a money laundering offense is not necessarily registered in the perpetrator's name.[333]

4.2.1.6 Lack of regulation

Concern exists over the fact that providers of mobile financial services are not subject to the same regulatory measures as other financial institutions.[334] AML controls, which are standard practice among traditional financial institutions such as

328 Solin and Zerzan "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks" (hereafter referred to as Solin and Zerzan "Mobile Money: Methodology for Assessing Money Laundering Risks") 14; World Bank Working Paper no.146 12.
329 World Bank Working Paper no.146 12.
330 As was discussed in Chapter 3.
331 Alexandre and Eisenhart 2013 *WJLTA* 287; World Bank Working Paper no.146 2
332 As was mentioned in Chapter 1. See World Bank Working Paper no.146 2, 12 in this regard.
333 World Bank Working Paper no.146 13.
334 Alexandre and Eisenhart 2013 *WJLTA* 287; World Bank Working Paper no.146 2.

banks, are not necessarily observed by mobile financial services providers.[335] This is especially true in terms of the operator-centric mobile money business model,[336] where the provider of the service is an MNO and not a bank.[337] Since the primary business of MNOs is communication and not financial services, it may often be the case that MNOs are not subject to an AML regulatory regime.[338] Even if an MNO itself is compliant with AML measures, it could be that its agents are not.[339] Dirty money can easily slip through these cracks and mobile financial services can be abused without enforcement authorities being aware thereof.[340]

These fears are not unfounded, especially not in the context of mobile money. While it is true that mobile money creates significant opportunities for increased financial inclusion, it also poses significant money laundering risks since it is the mobile financial services model which deviates the most from traditional financial services models.[341] It makes provision for a completely unique manner of performing financial transactions and is the fastest developing mobile financial service. As such, it presents not only the greatest potential for development, but also for manipulation and exploitation.[342] There are four proven money laundering risk factors which are observed in all mobile financial services, namely anonymity, elusiveness, rapidity, and poor oversight,[343] each of which will accordingly be briefly discussed.

4.2.2 Proven financial integrity risks of mobile financial services

4.2.2.1 Anonymity

Anonymity is the risk of being unfamiliar with a client's true identity, which could result in unauthorised use of an existing mobile financial services account by means of, for example, theft of a mobile phone.[344] Mobile financial services further pose the

335 World Bank Working Paper no.146 40.
336 As discussed in Chapter 2 under par 2.2.3.1.
337 World Bank Working Paper no.146 40.
338 Alexandre and Eisenhart 2013 *WJLTA* 287; World Bank Working Paper no.146 40.
339 World Bank Working Paper no.146 13.
340 World Bank Working Paper no.146 13.
341 In comparison to mobile banking, for example. See World Bank Working Paper no.146 28.
342 As mentioned in Chapter 2. See World Bank Working Paper no.146 28.
343 World Bank Working Paper no.146 xiii, 13.
344 World Bank Working Paper no.146 xiii; 71.

threat of anonymity since it facilitates the opening of multiple accounts in order to obscure the true value of deposits.[345] Not being familiar with clients' identities also allows dirty money to be easily withdrawn.[346] Since suspicious names cannot be flagged by the system, mobile financial services is a safe way for known criminals to conduct their money laundering operations.[347] This risk can only be mitigated through the implementation of enhanced CDD measures.[348]

4.2.2.2 Elusiveness

Elusiveness is the ease with which the source, destination, and sum of a mobile transaction can be camouflaged[349] and is a risk factor which is particularly prevalent in mobile money.[350] Using multiple mobile money accounts makes it possible to carry out untraceable transactions[351] and money launderers can therefore indeed utilise mobile money to conceal the original source of illicitly obtained funds.[352] Mobile money also allows for a large transfer of funds to be divided into several smaller sums, causing the transfer to arouse less suspicion and thereby hampering the ability of mobile money service providers and authorities to detect the money laundering effort[353] – exactly as regulators fear. It is submitted that mobile money therefore facilitates smurfing by its very nature and as such has the potential to be a prime tool in money laundering operations. It is therefore understandable that concerns exist surrounding the detrimental effect that mobile money can have on financial integrity.[354] The risk of elusiveness can be mitigated by means of transaction limits, enhanced client CDD, and reporting.[355]

4.2.2.3 Rapidity

345 Solin and Zerzan "Mobile Money: Methodology for Assessing Money Laundering Risks" 14.
346 Solin and Zerzan "Mobile Money: Methodology for Assessing Money Laundering Risks" 14.
347 Solin and Zerzan "Mobile Money: Methodology for Assessing Money Laundering Risks" 14.
348 World Bank Working Paper no.146 xiv, 71.
349 World Bank Working Paper no.146 xiv.
350 World Bank Working Paper no.146 28.
351 Solin and Zerzan "Mobile Money: Methodology for Assessing Money Laundering Risks"14; World Bank Working Paper no.146 28, 71.
352 World Bank Working Paper no.146 28.
353 World Bank Working Paper no.146 28.
354 Grabosky, Smith and Dempsey *Electronic Theft: Unlawful Acquisition in Cyberspace* 1.
355 World Bank Working Paper no.146 xiv, 72.

Rapidity is the speed with which illegal transactions can be conducted.[356] Mobile financial services poses a money laundering risk in terms of rapidity since it allows illicitly obtained funds to be deposited into one account and transferred to another within a very short space of time.[357] Since transactions conducted by means of mobile financial services take place in real time, it is difficult for authorities to prevent the transaction from being completed if money laundering is suspected.[358] Mobile financial services make it possible for illegal earnings to be moved through the financial system rapidly, after which it can be withdrawn from another account.[359] The risk which is posed by rapidity can be mitigated by flagging certain types of transactions and managing risks of third-party providers.[360]

4.2.2.4 Poor oversight

Poor oversight does not constitute an inherent risk on its own but rather contributes to and exacerbates the three aforementioned risks, which are inherent to mobile financial services.[361] Lack of proper oversight may cause mobile financial services to pose a systemic risk.[362] Poor oversight can be mitigated by clear guidelines regarding mobile financial services, better licensing, regulation of providers, and successful risk supervision within bank and non-bank mobile financial service providers.[363]

It is thus clear that all of the perceived risks, are in fact, real, since each perceived risk can be linked to one of the aforementioned proven risk factors.[364] It is also, however, clear that there are mitigating measures which can be taken in each instance to decrease the risk. It stands to reason that regulators will aim to address their concerns by implementing available AML measures as strictly as possible.

356 World Bank Working Paper no.146 xiv, 72.
357 Solin and Zerzan “Mobile Money: Methodology for Assessing Money Laundering Risks” 14.
358 Solin and Zerzan “Mobile Money: Methodology for Assessing Money Laundering Risks” 14.
359 Solin and Zerzan “Mobile Money: Methodology for Assessing Money Laundering Risks” 14.
360 World Bank Working Paper no.146 xiv, 72.
361 World Bank Working Paper no.146 13.
362 Solin and Zerzan “Mobile Money: Methodology for Assessing Money Laundering Risks” 14.
363 World Bank Working Paper no.146 xiv, 29, 72.
364 See World Bank Working Paper no.146 13 for more detail in this regard.

As mentioned previously,[365] however, the FATF concedes that a so-called "overly cautious approach" to AML measures can inadvertently lead to the exclusion of legitimate individuals from the financial system.[366] Financial exclusion could, in turn, compromise the effectiveness of an AML regime. Therefore, financial inclusion initiatives and AML measures should be viewed as "serving complementary objectives."[367] There are three fundamental aspects of mobile money which can further both financial inclusion and financial integrity.[368] Firstly, mobile money could lead to decreased reliance on cash,[369] which is the "common enemy" of both financial inclusion and financial integrity.[370] Secondly, mobile money generates data, which contributes to the well-being and increase of financial inclusion as well as financial integrity.[371] Lastly, mobile money facilitates the increased occurrence of accounts, which is at the core of both financial inclusion and financial integrity.[372] Winn and De Koker[373] are of the opinion that mobile money will, however, not be in a position to reach its full potential for furthering financial inclusion and financial integrity unless certain regulatory barriers are removed.[374]

South African AML regulations predominantly influence mobile money by means of CDD requirements which financial institutions are expected to observe.[375] The current position in most instances is that the same CDD requirements exist for all categories of accounts, regardless of what amounts are held in, or can be transferred by means of, these accounts.[376] This is counterproductive since it defeats the very objective of CDD measures and causes the general system to be unproductive.[377] As was seen in Chapter 3, uniform CDD measures entail that certain individuals will not be in a position to open accounts, solely based on the fact that they are not in possession of the required documentation.[378] As a result, these

365 In Chapter 1.
366 *FATF Guidance for a Risk-Based Approach* 2.
367 *FATF Guidance for a Risk-Based Approach* 3.
368 Winn and De Koker 2013 *WJLTA* 159; Alexandre and Eisenhart 2013 *WJLTA* 287.
369 As was seen in Chapter 2.
370 Winn and De Koker 2013 *WJLTA* 159; Alexandre and Eisenhart 2013 *WJLTA* 287.
371 Winn and De Koker 2013 *WJLTA* 159; Alexandre and Eisenhart 2013 *WJLTA* 287.
372 Winn and De Koker 2013 *WJLTA* 159; Alexandre and Eisenhart 2013 *WJLTA* 287.
373 Winn and De Koker 2013 *WJLTA* 159.
374 Winn and De Koker 2013 *WJLTA* 159.
375 Lawack 2013 *WJLTA* 332.
376 Alexandre and Eisenhart 2013 *WJLTA* 299.
377 Alexandre and Eisenhart 2013 *WJLTA* 299.
378 Alexandre and Eisenhart 2013 *WJLTA* 299.

individuals will be compelled to resort back to informal financial instruments or services which are not subject to AML measures.[379] Thus, the financial inclusion potential of mobile money will be lost on these individuals, and the opportunity for improved financial integrity will go to waste.

This having been said, it cannot be denied that client identification and verification is one of the most fundamental principles of mitigating money laundering risks which should enjoy continued implementation.

4.3 Customer due diligence, mobile money and the risk-based approach

As was previously seen,[380] mobile money service providers are "accountable institutions"[381] which usually establish business relationships with clients as provided for by FATF Recommendation 10 and as such they will consequently be subject to the provisions of legislation enacted by virtue of FATF Recommendation 10, such as section 21 of FICA.[382]

Implementing CDD measures can, however, pose a challenge for financial institutions.[383] In this regard, it is imperative to make a distinction between identifying a client and verifying a client's identification. Client identification consists of obtaining information with regard to the prospective client for the purpose of identifying said client. No documentation is gathered at this stage, as opposed to the stage where the client's identification is verified, which involves scrutinising "reliable, independent source documentation, data or information"[384] that verifies the authenticity of the information that was collected during the preceding process of identification.[385]

379 Alexandre and Eisenhart 2013 *WJLTA* 299; *FATF Guidance for a Risk-Based Approach* 2; *FATF Guidance: AML and Financial Inclusion* 38.
380 In Chapters 2 and 3
381 See Chapter 2 in this regard.
382 *FATF Guidance for a Risk-Based Approach* 94; *FATF Guidance: AML and Financial Inclusion* 64.
383 *FATF Guidance: AML and Financial Inclusion* 66.
384 *FATF Guidance: AML and Financial Inclusion* 66.
385 *FATF Guidance: AML and Financial Inclusion* 66.

As was seen in Chapter 3, South African AML measures give rise to certain practical complications as far as identification and verification requirements are concerned. It should be stressed that these difficulties are not brought about by the *FATF Recommendations*. In an ordinary CDD situation, the *FATF Recommendations*, unlike FICA, do not necessitate the collection of information regarding issues such as residential address.[386] In fact, FATF Recommendation 10 makes it clear that although it should be obligatory for financial institutions to implement CDD measures, the scope of such measures should be established by means of a risk-based approach (RBA).[387]

The notion behind an RBA is, in essence, that jurisdictions are permitted and encouraged to do away with uniform or so-called "one-size-fits-all" approaches to AML regimes, and adapt existing AML regimes according to "specific national risk context."[388] The RBA places an obligation on jurisdictions to follow a stricter approach in instances where higher money laundering risks have been identified, and gives them the option to follow a simplified approach in the instances where lower money laundering risks have been identified.[389] It furthermore allows for exemptions from specific AML requirements in certain justified cases.[390] The nature and intensity of the money laundering risks identified will consequently determine the stringency of AML measures under the RBA.[391]

Following an RBA thus enables jurisdictions to implement AML measures which are more accommodating towards clients and financial institutions alike, thereby enabling them to assign their resources more efficiently and implement preventative

386 *FATF Guidance: AML and Financial Inclusion* 67.
387 In accordance with the Interpretive Notes to Recommendation 10 and Recommendation 1. See *FATF Guidance for a Risk-Based Approach* 95 in this regard as well.
388 FATF Recommendation 1; Interpretive Note 2 to Recommendation 1; *FATF Guidance for a Risk-Based Approach* 64, 90; *FATF Guidance: AML and Financial Inclusion* 37.
389 *FATF Guidance for a Risk-Based Approach* 64, 90. Simplified CDD measures can, for instance, be considered where NPPS pose lower risks. See *FATF Guidance for a Risk-Based Approach* 95 in this regard.
390 Interpretive Note 2 to Recommendation 1; *FATF Guidance for a Risk-Based Approach* 64, 87, 90. See Interpretive Note 6 to Recommendation 1 regarding conditions which need to be met before exemption will be justified. CDD has, however, proven to be an effective measure to mitigate money laundering risk associated with NPPS (see *FATF Guidance for a Risk-Based Approach* 63) and as such it is unlikely for jurisdictions to exempt NPPS providers from being subject to CDD measures altogether.
391 *FATF Guidance for a Risk-Based Approach* 90; Alexandre and Eisenhart 2013 *WJLTA* 287.

measures which are proportionate to identified risks, placing them in a position to focus their efforts in combating money laundering effectively.[392]

The *G20 Principles for Innovative Financial Inclusion* also promote the application of the so-called "proportionality principle"[393] which entails finding the correct balance between risks and benefits and accordingly shaping AML regulation to mitigate the money laundering risk of the mobile financial service "without imposing an undue regulatory burden that could stifle innovation."[394] An RBA will prevent the imposition of unwarranted and disproportionate AML obligations, including requirements that may impede access to mobile money for unbanked individuals.[395] An RBA to mobile money thus enables jurisdictions to effectively address the problem of financial exclusion, which embodies a money laundering risk and an obstruction to accomplishing successful implementation of the *FATF Recommendations* in itself,[396] by allowing both regulators and mobile money providers to tailor AML frameworks so as to "better align financial inclusion and financial integrity objectives."[397]

The fact that the FATF encourages and indeed recommends the implementation of an RBA towards AML is set out at the very onset of the *FATF Recommendations* – in FATF Recommendation 1. According to this Recommendation,[398] the risks of money laundering should first be identified, assessed, and understood, after which appropriate measures to mitigate the risk should be adopted.[399] This is an essential first step in applying an RBA[400] and an all-encompassing principle which must be

392 Interpretive Note 1 to Recommendation 1; *FATF Guidance for a Risk-Based Approach* 89.
393 G20 Principles for Innovative Financial Inclusion Principle 8.
394 *FATF Guidance for a Risk-Based Approach* 87.
395 *FATF Guidance for a Risk-Based Approach* 86.
396 Continued financial exclusion leads to a continued increase in transactions being conducted through the informal financial system, away from regulatory and supervisory oversight. See *FATF Guidance for a Risk-Based Approach* 90; *FATF Guidance: AML and Financial Inclusion* 37, 38; Alexandre and Eisenhart 2013 *WJLTA* 300 in this regard.
397 De Koker 2013 *WJLTA* 182.
398 FATF Recommendation 1.
399 FATF Recommendation 1. Interpretive Note 2 to Recommendation 1 makes it clear that in implementing an RBA, financial institutions should have processes in place to identify, assess, monitor, manage and mitigate money laundering risks.
400 *FATF Guidance for a Risk-Based Approach* 89.

kept in mind in applying any AML measure provided for by the *FATF Recommendations*.[401]

The general application of an RBA can allow for flexibility regarding, *inter alia*, CDD measures.[402] The FATF's stance on simplified CDD, specifically in the context of NPPS,[403] will now be discussed against the backdrop of the South African legal position as discussed in Chapter 3.[404]

4.3.1 Simplified customer due diligence, mobile money and the FATF

When developing an AML regime for NPPS, such as mobile money, the effect that proposed regulation will have on the existing NPPS market should be taken into consideration.[405] Ideally, steps should be taken to ensure that AML measures remain commensurate to the money laundering risks posed by NPPS. Regulators should contemplate the potential benefits and the potential detriments and then take a pragmatic RBA to CDD.[406] Failure to do this may affect the operation of existing NPPS in a negative manner, or stifle the progress of yet-to-be-developed NPPS.[407]

When exploring the options of applying an RBA, it should be kept in mind that different financial products and services hold different risks for the financial system.[408] It is for this reason that FATF Recommendation 15 – which expects jurisdictions and financial institutions to identify and assess the money laundering risks that may stem from "(a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing

401 *FATF Guidance for a Risk-Based Approach* 89. Specific FATF Recommendations set out more precisely how this general principle applies to particular requirements. See Interpretive Note 2 to Recommendation 1 in this regard.
402 *FATF Guidance: AML and Financial Inclusion* 77.
403 Including mobile money.
404 The CDD obligations imposed by South African legislation were comprehensively discussed in Chapter 3 and will therefore not be repeated here.
405 *FATF Guidance for a Risk-Based Approach* 85.
406 Jenkins "Developing Mobile Money Ecosystems" 22-23.
407 *FATF Guidance for a Risk-Based Approach* 85.
408 Lawack 2013 *WJLTA* 329.

technologies for both new and pre-existing products"[409] – is of specific relevance in the context of mobile money.[410]

Under an RBA, the extent to which providers of NPPS should implement CDD measures[411] will thus vary depending on the outcome of the application of Recommendation 15, consistent with the *FATF Recommendations* and the regulative measures in the specific jurisdiction.[412] The underlying principle in this regard is that the intensity of AML measures should be commensurate to the risk posed by the NPPS[413] – therefore, a uniform approach to CDD for NPPS is not applicable, since a uniform approach is not proportionate to the risks of different types of products and services.[414] A low-value product or service should be subject to fewer enquiries than a product or service which is designed to facilitate larger transfers or account balances.[415] If CDD measures are too stringent, only a small percentage of the total amount of transactions within a jurisdiction will be subject to it – the overall amount of transactions performed within a jurisdiction will not be less, there will merely be a greater percentage of transactions which are conducted informally and which will therefore not be subject to control measures such as CDD.[416] As Alexandre and Eisenhart so eloquently put it:

> Applying a disproportionately high level of [CDD] to some accounts and/or transactions does not make them safer in any way but simply more expensive. Putting on a helmet, gloves, and a padded jacket before heading out for a stroll on a walkway similarly does not add much to one's security. It mostly adds cost and inconvenience. Finding the right level of [CDD] is a matter of efficiency for the service providers and for the whole system.[417]

409 FATF Recommendation 15.

410 FATF Recommendation 15; *FATF Guidance for a Risk-Based Approach* 89; De Koker 2013 *WJLTA* 177. While De Koker is of the opinion that Recommendation 15 is redundant in light of FATF Recommendation 1 which contains more comprehensive and fundamental obligations regarding risk assessment (see De Koker 2013 *WJLTA* 177), it is the author's submission that Recommendation 15 can be viewed as a reiteration of the importance of risk assessment aimed at implementing an RBA, not only in terms of already existing AML regulations but also when designing and adopting new AML measures for purposes of regulating NPPS (see *FATF Guidance for a Risk-Based Approach* 89 in this regard).

411 Specifically measures to identify clients and verify clients' identity. See *FATF Guidance for a Risk-Based Approach* 63.

412 *FATF Guidance for a Risk-Based Approach* 63. See par 4.4 regarding South Africa's regulatory stance in terms of varying measures for varying risks.

413 *FATF Guidance for a Risk-Based Approach* 114.

414 Alexandre and Eisenhart 2013 *WJLTA* 299 in this regard.

415 Alexandre and Eisenhart 2013 *WJLTA* 299 in this regard.

416 I.e. financial exclusion is exacerbated. See Alexandre and Eisenhart 2013 *WJLTA* 299 in this regard.

417 Alexandre and Eisenhart 2013 *WJLTA* 299-300.

The proposed solution is to implement a so-called "tiered" approach in terms of which different CDD measures apply to different types of products, services or accounts, as provided for in FATF Recommendation 10.[418]

Interpretive Note 21 to Recommendation 10 makes specific provision for simplified CDD measures and lists the following examples:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions exceed an established monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.[419]

Simplified CDD never amounts to an absolute exemption or absence of CDD measures. Even in cases of simplified CDD, there must be rudimentary measures responding to all components of CDD.[420] Simplified CDD measures simply influence the type and the extent of information required, and the means by which compliance with these minimum standards[421] are effected.[422]

In a lower risk situation, complying with CDD requirements as per FATF Recommendation 10 could, for example, involve less stringent means of obtaining information.[423] The *FATF Recommendations* provide examples of instances where the risk of money laundering can be considered as potentially lower, with regard to certain variables.[424] "Financial products or services that provide appropriately defined and limited services to certain types of clients**,** so as to increase access for

418 Alexandre and Eisenhart 2013 *WJLTA* 300.
419 Interpretive Note 21 to Recommendation 10. See also *FATF Guidance for a Risk-Based Approach* 64.
420 I.e. identification and verification of the client's identity; identification of the beneficial owner; understanding the purpose of the business relationship; and on-going monitoring of the relationship. See *FATF Guidance for a Risk-Based Approach* 95.
421 These minimum standards being the four components as mentioned in fn 95 above.
422 See *FATF Guidance for a Risk-Based Approach* 64.
423 *FATF Guidance for a Risk-Based Approach* 64.
424 See Interpretive Notes 16 and 17 to Recommendation 10 in this regard.

financial inclusion purposes" is explicitly included as such a lower risk example pertaining to NPPS.[425] This makes it clear that the FATF supports the development of financial products and services that will facilitate financial inclusion, whilst mitigating money laundering risks associated with financial exclusion.[426]

4.3.2 Mitigating measures which facilitate the application of simplified customer due diligence

The implementation of thresholds, or limitations as it is also called, is an important consideration with respect to CDD and NPPS. Thresholds have proven to effectively mitigate service-specific financial integrity risk, and could therefore be a measure towards the effective application of simplified CDD.[427] The degree of threshold will vary from jurisdiction to jurisdiction and should be determined in accordance with a risk assessment of the specific NPPS.[428]

As far as mobile money is concerned, thresholds could be placed on several different aspects of the service, including the following:[429]

- the maximum amount of stored value that can be held in the account at any given time;
- the maximum amount allowed per single transaction, including cash withdrawals;
- the frequency or amount of transactions and cash withdrawals permitted per time period;[430]
- the total value of transactions and cash withdrawals permitted per time period;[431]

425 Interpretive Note 17(b) to Recommendation 10. Providers of NPPS should, however, also take note of the circumstances under which a client of an NPPS may be considered higher risk and ensure that there are procedures in place to conduct enhanced CDD measures in instances where higher money laundering risk is identified. See *FATF Guidance for a Risk-Based Approach* 64; Interpretive Notes 15 to Recommendation 10 for higher risk circumstances.

426 *FATF Guidance: AML and Financial Inclusion* 70.

427 See Interpretive Note 21 to Recommendation 10 which specifically mentions instances where simplified CDD is to be implemented in parallel with thresholds.

428 *FATF Guidance for a Risk-Based Approach* 96.

429 *FATF Guidance for a Risk-Based Approach* 75.

430 E.g. per day, week, month or year. See *FATF Guidance for a Risk-Based Approach* 75.

431 E.g. per day, week, month or year. See *FATF Guidance for a Risk-Based Approach* 75.

- a combination of any or all of the above.

Geographical or purchasing limitations could also act as mitigating factors which decrease the risk of mobile money being abused for money laundering purposes.[432] Applying thresholds or limitations to certain financial services could cause those services to become lower risk products due to the fact that thresholds in itself lower money laundering risks.[433]

The tiered approach[434] yet again poses a feasible option for effectively implementing the above thresholds in conjunction with simplified CDD as part of an RBA, given the fact that the money laundering risk increases proportionately to the functionality of a specific NPPS.[435] Such a tiered approach should be developed "on a case-by-case basis during the design phase of each NPPS."[436] This will afford financial institutions the opportunity to consider applying different thresholds and other restrictions to different forms of NPPS in order to ensure that each individual NPPS remains a lower risk product, which in turns allows for the application of simplified CDD in respect of each form of NPPS.[437] The level of CDD and other AML measures should increase as the functionality of the NPPS, and therefore also the risk, increases.[438] This approach may provide financially excluded individuals the opportunity to open accounts or access other financial services, albeit with very limited functionalities.[439] Access to additional services[440] should be allowed only once the client provides proof of identity and address.[441]

---

432 *FATF Guidance for a Risk-Based Approach* 75.
433 The stricter the limits that are set for particular types of products/services, the more likely it would be that the overall money laundering risk would be reduced and that those products/services could be considered as lower risks. See *FATF Guidance for a Risk-Based Approach* 97; *FATF Guidance: AML and Financial Inclusion* 74.
434 As previously discussed under par 4.3.1
435 As was seen in par 2.2 above. See also *FATF Guidance for a Risk-Based Approach* 72.
436 *FATF Guidance for a Risk-Based Approach* 72.
437 *FATF Guidance for a Risk-Based Approach* 72.
438 *FATF Guidance for a Risk-Based Approach* 72, 74.
439 *FATF Guidance: AML and Financial Inclusion* 74.
440 Such as higher transaction limits or account balances or access through diversified delivery channels. See *FATF Guidance: AML and Financial Inclusion* 74 in this regard.
441 *FATF Guidance: AML and Financial Inclusion* 74.

4.4 South Africa and the risk-based approach in terms of customer due diligence

In their endeavour to develop banking products aimed at enhancing financial inclusion, South African authorities were mindful of the fact that most individuals living in South Africa typically did not have residential addresses which could be verified by means of formal documentation and that imposing full CDD – which, under national legislation,[442] includes obtaining and verifying a residential address – would accordingly be impractical. Such stringent CDD measures would have the effect that the majority of individuals whom these products would be designed for would not have access to it. The South African legislator thus devised Exemption 17[443] in this regard, in terms of which financial institutions are exempt from verifying the residential address of a client, provided certain requirements are met.[444] If the client breaches compliance of these requirements after having opened such an account, the accountable institution must conduct full CDD before executing any further transactions associated with the account of the client in question.[445]

The FIC furthermore published Guidance Note 1 in April 2004,[446] which is aimed at assisting accountable institutions and supervisory bodies with the practical application of the client identification obligations of FICA and in effect describes an RBA for purposes of establishing and verifying identity. It is submitted that the guidance discussed under Guidance Note 3A[447] is another instance where the FIC describes an RBA.

FICA and the MLTFC Regulations[448] compel accountable institutions to identify all their clients unless circumstances exist which warrant the application of an exemption. However, no uniform approach is prescribed for the methods which should be used to effect this identification or the levels of verification which should be

442 Namely the *Financial Intelligence Centre Act* 38 of 2001.
443 Reg R1353 in GG 27011 of 19 November 2004.
444 For a complete discussion of Exemption 17, refer to par 3.3.4 of this dissertation. See aslo Interpretive Note 16 to Recommendation 10; World Bank Working Paper no.146 61.
445 Reg R1353 in GG 27011 of 19 November 2004.
446 GN 534 in GG 26278 of 30 April 2004.
447 As discussed under par 3.3.4
448 Reg R1595 in GG 24176 of 20 December 2002.

applied. The MLTFC Regulations[449] state that accountable institutions must verify certain particulars which they have obtained from a client or potential client by means of "information which can reasonably be expected to achieve such verification *and* is obtained by reasonably practical means."[450] This suggests that an accountable institution has a discretion regarding the information which is necessary for purposes of verification, as well as the means by which it should be obtained.[451] In exercising this discretion, the "accuracy of the verification required and the level of effort invested to obtain such verification" should be balanced to ensure that the verification process is proportional to the nature of the risk which is posed by the transaction or business relationship.[452]

From the above it becomes apparent that South Africa has clearly followed an RBA, at least to some extent. However, no formal risk assessment regarding mobile money has been conducted to date.[453] The FATF makes it clear that in "*all* situations of simplified CDD,"[454] the lower risk circumstances need to be validated "based on a thorough and documented risk assessment, conducted at the national, sectoral or at the financial institution level."[455] According to the World Bank, it is worthwhile to go through the process of identifying, measuring, and decreasing potential money laundering risks given the developmental potential of mobile financial services[456] – a statement with which the author agrees. Recommendations in this regard will be made in Chapter 5.

4.5 Conclusion

From the above it can be concluded that while mobile money does indeed pose a threat to financial integrity if not regulated appropriately, it can also strengthen financial integrity by means of eradication of financial exclusion. Reaching both the

449 Reg R1595 in GG 24176 of 20 December 2002.
450 Reg R1595 in GG 24176 of 20 December 2002 Regs 4(3) and 16(2), own emphasis added.
451 *FATF Guidance: AML and Financial Inclusion* Annex 7; G20 Principles for Innovative Financial Inclusion Principle 9.
452 *FATF Guidance: AML and Financial Inclusion* Annex 7; G20 Principles for Innovative Financial Inclusion Principle 9.
453 Lawack 2013 *WJLTA* 341.
454 *FATF Guidance: AML and Financial Inclusion* 69, own emphasis added.
455 Interpretive Note 16 to Recommendation 10; *FATF Guidance: AML and Financial Inclusion* 69.
456 World Bank Working Paper no.146 2.

objectives of enhanced financial integrity and financial inclusion can be made possible by means of the application of an RBA as provided for by the *FATF Recommendations*.[457] This will typically entail simplified CDD measures.

While the implementation of simplified CDD measures is not obligatory, the failure to do so could frustrate financial inclusion objectives.[458] These factors should be given due consideration in the application of an RBA to AML regulation. It is eventually the responsibility of each jurisdiction to ensure that its AML regime conforms to the *FATF Recommendations*, while remaining cognisant if its own circumstances and risk profile.[459] Jurisdictions will have to decide on the different criteria required to benefit from a simplified CDD regime within their own unique national risk context, or require financial institutions to do so within their own risk management framework.[460]

Everything considered, it would seem as if applying an RBA which is tiered in terms of services is the most suitable method for implementing AML measures without over-burdening developmental efforts of NPPS.[461]

5 Conclusion and recommendations

Throughout this dissertation, it has become abundantly clear that mobile money is a powerful tool towards financial inclusion, as initially suggested in Chapter 1. However, it also became clear that mobile money poses significant money laundering risks if not suitably regulated. The question to be answered was: how can the preservation of financial integrity and the promotion of financial inclusion be balanced in such a way that mobile money can be utilised and developed effectively, thereby promoting financial inclusion, without being detrimental to financial integrity?

Although the opposite may have seemed true at first, it eventually became apparent that mobile money serves the objectives of both financial inclusion and financial

457 FATF Recommendation 1.
458 De Koker 2013 *WJLTA* 177.
459 *FATF Guidance for a Risk-Based Approach* 116.
460 *FATF Guidance for a Risk-Based Approach* 116.
461 Lawack 2013 *WJLTA* 329; World Bank Working Paper no.146 xiv.

integrity,[462] since financial exclusion is a money laundering risk, which means that financial inclusion can promote a more effective AML regime.[463] Therefore, increased financial inclusion and increased financial integrity by means of an effective AML regime can – and should – be "complementary national policy objectives with mutually supportive policy goals."[464] Mobile money can only deliver on its promises for both financial inclusion and financial integrity as long as it is not stifled by over-regulation.[465]

Reaching both the objectives of enhanced financial integrity and enhanced financial inclusion can be made possible by means of the application of an RBA as provided for by the *FATF Recommendations*, specifically by implementing simplified CDD measures,[466] which is optional, but can be highly conducive to increased financial inclusion, and as a result, financial integrity.

South Africa currently has a comprehensive AML framework which has been criticised for being too stringent and held responsible for the fact that mobile money is not reaching its full potential in South Africa.[467] Although initial research indicated that an over-cautious and uniform approach to CDD could indeed be what is stifling the widespread development and acceptance of mobile money, it eventually became clear that South Africa is following an RBA to a large extent in the application of simplified CDD in certain instances. This is evident from measures such as Exemption 17,[468] which also prescribes the use of thresholds in tandem with simplified CDD – completely in line with the FATF Recommendations.[469] The problem which was identified by the author is rather the fact that no formal risk assessment of mobile money products and services has been conducted in South Africa to date.[470]

462 Alexandre and Eisenhart 2013 *WJLTA* 287; *FATF Guidance: AML and Financial Inclusion* 39.
463 As discussed under par 4.2.2. See also *FATF Guidance: AML and Financial Inclusion* 27.
464 *FATF Guidance: AML and Financial Inclusion* 29.
465 Alexandre and Eisenhart 2013 *WJLTA* 287.
466 FATF Recommendation 1.
467 Lawack 2013 *WJLTA* 336; De Koker 2004 *Journal of South African Law* 742.
468 Reg R1353 in GG 27011 of 19 November 2004.
469 Interpretive Note 21 to Recommendation 10.
470 Lawack 2013 *WJLTA* 341.

The reason why this is a problem, is two-pronged. Firstly, the risk-based approach as provided for in FATF Recommendation 1 is a mandatory requirement, and the foundation of the risk-based approach is risk assessment.[471] Secondly, the FATF expressly requires that lower risk circumstances need to be validated "based on a thorough and *documented risk assessment*, conducted at the national, sectoral or at the financial institution level"[472] in all instances of simplified CDD.[473] This means that South African simplified CDD measures as contained in Exemption 17,[474] Guidance Note 1[475] and Guidance Note 3A fall in a grey area as far as the *FATF Recommendations* are concerned. The legislator has provided these instruments without conducting a national risk assessment and has left financial institutions to their own devices in applying an RBA to simplified CDD.

It is the author's submission that this is causing confusion regarding South Africa's regulatory stance towards mobile money. The fact that there is no South African legislation which explicitly provides for or regulates mobile money, which is a unique financial service, contributes to the confusion and legal uncertainty.

It is accordingly recommended by the author that a formal money laundering risk assessment should be done on national level in order to establish a national standard for lower-risk and higher-risk scenarios in terms of which a general RBA, and particularly simplified CDD, can be adopted in accordance with the *FATF Recommendations.*[476] According to the World Bank, a service-based approach is more effective than a provider-based approach in terms of assessing actual money laundering risks for mobile financial services.[477] The author therefore accordingly submits that this approach be kept in mind for purposes of mobile money in particular, if and when a formal risk assessment, as suggested, takes place. The *FATF Guidance for a Risk-Based Approach (2013): Prepaid Cards, Mobile*

471 Lawack 2013 *WJLTA* 341.
472 Interpretive Note 16 to Recommendation 10; *FATF Guidance: AML and Financial Inclusion* 69, own emphasis added.
473 *FATF Guidance: AML and Financial Inclusion* 69, own emphasis added.
474 Reg R1353 in GG 27011 of 19 November 2004.
475 GN 534 in GG 26278 of 30 April 2004.
476 Lawack 2013 *WJLTA* 344.
477 World Bank Working Paper no.146 xiii.

Payments and Internet-Based Payment Services could furthermore be effectively employed in such an endeavour.

Once a formal risk assessment has been conducted and a national standard for lower-risk and higher-risk scenarios has been established, the application of a tiered RBA in terms of the risks presented by individual services, rather than the individual institutions offering them, would most likely be the most suitable method for implementing AML measures without over-burdening developmental efforts of NPPS.[478]

It is lastly submitted that it would be in the interest of legal certainty if the legislator adopts specific regulatory measures which make provision for mobile money under different business models, thereby providing clarity and enhancing trust in mobile money services.

478 Lawack 2013 *WJLTA* 329; World Bank Working Paper no.146 xiv.

REFERENCE LIST

Aker and Mbiti 2010 Journal of Economic Perspectives

Aker JC and Mbiti IM "Mobile Phones and Economic Development in Africa" 2010 *Journal of Economic Perspectives* 207-232

Alexandre and Eisenhart 2013 *WJLTA*

Alexandre C and Eisenhart LC "Mobile Money as an Engine of Financial Inclusion and Lynchpin of Financial Integrity" 2013 *Washington Journal of Law, Technology & Arts* 285-302

Avina 2011 *Journal of Financial Crime*

Avina J "Public-private partnerships in the fight against crime: An emerging frontier in corporate social responsibility" 2011 *Journal of Financial Crime* 282-291

Chaix and Torre *Different models for mobile payments*

Chaix L and Torre D *Different models for mobile payments* 2010 Working Paper University of Nice Sophia-Antipolis

World Bank Working Paper no.146

Chatain P, Hernández-Coss R, Borowik K and Zerzan A *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing* (World Bank Working Paper no.146) 2008

Coetzee 2009 *South African Journal of Economic and Management Sciences*

Coetzee J "Personal or remote interaction? Banking the unbanked in South Africa" 2009 *South African Journal of Economic and Management Sciences* 448-461

De Koker 2004 *Journal of South African Law*

De Koker L "Client identification and money laundering control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004 *Journal of South African Law* 715-746

De Koker 2011 *Journal of Financial Crime*

De Koker L "Aligning anti-money laundering, combating of financing of terror and financial inclusion: Questions to consider when FATF standards are clarified" 2011 *Journal of Financial Crime* 361-386

FATF GAFI MER

FATF GAFI Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism, South Africa of 29 February 2009

FATF Guidance: AML and Financial Inclusion

FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (February 2013)

FATF Guidance for a Risk-Based Approach

FATF Guidance for a Risk-Based Approach (2013): Prepaid Cards, Mobile Payments and Internet-Based Payment Services

FATF Methodology

FATF Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems (2013)

FATF Recommendations

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: FATF Recommendations (2012)

G20 Principles for Innovative Financial Inclusion

G20 Principles for Innovative Financial Inclusion 2010

Grabosky, Smith and Dempsey Electronic Theft: Unlawful Acquisition in Cyberspace

Grabosky P, Smith R and Dempsey G *Electronic Theft: Unlawful Acquisition in Cyberspace* (Cambridge University Press Cambridge 2001)

Gurusamy *Financial Services and Systems*

Gurusamy S *Financial Services and Systems* 2nd edition (Tata McGraw-Hill Education 2009)

Jenkins “Developing Mobile Money Ecosystems”

Jenkins B “Developing Mobile Money Ecosystems” 2008 *Washington, DC: International Finance Corporation and the Harvard Kennedy School*

Jobodwana *JICLT*

Jobodwana ZN “E-Commerce and Mobile Commerce in South Africa: Regulatory Challenges” 2009 *Journal of International Commercial Law and Technology* 287-298

Kellerman “Mobile Risk Management: E-finance in the Wireless Environment”

Kellerman T “Mobile Risk Management: E-finance in the Wireless Environment” Financial Sector Discussion Paper 2002.

Klein and Mayer *Mobile banking and financial inclusion: The regulatory lessons*

Klein M and Mayer C *Mobile banking and financial inclusion: The regulatory lessons* 2011 Working Paper 116 form the Working Paper series of the Frankfurt School of Finance & Management

Lawack 2013 *WJLTA*

Lawack VA “Mobile Money, Financial Inclusion and Financial Integrity: The South African Case” 2013 *Washington Journal of Law, Technology & Arts* 317-346

Lyons, Phillips, Valdés-Valdivieso and Penteriani *Sub-Saharan Mobile Observatory 2012*

Lyons P, Phillips T, Valdés-Valdivieso L and Penteriani G *Sub-Saharan Mobile Observatory 2012*

O’Sullivan and Sheffrin *Economics: Principles in Action*

O’Sullivan A and Sheffrin SM *Economics: Principles in Action* (Prentice Hall New Jersey 2003)

Palermo Convention

United Nations Convention against Transnational Organised Crime (2000)

Reuter and Truman *Chasing Dirty Money*

Reuter P and Truman EM *Chasing Dirty Money: The Fight Against Money Laundering* (Institute for International Economics Washington 2004)

Schoombee 2004 *South African Journal of Economics*

Schoombee A "South African Banks and the Unbanked: Progress and Prospects" 2004 *South African Journal of Economics* 581 – 603

Solin and Zerzan "Mobile Money: Methodology for Assessing Money Laundering Risks"

Solin M and Zerzan A "Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks" 2010 GSMA Discussion Paper

Van Duyne *Criminal Finance and Organising Crime in Europe*

Van Duyne PC "Money laundering policy: fears and facts" 2003 *Criminal Finance and Organising Crime in Europe*

Vienna Convention

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)

Winn and De Koker 2013 WJLTA

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 & Arts* 155 – 164

Register of legislation

Banks Act 94 of 1990

Financial Intelligence Centre Act 38 of 2001

Financial Intelligence Centre Amendment Act 11 of 2008

Mutual Banks Act 124 of 1993

National Payment System Act 78 of 1998

Postal Services Act 124 of 1998

Prevention of Organised Crime Act 121 of 1998

R1595 in GG 24176 of 20 December 2002

GN 715 in GG 27803 of 18 July 2005

Financial Intelligence Centre Guidance Note 3A: Guidance for accountable institutions on client identification and verification and related matters of 28 March 2013

Position Paper NPS 01/2009: South African Reserve Bank National Payment System Department Position Paper on Electronic Money of November 2009

The Banks Act Guidance Note 6/2008 issued by the Registrar of Banks

Register of case law

Standard Bank of South Africa Ltd v 3MFuture Africa (Pty) Ltd 2013 JDR 2748 (SCA)

Register of internet sources

Anon 2012 www.southafrica.info

Anon 2012 *South Africa's Population* http://www.southafrica.info/about/people/population.htm#.VHe9cjGUeAU

Anon 2013 http://www.mobileburn.com

Anon 2013 *What is "prepaid"?* http://www.mobileburn.com/definition.jsp?term=pre-paid

Anon 2013 tradingeconomics.com

Anon 2013 *South Africa 'two-thirds urbanised'* www.southafrica.info accessed 12 June 2014

BusinessDictionary.com 2014 http://www.businessdictionary.com

BusinessDictionary.com 2014 *Emerging Markets* http://www.businessdictionary.com/definition/emerging-markets.html#ixzz3IzH3nPli

BusinessDictionary.com 2014 *Financial Services* http://www.businessdictionary.com/definition/financialservices.html#ixzz3I5Sdfxj7

FIC 2008 https://www.fic.gov.za

FIC 2008 *Financial Action Task Force* https://www.fic.gov.za/SiteContent/ContentPage.aspx?id=115 accessed 9 May 2013

FIC 2013 https://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/FIC%20Annual% 20 Report %202012-13.pdf

FIC 2013 *Financial Intelligence Centre Annual Report 2012/13* https://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/FIC%20Annual%20Report%202012-13.pdf

Goldstuck 2014 http://mg.co.za

Goldstuck A 2014 *Vodacom re-launches M-pesa (again)* http://mg.co.za/article/2014-08-04-vodacom-re-launches-m-pesa-again accessed 7 August 2014

GSMA 2013 https://mobiledevelopmentintelligence.com

GSMA 2013 *South Africa (Africa)* https://mobiledevelopmentintelligence.com/countries/ZAF-south-africa accessed 12 June 2014

GSMA 2013 *Impact Pathways – Mobile Money* https://mobiledevelopmentintelligence.com/impact_pathways/mobile-money accessed 12 June 2014

GSMA 2013 *Market penetration, total (%)* https://mobiledevelopmentintelligence.com/statistics/76-market-penetration-total accessed 12 June 2014

GSMA 2013 *Connections, prepaid (%)* https://mobiledevelopmentintelligence.com/statistics/75-connections-prepaid accessed 12 June 2014

GSMA 2013 *Mobile Money* https://mobiledevelopmentintelligence.com/sectors/2-mobile-money accessed 12 June 2014

GSMA 2013 *Population, rural (%)* https://mobiledevelopmentintelligence.com/statistics/33-population-rural accessed 12 June 2014

Khanna and Palepu 2010 http://www.forbes.com

Khanna T and Palepu KG 2010 *How To Define Emerging Markets* http://www.forbes.com/2010/05/27/winning-in-emerging-markets-opinions-book-excerpts-khanna-palepu.html accessed 30 June 2014

South African Reserve Bank 2011 https://www.resbank.co.za

South African Reserve Bank 2011 *Banking Legislation* https://www.resbank.co.za/RegulationAndSupervision/BankSupervision/BankingLegislation/Pages/default.aspx

United Nations 2014 https://treaties.un.org

United Nations 2014 *United Nations Treaty Collection* https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=vi-19&chapter=6&lang=en accessed 17 February 2014

United Nations 2014 *United Nations Treaty Collection* https://treaties.un.org/pages/viewdetails.aspx?src=ind&mtdsg_no=xviii-12&chapter=18&lang=en accessed 17 February 2014