

THE UNIVERSITY OF THE WESTERN CAPE

FACULTY OF LAW

Mobile Money Payments as Vehicles for Money Laundering: A Case Study of Malawi

Research paper submitted in partial fulfilment of the requirements for the award of the

LLM degree

COLLIN BRIAN SUKALI CHITSIME



Supervisor

Professor Lovell Fernandez

2016

Table of Contents

Declaration.....	vii
Acknowledgements.....	viii
List of Acronyms and Abbreviations.....	ix
Key Words.....	x
Chapter One.....	1
1.1 Introduction.....	1
1.2 Money Laundering, Illicit Financial Flows and the Anti-Money Laundering Legal Regime in Malawi.....	4
1.3 The Concept of New Payment Methods.....	6
1.4 Theoretical Premise of the Study.....	11
1.5 Research Question.....	12
1.6 Research Methodology.....	12
1.7 Conclusion.....	13
Chapter Two.....	14
The International Legal Framework on Combating Money Laundering Through Mobile Money Payments	14
2.1 Introduction.....	14
2.2 The United Nations Anti-money laundering legal instruments.....	15

2.2.1 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (The Vienna Convention 1988).....	15
2.2.2 UN Convention against Transnational Organised Crime (The Palermo Convention, 2000).....	17
2.2.3 UN Convention against Corruption (UNCAC) (The Merida Convention, 2003).....	18
2.3 European Union Conventions and Directives on Money Laundering.....	20
2.3.1 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (CoE Convention, 1990).....	20
2.3.2 First EU Directive on Money Laundering: Council Directive 91/308 ECC on Prevention of the Use of the Financial System for the Purpose of Money Laundering.....	22
2.3.3 Second EU Directive on Money Laundering: Directive 2001/97 EC of the European Parliament and of the Council of 4 December 2001 Amending Council Directive 91/308 ECC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering.....	23
2.3.4 Third EU Directive on Money laundering: Council Directive 2005/60/EC on the Prevention of the Use of the financial System for the Purposes of	

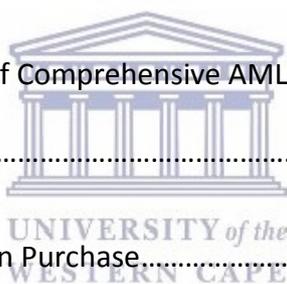


Money Laundering and Terrorist Financing.....	24
2.3.5 The Fourth EU Directive on Money Laundering: Council Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, And Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.....	26
2.4 The FATF International Standards for Combating of Money Laundering and the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.....	27
2.5 Conclusion.....	31
Chapter Three.....	33
3. The Legal Regime Regulating Mobile Money Payments in Malawi.....	33
3.1 Introduction.....	33
3.2 Laws and Institutions Regulating Mobile Money Payments in Malawi.....	34
3.2.1 The Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act and the Regulations made Pursuant to that Act.....	35

3.2.2	The Reserve Bank of Malawi Act (RBM Act).....	38
3.2.3	Guidelines for Mobile Payment Systems.....	40
3.2.4	The Financial Services Act (2010).....	43
3.2.5	Communications Act.....	44
3.3	Gaps in the Regulation and Operation of Mobile Money Payments Services and the Potential Risk to ML/TF in Malawi.....	45
3.3.1	Lack of National Identity Cards.....	47
3.3.2	Non-Registration of SIM Cards on Purchase.....	48
3.3.3	Malawi is a Largely Cash-Based Economy.....	48
3.3.4	Employment of Generic AML/CFT Procedures by Staff of Financial Institutions.....	49
3.3.5	Absence of Credit Risk.....	50
3.3.6	Speed of Transactions.....	51
3.3.7	Non-Face to Face Business Relationship.....	51
3.4	Financial Inclusion.....	51
3.4.1	Balancing between AML/CFT Obligations and Financial Inclusion.....	53
3.5	The Regulation of Mobile Money Payments Services in Kenya: The Case of M-PESA.....	55



3.6	Conformity to FATF Standards by Malawian Regulatory Authorities and Mobile Money Payments Service Providers.....	59
3.7	Conclusion.....	60
Chapter Four.....		62
Conclusions and Recommendations.....		62
4.1	General Conclusions.....	62
4.2	Establishing a National Identification System.....	63
4.3	Extending all AML/CFT Obligations Imposed by Law to Agents.....	63
4.4	Adoption and Application of Comprehensive AML/CFT Procedures by Financial Institutions.....	64
4.5	Registration of SIM Cards on Purchase.....	64
4.6	Investment in Information Communication Technology (ICT).....	65
4.7	Conducting National and Product Risk Assessment.....	65
BIBLIOGRAPHY.....		67



Declaration

I, Collin Brian Sukali Chitsime, declare that *'Mobile Money Payments as Vehicles for Money Laundering: A Case Study of Malawi'* is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Signature:.....

Date:.....



Supervisor: Professor Lovell Fernandez

Signature:.....

Date:.....

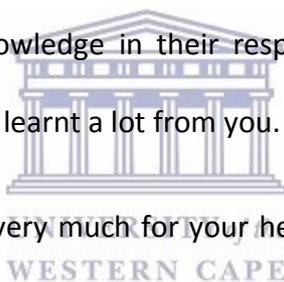
Acknowledgements

First and foremost, I thank Lord God Almighty for the gift of life, the opportunity to study in this wonderful LLM course and making it possible for me to reach this far.

Secondly, I would like to express my deepest gratefulness to my supervisor, Professor Lovell Fernandez for his patience with me, insightful supervision and support. He was with me every step of the way and made it easier for me to write this paper.

Special thanks should go to the generous people of the Federal Republic of Germany for making it possible to study for and complete this LLM course through the DAAD Scholarship.

I am also eternally indebted to Professor G Werle, Professor RA Koen and Dr. M Vormbaum for being immense sources of knowledge in their respective areas of specialisation and imparting the same astutely. I have learnt a lot from you.



To Mr. Windell Nortje, thank you very much for your help and wonderful co-ordination of the course.

My most profound gratitude should go to my classmates, the DAAD class of 2016 (*the ungovernables*). We met as strangers from different African countries but ended up forming bonds that will last a lifetime. You guys made the journey to obtaining the LLM degree bearable. You are part of my extended family.

Lastly, I would like to thank my family for being patient with me and supporting every step of the way. God bless you all for all your sacrifices you have made for me. Mbumba and Uwemi, I love you guys a lot.

“Danke schön”

List of Acronyms and Abbreviations

AFI: Alliance for Financial Inclusion

BTCA: Better Than Cash Alliance

MNO: Mobile Network Operators

AML: Anti-Money Laundering

CDD: Customer Due Diligence

CFT: Combating of Financing of Terrorism

CoE: Council of Europe

ESAAMLG: Eastern and Southern African Anti-Money Laundering Group

EU: European Union

FATF: Financial Action Task Force

FIU: Financial Intelligence Unit

MACRA: Malawi Communications Regulatory Authority

RBM: Reserve Bank of Malawi

MER: Mutual Evaluation Report

STR: Suspicious Transaction Report



Key Words

Airtel Money

Airtel Money Cross Boarder Transfer

Customer Due Diligence

FATF 40 Recommendations

Financial Institutions

Financial Services

Know Your Customer

Malawi

Mobile Phone Operators

Money Laundering

Mobile Money Payments



Chapter One

1.1 Introduction

Money laundering is defined as the process of converting the proceeds derived from a wide range of underlying criminal offences, called predicate offences, to apparently legitimate property.¹ In other words, it is the process of washing away the stain of illegality from the proceeds of crime in order to give them the appearance of legality.² In fact, the nomenclature of the practice itself was inspired by America's notorious gangster Al Capone's practice of channelling the proceeds of his criminal enterprise through his laundromats in order to cloak their illegality so as to endow them with an appearance of legality.³ The crime of money laundering has been a scourge on the economies of the world, hence it has become a crime of international concern. The international community has developed numerous international treaty norms obligating states to criminalise money laundering. These norms, when incorporated into national legislation, are expected to serve as the legal basis not only for national prosecution of money laundering offences but also for international mutual legal assistance in AML (for example, international co-operation in the confiscation of criminal proceeds and extradition of money launderers).⁴



¹ Nguyen C 'Criminalisation of Money Laundering in the International Anti-Money Laundering Regime and its Adoption by Vietnam' *Australian Journal of Asian Law* (2013) 14(1) at 2.

² Gordon R K 'Anti-Money Laundering Policies- Selected Legal, Political, and Economic Issues' *International Monetary Fund; Legal Department; Current Developments in Monetary and Financial Law* (1999) (1) 407.

³ Van Duyne P C 'Money laundering policy'. *Fears and Facts* (2003) 69, available at <http://petrusvandyne.nl/files/Witwassen%20Fears%20and%20Facts.pdf> (Accessed on 23 September 2016).

⁴ Nguyen C (2013: 7).

As indicated above, the crime of money laundering has become a crime of global concern with governments, international organisations, financial institutions, regulators of financial institutions and law enforcement agencies, with all of them investing in efforts to prevent and combat it. Prior to the 1980s, the practice of laundering money was not a criminal offence anywhere in the world.⁵ The United States of America pioneered the efforts to criminalise the practice of money laundering. These efforts to fight money laundering were necessitated by chronic drug and substance abuse, and the increase in international drug trafficking by organised international criminal enterprises.⁶ Money laundering was only dealt with in so far as it related to drug trafficking and dealing.

The first piece of legislation aimed at tackling the scourge of money laundering in the United States of America was the Banking Secrecy Act of 1970.⁷ This law did not deal with money laundering specifically. It dealt mainly with bank secrecy practices and touched on only few aspects of money laundering. The Money Laundering Control Act of 1986, however, addressed the issue of money laundering comprehensively. It is the first enactment in the world to criminalise money laundering. It is the first specific anti-money laundering legislation.⁸

At about the time the United States was enacting the above-mentioned laws, there was a growing recognition elsewhere that there was a need to combat money laundering.

⁵ Sharman J C 'The Global Anti-Money Laundering Regime and Developing Countries: Damned if they Do, Damned if they Don't?' *Government and International Relations University of Sydney, NSW* (2006) 2.

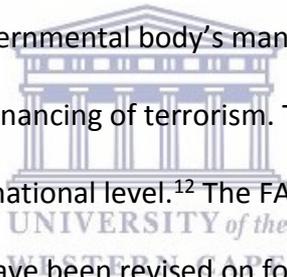
⁶ Gordon R K (1999: 407).

⁷ Unger B and Van Waarden F 'How to Dodge Drowning in Data? Rule- and Risk-Based Anti-Money Laundering Policies Compared' *Review of Law and Economics* 5(2) (2009) 962.

⁸ Unger B and Van Waarden F (2009: 962).

This awareness culminated in the adoption of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances by the United Nations General Assembly in 1988 (Vienna Convention). As was the case with the US anti-money laundering laws, the Vienna Convention regulates money laundering only in so far as it pertains to laundering the proceeds derived from the lucrative illicit trade in narcotic drugs and psychotic substances, hence the full name of the Convention.⁹ The Vienna Convention places an obligation on states parties to criminalise drug-related money laundering and other drug-related processes such as production, cultivation, possession, organisation, management and financing of trafficking operations.¹⁰

After the adoption of the Vienna Convention, G7 countries established the Financial Action Task Force in 1989.¹¹ This inter-governmental body's mandate is to set global standards for combating money laundering and financing of terrorism. The FATF supervises how its standards are implemented at the national level.¹² The FATF first set the money laundering standards in 1990. The standards have been revised on four occasions in order to ensure that they remain up to date and relevant. They were last revised in 2012.¹³



⁹ See United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

¹⁰ Stewart D P 'Internalising the War on Drugs: The UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances' 18 *Denver Journal of International Law and Policies* (1990) 387.

¹¹ Gill M and Taylor G 'Preventing Money Laundering or Obstructing Business?' *British Journal of Criminology* (2004) 583.

¹² Introductory note to the FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism Proliferation (16 February 2012), available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (accessed on 1 September 2016).

¹³ FATF Standards, available at www.fatf-gafi.org/about/ (accessed on 23 August 2016).

Since the Vienna Convention of 1988, there have been further international developments in strengthening the AML/CFT legal regime. In the year 2000, the United Nations General Assembly adopted the Convention against Transnational Organised Crime (the Palermo Convention). This Convention extends the predicate offences of money laundering beyond drug-related offences. It obligates states parties to criminalise money laundering which is predicated on all other serious offences.¹⁴

1.2 Money Laundering, Illicit Financial Flows and the Anti-Money Laundering Legal Regime in Malawi

Malawi, like many African countries and other developing countries, has been heavily affected by the plague of money laundering and other serious economic crimes. Grand corruption and tax evasion are the most prevalent predicate offences of money laundering in Malawi.¹⁵



The widespread nature of public corruption and thievery was well demonstrated when a criminal scheme of serious looting of public funds by public officials and business magnates was exposed in the local media towards the end of 2013. This financial scandal involved the pilfering of 13 billion Malawian Kwacha from the treasury in a space of six months.¹⁶ The crux of the scam involved public officers making sham payments from state coffers to companies which had no contracts with government or which had not rendered any services to the government. In other words, public officials and influential members in the business

¹⁴ Art 5(3) of the Palermo Convention.

¹⁵ Yikona S, Slot B, Geller M et al *Ill-Gotten Money and the Economy: Experiences from Malawi and Namibia* (2011) 25.

¹⁶ Baker Tilly Report on Fraud and Mismanagement of Malawi Government Finances: Covering transactions and controls in the six month period 1 April 2013-30 September 2013 (2014), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/285877/20140221_National_Audit_Office_Malawi_-_Forensic_Audit_Report_-_FINAL_ISSUED.pdf (accessed on 28 September 2016).

community connived to misappropriate public funds. The scam has had dire consequences, for the poor especially, who constitute the majority of the population.

Apart from corruption and tax evasion, Malawi has been heavily affected also by illicit financial flows. According to Global Financial Integrity, illicit financial flows consist in the cross-border movement of money that is illegally earned, transferred, or utilised. This definition was adopted by the African Union Panel on Illicit Financial Flows from Africa (2015).¹⁷ Malawi's illicit financial flows constitute 12-14 percent of the country's gross domestic product (GDP).¹⁸ This represents a serious haemorrhaging of funds out of the country which could have been utilised towards its development.

Malawi is part of the global campaign to fight and stamp out the scourge of money laundering. This is evinced by the fact that Malawi is a party to several international instruments on money laundering and is also a member of a regional body involved in the fight against money laundering. Malawi is party to the Vienna and Palermo Conventions mentioned above, as well as the United Nations Convention against Corruption of 2003 (Merida Convention). Malawi is also a member of the Eastern and Southern Africa Anti-money Laundering Group (ESSAMLG). This is a grouping of states from the eastern and southern part of the African continent whose aim is to combat money laundering and terrorist financing, based on the standards set by the Financial Action Task Force (FATF) and other similar styled bodies.

In 2006, Malawi enacted the Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act of 2006. The long title of the Act states that it is "an Act to enable the unlawful

¹⁷ United Nations Economic Commission for Africa and the African Union Commission Report of the High Level Panel on Illicit Financial Flows from Africa, "Track it, Stop it and Get it: Illicit Financial Flows" (2015).

¹⁸ Report of the High Level Panel on Illicit Financial Flows from Africa (2015: 12).

proceeds of all serious crime and terrorist financing to be identified, traced, frozen, seized and eventually confiscated; to establish a Financial Intelligence Unit for the better prevention, investigation and prosecution of money laundering, terrorist financing and other financial and serious crimes; to require financial institutions to take prudential measures to help combat money laundering and terrorist financing; and to provide for matters connected with or incidental to the foregoing”.

1.3 The Concept of New Payment Methods

Criminals have a keen interest in keeping their ill-gotten gains. They utilise all sorts of techniques to give their ill-gotten gains an appearance of legality. In most cases they adopt sophisticated techniques which elude law enforcement authorities, hence they avoid detection. Convoluting money laundering schemes necessitate a legal regime that covers various aspects of money laundering and terrorist financing. The law needs to adapt easily to new risks and threats posed by rapid advancements in the sphere of technology, since research has shown that criminals are more likely to use technologically inspired innovations to conceal their ill-gotten gains.¹⁹ Such technological innovation can be found in the field of new payment methods. These include prepaid cards, Internet payment systems, mobile payments and digital precious metals.²⁰ These are perfectly legal methods used to



¹⁹ FATF Typologies Report on Money Laundering Using New Payment Methods (October 2006) FATF-GAFI: Paris, available at <http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html>, (Accessed on 12 March 2016).

²⁰ FATF Typologies Report on Money Laundering Using New Payment Methods (October 2006) FATF-GAFI: Paris, available at <http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html>, (Accessed on 12 March 2016).

pay for goods and services and also to transfer funds from one individual to another. The afore-mentioned payment systems represent a move from the traditional payment methods such as cash and regular bank payment transactions. The novelty of these new payments may attract criminals and criminal organisations to utilise them to launder money and finance terrorism because countries may not have the necessary legal regime to regulate them, or other countries may not have the capability and expertise to detect their use for criminal purposes. It is not always easy to identify new payment methods.²¹ It bears noting that there is a legitimate market demand served by each of the new payment methods, but they may also be used to launder money.²²

This paper will focus on mobile payments only because they are the most widely used medium for business transactions in Malawi. It will look at the potential use of mobile payments by criminals as a vehicle for money laundering and terrorist financing as compared to the AML/CFT regulatory regime currently obtaining in Malawi.



There are two types of mobile money payments. With the one, all that is required is a phone as an access device to initiate and authenticate transactions from existing bank accounts or payment cards. The other payment is not based on an underlying bank or

²¹ FATF Typologies Report on Money Laundering Using New Payment Methods (October 2006) FATF-GAFI: Paris, available at <http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html>, p5 (Accessed on 12 March 2016).

²²FATF Typologies Report on Money Laundering Using New Payment Methods (October 2006) FATF-GAFI: Paris, available at <http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html>, (Accessed on 12 March 2016).

payment card account, but on the services of the telecommunications operator who, typically, acts as a payment intermediary to authorise, clear and settle the payment.²³ The former is subject to the AML/CFT precautionary procedures of banks and is very easy to regulate because it is linked intrinsically to the general banking system, whereas the second one presents many ML/FT challenges because it is independent of the general banking system. For this reason this paper will focus on the second mobile money payment method.

In Malawi there are four mobile phone operator companies.²⁴ Of these four, only two, namely, Airtel Malawi and Telecom Networks Malawi (TNM), provide mobile money payment products. Airtel has a product called *Air Money* and TNM has a product called *Mpamba*. Both these products enable people to pay for goods and services and also to transfer funds from one individual to another. All that is required to register an account and a particular product is a national identity card or passport and a personal phone number. One may apply for registration only in respect of one account. The registration is done either through agents or at the operators' service centres.²⁵

²³FATF Typologies Report on Money Laundering Using New Payment Methods (October 2006) FATF-GAFI: Paris, available at <http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html>, p5 (Accessed on 12 March 2016).

²⁴ Airtel Malawi, Telecom Networks Malawi (TNM), Access Malawi and Malawi Telecommunications Limited.

²⁵ Airtel Money Terms and Conditions, available at http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/Malawi/Airtel_Money/Home/Personal/Terms-and-Conditions, (Accessed on 31st March, 2016). See also Mpamba Terms and Conditions, available at <http://www.tnm.co.mw/index.php/tnm-mpamba.html>, (Accessed on 31 March, 2016).

With these products, the two operators are offering a valuable service to the Malawian people, as only 27 per cent of the Malawian adult population is banked.²⁶ This means that 73 per cent of the adult Malawian population has no access to the formal banking system. The operators thus bring financial services to the multitude of unbanked adult Malawians. But, there are several challenges which may expose these wonderful products to the threat of being misused as vehicles of ML/TF.

To begin with, Malawi does not have a national identity card for its citizenry.²⁷ This makes it difficult to distinguish clearly who is a Malawian citizen and who is not. The situation is exacerbated by the fact that the majority of Malawians do not have birth certificates, or are not issued with them at birth, despite a clear legal provision that all births should be registered and that a birth certificate should be issued upon payment of a fee by the parents or guardians of the child.²⁸ The law is applied laxly, hence the difficulty in establishing who are and who not Malawian citizens. In addition, there is no automated central biographical data centre where information about Malawian citizens is stored. Most of the information about the public is kept manually and is very scanty. This practical imperfection has been exploited fully by illegal immigrants who have managed to pass themselves off as *bona fide* Malawians. Some have managed even to obtain Malawian passports.²⁹

²⁶ Mandiwa M 'Access to Financial Services in Malawi: Policies and Challenges', available at http://unctad.org/meetings/en/Presentation/ciem6_2014_Malawi_en.pdf_p6 (Accessed on 10 April 2016).

²⁷ Nkhoma G B 'Transnational Threats: The Problem of Illegal Immigration in Northern Malawi' *Southern African Peace and Security Studies* 1(2) (2012) 36.

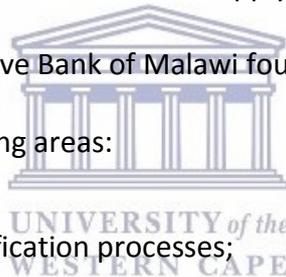
²⁸ Sections 3, 4 and 5 of the Births and Deaths Registration Act (Chapter 24:01 of the Laws of Malawi) provide for registration of a child's birth while section 16 of the same Act provides for the issuance of a birth certificate by the Registrar upon request and payment of the prescribed fee.

²⁹ Nkhoma G B (2012: 34).

The illegal immigrants are often involved in money laundering, illegal foreign exchange businesses, drug trafficking and smuggling.³⁰

The other challenge is that some of the products do not require paper work and almost all the products do not require the disclosure of the purpose of the funds being transferred.³¹ Furthermore, registration for these products is done mainly by agents, most of whom disregard that 'know your customer' (KYC) rule and the prerequisite customer due diligence (CDD) procedures that need to be complied with before entering into a financial transaction with a customer. These requirements are ignored for the sake of making a huge commission.

Another challenge is that most financial institutions apply only generic AML/CFT measures. In its 2014 annual report, the Reserve Bank of Malawi found that financial institutions were falling short seriously in the following areas:



- a) Customer identification and verification processes;
- b) Record keeping of client information;
- c) Ongoing monitoring of customer transactions;

³⁰ Nkhoma G B (2012: 36). See also FATF Mutual Evaluation Report on Malawi (2008), available at http://www.esaamlg.org/evaluationreports/Malawi_Report.pdf in which it was indicated that Malawi faces a big challenge in as far as production and trade of Indian hemp is concerned and that very little is known about the proceeds generated or laundered from this trade (Accessed on 16 April 2016).

³¹ Airtel Money Cross Boarder Transfer, available at http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/malawi/airtel_money/home/airtel-money-cross-border, (Accessed on 16 April 2016).

d) ML/TF risk assessment of customers, products and services, delivery methods and geographical locations.

The Central Bank also noted that financial institutions conduct limited and generic AML/CFT staff training that does not cover all legislative requirements and specialised business areas.³² This is very worrying, considering the fact that one of the mobile phone operators offers a mobile money payment product that allows for cross-border transfer of money from one individual to another.

It is in the light of the above-mentioned challenges that this research paper aims to assess the vulnerability of mobile money payment systems to abuse as vehicles of ML/TF in the Malawian context.

1.4 Theoretical Premise of the Study

The research paper aims to examine the degree to which the mobile money payment products offered by Malawian mobile service providers can be exploited by criminal enterprises as vehicles for money laundering and terrorist financing. It proceeds on the theoretical premise that criminals will use the perfectly legal mobile money payment products which serve a legitimate market demand in order to give legitimacy to the proceeds of their criminal activities. The author assumes that criminals will be attracted to these products because they are legal and are not regulated thoroughly by the authorities. It is also the author's assumption that the challenges of positive identification and other loopholes, such as anonymity, currently plaguing the mobile money payment products

³² Reserve Bank of Malawi 'Financial Institutions Supervision Annual Report (2014)', available at <https://www.rbm.mw/Supervision/BankSupervision/?activeTab=BASUDirectivesandGuidelines>, (Accessed on 16 April 2016).

which have been highlighted above will serve as an extra incentive to criminals to use them in order to integrate their ill-gotten gains into the formal economy. These are novel products whose susceptibility to misuse as vehicles for ML/TF has been brought to the attention of the authorities only through the research conducted by entities such as the FATF, ESAAMLG, the World Bank and the International Monetary Fund (IMF).

1.5 Research Question

The question which this research paper aims to address is whether or not the mobile money payment products offered by the Malawian mobile phone service providers to Malawians can be misused by criminals as vehicles for ML/TF when compared to the traditional AML/CFT regulatory regime currently operational in the country.

1.6 Research Methodology

This paper will be a desktop-based research project. It will make use of primary and secondary sources such as laws, supervisory directives, international instruments, cases, case studies, academic articles and books in a quest to find the answer to the research question. The paper will give a picture of the extent to which mobile money payments in Malawi are vulnerable to be exploited for ML/TF. Since money laundering is a global phenomenon, the paper will seek guidance from the approaches adopted by other jurisdictions in so far as mitigating the risk of mobile money payments being used as vehicles for money laundering is concerned.



1.7 Conclusion

The chapter is a cursory description of the flaws in the mobile money payment systems that have necessitated the need to conduct this study in order to establish the extent to which they can be exploited for ML/TF by criminal elements.



Chapter Two

The International Legal Framework on Combating Money Laundering Through Mobile

Money Payments

2.1 Introduction

Ever since money laundering was identified as a scourge posing a serious threat to the well-being of the global financial system, the global community has concentrated its efforts to devise a legal regime aimed at combating and mitigating the negative effects of money laundering. This chapter will discuss the international legal regime that has been developed to combat the use of mobile money payments as vehicles for money laundering. It will trace the origin of the global fight against the scourge of money laundering to the present, highlighting specific legal instruments that address the use of mobile money payments as vehicles for money laundering. The first part of the chapter will discuss the money laundering legal regime put in place through the efforts of the United Nations (UN). There are three money laundering international legal instruments which came into existence because of the concerted efforts of the UN. These are the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (the Vienna Convention), the UN Convention against Transnational Organised Crime of 2000 (the Palermo Convention), and the UN Convention against Corruption of 2003 (the Merida Convention).

After discussing the UN legal instruments, this chapter will move on to examine and discuss the initiatives of the European Union (EU) in the fight against money laundering in general and in so far as they relate to mobile money payments in particular. These include the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds

from Crime (CoE Convention of 1990), and the first, second, third and fourth Council Directives on Prevention of the Use of the Financial System for the Purpose of Money Laundering.

The last part of the chapter will look at the standards and guidelines propounded by the FATF. The focus will fall on the specific FATF Recommendations which address the intersection between money laundering and mobile money payments.

2.2 The United Nations Anti-Money Laundering Legal Instruments

The UN is a major player in the global fight against the phenomenon of money laundering. To date, it has adopted three conventions dealing with the crime of money laundering. These conventions, in the order of their adoption, are the Vienna Convention (1988), the Palermo Convention (2000) and the Merida Convention (2003).

2.2.1 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (The Vienna Convention, 1988)



This Convention was the first international legal instrument to address the problem of money laundering. However, it is limited in its scope of application because it deals only with drug-related money laundering and not any other serious offences.³³

The Convention places an obligation on states parties to see to it that they 'criminalise drug-related money laundering with the scope of criminalisation covering a comprehensive list

³³ Article 3(1)(b) of the Vienna Convention.

connected to drug trafficking; from production, cultivation and possession to the organisation, management and financing of trafficking operations'.³⁴

The Convention also obligates states parties to adopt laws in their domestic legislation which empower competent authorities to confiscate and seize proceeds from drug-related crimes and tainted property.³⁵

In addition, the Vienna Convention encourages states parties to co-operate in the fight against money laundering. This encouragement of co-operation is two-fold. Firstly, states parties are called upon to enter into bilateral and multilateral treaties, agreements or arrangements in order to enhance the efficacy of international co-operation.³⁶ Secondly, the Convention obligates states parties to accord each other mutual legal assistance (MLA) in order to smoothen and expedite the investigation and prosecution of money laundering offences and also seizure and confiscation proceedings.³⁷



One of the outstanding features of the Vienna Convention which has enhanced the fight against money laundering, is the obligation on states to enact legislation which empowers courts to override bank secrecy laws.³⁸ This has enabled law enforcement agencies to carry out their investigations without obstacles.

³⁴ Stewart D P 'Internationalising the War on Drugs: The UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances' *Denver Journal of Law and Policies* (1990) 387.

³⁵ Article 5 of the Vienna Convention.

³⁶ Article 5(4) (g) of the Vienna Convention.

³⁷ Article 7 of the Vienna Convention.

³⁸ Article 5(3) of the Vienna Convention.

2.2.2 UN Convention against Transnational Organised Crime (The Palermo Convention, 2000)

The Palermo Convention was adopted by the UN General Assembly, by way of resolution A/RES/55/25 of 15 November 2000 and came into force on 11 November 2003.³⁹ This Convention is of great significance because it is the first legally binding UN instrument dealing with transnational organised crime and other serious crimes.⁴⁰ Unlike the Vienna Convention which limited predicate offences to drug-related crimes, the Palermo Convention broadened the range of predicate offences for money laundering. It extended them beyond drug-related offences to other serious offences.⁴¹ States parties to the Convention are under an obligation to extend the criminalisation of money laundering to other predicate offences such as participation in organised crime, corruption and obstruction of justice.⁴²



The Palermo Convention provides also for identification, tracing, freezing, seizure and confiscation of proceeds of crime.⁴³

The Palermo Convention, too, contains some provisions which are very relevant to the focus topic of this paper. These provisions call for the regulation of banks, non-financial institutions, and where appropriate, other bodies which are deemed to be particularly predisposed to money laundering.⁴⁴ These provisions apply to mobile money payments by extension. By their nature, the latter do not fall within the ambit of the traditional financial

³⁹ UN website www.un.org/en/documents/ (Accessed on 23 August 2016).

⁴⁰ Hopton D *Money Laundering: A Concise Guide for all Businesses* (2009) (2 ed) 10.

⁴¹ Hopton (2009: 10). See also Article 6 of the Palermo Convention.

⁴² Article 6(1) (a) and (b) of the Palermo Convention.

⁴³ Article 12 of the Palermo Convention.

⁴⁴ Article 7(1)(a) of the Palermo Convention.

system. As such, they can fall under the category of non-financial institutions or bodies particularly susceptible to money laundering. The traditional financial institutions, especially banks, have been heavily regulated ever since the global fight against money laundering began. Consequently, criminals have had to find new ways to launder their ill-gotten gains. One such avenue is through mobile money payments. Although article 7(1)(a) does not specifically mention mobile money, it is clear, as demonstrated above, that it covers such payments.

2.2.3 UN Convention against Corruption (The Merida Convention, 2003)

The Merida Convention is the only legally binding anti-corruption instrument whose scope of application is global.⁴⁵ It is the most comprehensive anti-corruption legal instrument.⁴⁶

Despite being dedicated substantially to the fight against corruption, the Merida Convention deals also with the issue of money laundering. Of significance to this paper is article 14 of the Convention. The article calls upon states parties to formulate a comprehensive regulatory and supervisory regime capable of deterring and detecting all forms of money laundering.⁴⁷ The subjects to be regulated and supervised by this comprehensive regime include banks, non-financial institutions, legal and non-legal persons that provide formal or informal services for transmission of money or value, and other bodies susceptible to money laundering.⁴⁸ The methods to be employed to deter and detect money laundering include



⁴⁵ Babu R R 'The United Nations Convention against Corruption: A Critical Overview' 6, available at <http://ssrn.co/abstract=891898> (accessed on 11th September 2016).

⁴⁶ Carr I and Goldby M 'The UN Anti-Corruption Convention and Money Laundering Working Paper', available at <http://ssrn.com/abstract=1409628> (accessed on 11 September 2016).

⁴⁷ Article 14(1)(a) of the Merida Convention.

⁴⁸ Article 14(1)(a) of the Merida Convention.

identification of beneficial owners, record keeping and reporting of suspicious transactions.⁴⁹

Article 14 also requires states parties, where possible, to require financial institutions, including money remitters, to demand information on the origin of funds and persons involved in electronic funds transfer transactions. This information must be meaningful and accurate, and must be maintained throughout the payment chain.⁵⁰ If an electronic funds transfer transaction lacks the two preceding preconditions then it should be subjected to close scrutiny by the financial institution or money remitters.⁵¹

As pointed out above, article 14 has a close bearing on the issue of mobile money payments. It calls on states parties to design a regulatory and supervisory regime to deter and detect all forms of money laundering, not only in relation to banks but also in relation to other non-financial institutions, including those engaged in formal and informal transmission of money or value. Thus, mobile money payments service providers are included because they are involved in the transfer of money or value. To remove doubt, the comprehensive regime has been extended to any other bodies susceptible to money laundering. Mobile money payments service providers can also be slotted under this category. Article 14 also makes a specific reference to electronic funds transfers, of which mobile money payments are part. It emphasises the need to have information on the origin of funds and the need for application of close scrutiny to transactions which are devoid of adequate originator information. All this regulation could go a long way in detecting money laundering and

⁴⁹ Article 14(1)(a) of the Merida Convention.

⁵⁰ Article 14(3) (a) and (b) of the Merida Convention.

⁵¹ Article 14(3)(c) of the Merida Convention.

preventing mobile money payments from being utilised as vehicles for money laundering if effectively implemented.

2.3 European Union Conventions and Directives on Money Laundering

As part of the global fight on money laundering and terrorist financing, the European Union has adopted several legal instruments which are binding on its member states. These instruments include the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the four European Union Directives on the Prevention of the use of Financial Systems for the Purpose of Money Laundering. The fourth Directive was adopted recently in 2015.

2.3.1 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (CoE Convention, 1990)

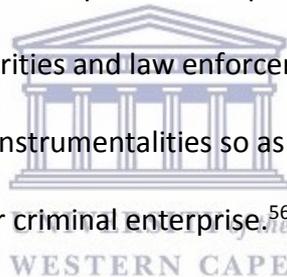
The purpose of the adoption of this particular Convention is very clear from the wording of its preamble. The aim was to provide for a uniform legal regime amongst member states of the EU in their collective efforts to fight and combat money laundering. Part of the preamble asserts that the Convention was adopted with the aim of achieving a greater unity among members of the EU by pursuing a common 'criminal policy aimed at the protection of society'.⁵²

⁵² Paragraphs 2 and 3 of the Preamble to the CoE Convention

These sentiments are shared by Mugarura who writes that the aim of adopting the Convention was to synchronize anti-money laundering practices and policies within the EU.⁵³

Apart from harmonising the anti-money laundering legal regime within the member states of the EU, the CoE Convention also stresses the need for international co-operation in the fight against money laundering.⁵⁴ This theme is reiterated in articles 7 and 8 of the CoE Convention. These articles call upon member states to accord each other co-operation to the widest extent possible during investigations, tracing and confiscation of proceeds, instrumentalities and other property which has been found to be liable for confiscation.⁵⁵

Articles 2 and 3 of the CoE Convention requires states parties to adopt laws and measures which will enable competent authorities and law enforcement agencies to identify and confiscate proceeds of crimes and instrumentalities so as to make it easier to deny criminals enjoying the fruits of their criminal enterprise.⁵⁶



In addition, the CoE Convention criminalises various money laundering offences.

⁵³ Mugarura *The Global Anti-Money Laundering Regulatory Landscape in Less Developed Countries* (2012) 71.

⁵⁴ Paragraphs 3 and 4 of the Preamble to the CoE Convention.

⁵⁵ Articles 7 and 8 of the CoE Convention.

⁵⁶ Articles 2 and 3 of the CoE Convention.

2.3.2 First EU Directive on Money Laundering: Council Directive 91/308 ECC on Prevention of the Use of the Financial System for the Purpose of Money Laundering

This is the first of a series of Directives issued by the CoE on combating money laundering. It was adopted in 1991.⁵⁷ This Directive asserted that combating money laundering using penal sanctions alone, as advocated by the Vienna Convention and the CoE Convention, was not enough. It championed the view that penal sanctions should not be the only tool in the quest to fight and prevent money laundering.⁵⁸

Under this First Directive, states parties were obligated to adopt measures that reflect the international character of money laundering for them to be effective in the fight against it.

Moreover, it was recognised under this Directive that money laundering is not confined to being perpetrated only within credit and financial institutions such as banks, but can also take place through other avenues, including some other professions. States parties were thus called upon to extend measures aimed at combating and preventing money laundering to such professions and categories of undertakings that are susceptible to being used for money laundering purposes.⁵⁹ Arguably, this includes mobile money payments since they are a system which is prone to abuse for money laundering by criminals. The mobile payment system is attractive to criminals since most states have not considered it to be seriously vulnerable to money laundering.



⁵⁷ Ionescu L 'Money Laundering Directives and Corruption in the European Union', *Contemporary Readings in Law and Social Justice* Volume 4(2)(2012)562.

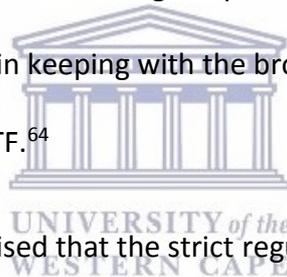
⁵⁸ Paragraphs 8 and 9 of the Preamble to the First EU Directive on Money Laundering. See also Article 12 of the First Directive.

⁵⁹ Paragraph 22 of the Preamble to the First EU Directive on Money Laundering.

2.3.3 Second EU Directive on Money Laundering: Directive 2001/97 EC of the European Parliament and of the Council of 4 December 2001 Amending Council Directive 91/308 ECC on the Prevention of the Use of the Financial System for the Purpose of Money Laundering.

The second Directive was adopted in 2001 and was aimed at amending the first Directive.⁶⁰ It introduced significant changes in two critical aspects of the fight against money laundering. Firstly, it extended the application of the Directive to all non-financial activities and professions, such as lawyers and notaries.⁶¹ The application of the Directive was also extended to cover currency exchanges, money remittance offices⁶² and investment firms.⁶³

Secondly, the second Directive extends the range of predicate offences from drug-trafficking to include all other serious crimes, in keeping with the broader definition of money laundering as advocated by the FATF.⁶⁴



Lastly, the Second Directive recognised that the strict regulation of the formal financial system had made it difficult for potential money launderers to abuse it for their nefarious schemes. This led economic criminals to devise other avenues to launder the proceeds of their criminal enterprises. The Directive, therefore, called upon states parties to extend the obligations imposed by the Directive, such as customer identification and record keeping, to those activities and professions that are particularly vulnerable to money laundering.⁶⁵ For the purposes of this paper, it is arguable that activities that are particularly prone to money

⁶⁰ Ionescu L (2012: 562).

⁶¹ Ionescu L (2012: 562).

⁶² Ionescu L (2012: 562).

⁶³ Paragraph 5 of the Preamble to the Second EU Directive on Money Laundering.

⁶⁴ Paragraphs 8 and 9 of the Preamble to the Second EU Directive. See also Ionescu L (2012: 562).

⁶⁵ Paragraphs 14 and 15 of the Preamble to the Second EU Directive.

laundering include mobile money payments, since they represent a system that can be easily abused by criminals for money laundering purposes, given that it is not properly regulated by the relevant authorities. That mobile money payments are prone to be abused for money laundering purposes is supported by the FATF's typology on New Payment Methods.⁶⁶

2.3.4 Third EU Directive on Money laundering: Council Directive 2005/60/EC on the Prevention of the Use of the financial System for the Purposes of Money Laundering and Terrorist Financing.

This Directive was adopted on the 26 October 2005.⁶⁷ Its aim was to make the EU's anti-money laundering regime dovetail with international anti-money laundering practices. This was necessitated by the review of the FATF standards which took place in 2003.⁶⁸

A need thus arose to make the obligations under the Directive to reflect the changes made by the 2003 review of the FATF standards.⁶⁹



The third Directive represents a major paradigm shift in the global fight to preserve the integrity of the financial system in that it extended its obligations to the fight against terrorist financing. This is reflected in paragraph 8 of the preamble to the Directive which states firmly that the previous obligations it imposed should be extended to cover the collection of money or property used for terrorist purposes. The reason was that the misuse of the financial system as a conduit for the transfer of criminal or clean money for terrorist purposes is detrimental to the integrity, the proper functioning, and the reputation of the

⁶⁶ New Payment Methods, available at www.fatf-gafi.org/ (Accessed on 20 September 2016).

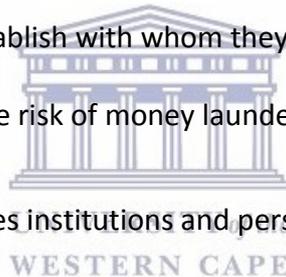
⁶⁷ Ionescu L (2012: 563).

⁶⁸ Paragraph 5 of the Preamble to the Third EU Directive on Money Laundering. See also Ionescu L (2012: 563).

⁶⁹ Paragraph 5 of the Preamble to the Third EU Directive on Money Laundering.

financial system.⁷⁰ This is a relevant factor to this study because clean or criminal money can be transferred through the financial system for terrorist purposes using mobile money payments.

In addition, this Directive provides for the need to have thorough and effective ways of conducting customer identification procedures which, as the Directive identified, are a crucial aspect in the fight against money laundering and terrorist financing.⁷¹ This encompasses the identification of beneficial owners⁷² which, according to Article 3(6) of the Directive, include corporate entities.⁷³ In the light of the fact that registered companies are able to utilise mobile money payments to make payments or send and receive money in Malawi, this Directive is of great guidance to what mobile money payments service providers should do in order to establish with whom they are doing business. Knowledge of their customers would minimise the risk of money laundering and terrorist financing.



Furthermore, this Directive obligates institutions and persons covered by it to focus their efforts on combating money laundering and terrorist financing where the risk is great. This is called the risk-based approach.⁷⁴

⁷⁰ Paragraph 8 of the Preamble to the Third EU Directive on Money Laundering.

⁷¹ Paragraphs 9 and 10 of the Preamble to the Third EU Directive on Money Laundering.

⁷² Paragraphs 9 and 10 of the Preamble to the Third EU Directive on Money Laundering.

⁷³ Article 3(6) of the Third EU Directive on Money Laundering.

⁷⁴ Paragraph 22 of the Third EU Directive on Money Laundering.

2.3.5 The Fourth EU Directive on Money Laundering: Council Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, And Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

This fourth Directive was adopted in May 2015. It recognised the susceptibility of financial technological innovations to exploitation by criminals for money laundering, terrorist financing and proliferation purposes.⁷⁵ It thus obligates states parties to draft legislation that tackles the danger of technological innovations being misused by money launderers to destabilise the financial system. It calls upon competent authorities to be proactive in combating new and innovative ways of money laundering.⁷⁶



In addition, this Directive acknowledges the substantial increase in the use of electronic money products by consumers as substitutes for bank accounts.⁷⁷ It goes on to state that this justifies subjecting these products to anti-money laundering and anti-financing of terrorism measures.⁷⁸ However, the Directive goes on to state that where there is low risk of money laundering or terrorist financing, such products should be exempt from strict AML/CFT obligations. Such exemptions would include situations where the products are utilised solely for purchasing goods and services.⁷⁹

⁷⁵ Paragraph 19 of the Preamble to the Fourth EU Directive on Money Laundering.

⁷⁶ Paragraph 19 of the Preamble to the Fourth EU Directive on Money Laundering.

⁷⁷ Paragraph 7 of the Preamble to the Fourth EU Directive on Money Laundering.

⁷⁸ Paragraph 7 of the Preamble to the Fourth EU Directive on Money Laundering.

⁷⁹ Paragraph 7 of the Preamble to the Fourth EU Directive on Money Laundering.

2.4 The FATF International Standards for Combating of Money Laundering and the Financing of Terrorism and Proliferation of Weapons of Mass Destruction

The FATF is an inter-governmental body set up by members of the G8 to develop standards to be used in the global fight against money laundering.⁸⁰ The first FATF standards were issued in 1990.⁸¹ Then, the standards addressed only the issue of money laundering and not terrorist financing. The standards have since been reviewed four times,⁸² first in 1996, and the second time in 2001. This latter review was necessitated by the terrorist attack of the Twin Towers of the World Trade Centre on 11 September 2001.⁸³ This review added 9 more recommendations to the FATF standards, addressing the issue of terrorism and terrorist financing. The standards came to be known as the 40+9 Recommendations.⁸⁴ The next review of the FATF standards took place in 2003.⁸⁵ The last review occurred in 2012. In this review the Recommendations were amalgamated into one set of standards. They are no longer called the 40+9 Recommendations. Currently there are just 40 Recommendations. In addition, the issue of the proliferation of weapons of mass destruction was addressed. The standards are now called the FATF international standards on money laundering, terrorist financing and proliferation of weapons of mass destruction.⁸⁶

The FATF standards provide a blueprint of the global legal regime in the fight against money laundering and terrorist financing. They are acknowledged as the global anti-money

⁸⁰ FATF website, available at www.fatf-gafi.org/about/ (Accessed on 23 August 2016).

⁸¹ FATF website.

⁸² FATF website.

⁸³ Gill M and Taylor G 'Preventing Money laundering or Obstructing Business?' *British Journal of Criminology* (2004) 584.

⁸⁴ Gill M and Taylor G (2004).

⁸⁵ FATF website.

⁸⁶ FATF Standards.

laundering and counter-terrorist financing standard.⁸⁷ Almost all international instruments on the subject are modeled on the FATF standards. For example, all the Directives issued by the EU on money laundering have been adopted in order to be in conformity with the FATF standards. The First EU Directive on money laundering was adopted in order for the EU legal regime on money laundering to conform to the first set of FATF standards which were issued in 1990.⁸⁸ Subsequent EU Directives on money laundering have been issued and adopted in order to conform to the FATF standards as they have been reviewed from time to time over the years.

As they currently stand, the FATF standards provide guidance to supervisory, regulatory and law enforcement agencies of states around the world on key issues to be addressed in the global fight against money laundering, terrorist financing and proliferation of weapons of mass destruction.



Firstly, the standards call upon countries to tackle money laundering on a risk-based approach. This is based on the fact that not all risks in the financial system are the same. Therefore, states and responsible institutions should allocate the most resources only to situations and products that present the highest risk of money laundering and terrorist financing.⁸⁹

Secondly, the standards specifically tackle the issues of terrorism, terrorist financing and non-proliferation in Recommendations 5, 6, 7 and 8. Recommendation 5 calls upon countries to criminalise terrorist financing in line with their obligations under the Terrorist Financing Convention. Recommendation 6 implores countries to impose targeted financial

⁸⁷ FATF website.

⁸⁸ Paragraph 11 of the Preamble to the First EU Directive on Money Laundering.

⁸⁹ Recommendation 1.

sanctions which comply with the contents of United Nations Security Council resolutions which address the issues of prevention and suppression of terrorism and terrorist financing. Recommendation 7 calls upon countries to consider implementing targeted financial sanctions to comply with UN resolutions on the prevention and suppression of proliferation of weapons of mass destruction, and Recommendation 8 asks countries to enact laws that prevent charitable organizations that being abused for terrorist financing purposes and to review the adequacy of such laws.

Thirdly, the standards call upon states and players in the financial system to identify people with whom they do business, both at the inception and during the subsistence of the business relationship.⁹⁰ This helps to identify possible occurrences of money laundering. The customer information has to be verified independently by the financial institutions in order to ensure its credibility.⁹¹ The records of transactions between financial service providers and their clients have to be kept for a period of 5 years.⁹²



In addition, financial institutions and other professionals and service providers which are susceptible to money laundering and terrorist financing threats are required to report to competent authorities all suspicious transactions and transactions that exceed maximum thresholds.⁹³

⁹⁰ Recommendation 10 of the FATF Standards.

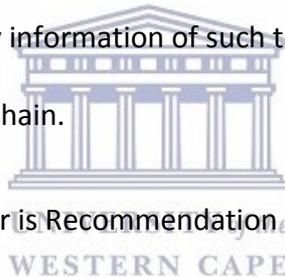
⁹¹ Recommendation 10.

⁹² Recommendation 11.

⁹³ Recommendation 20.

Furthermore, when a suspicious transaction is filed with the Financial Intelligence Unit in respect of a customer, it is prohibited to warn him or her that the transaction has been reported to the FIU. This is called the rule against tipping-off.⁹⁴

The fourth EU Directive addresses also issues bearing on the electronic transfer of money and innovative ways of transferring money or value. Recommendation 14 addresses the issue of money or value transfer services. It calls upon countries to ensure the registration and licensing of natural or legal persons that provide these services. Countries are also called upon to subject money or value transfer service to effective monitoring systems and ensure that they follow the FATF Recommendations to the letter. Recommendation 16 provides for the regulation of wire transfers. It suggests that all relevant information including originator and beneficiary information of such transfers should be required and be retained throughout the payment chain.



Of particular relevance to this paper is Recommendation 15, which calls upon countries and financial institutions to ‘identify and assess the money laundering and financing of terrorism risks’ associated with new products, new delivery mechanisms, new business practices and new technologies. This includes mobile money payments. They represent a new financial product which utilizes new technological mechanisms. Both these traits make them attractive to criminals for money laundering and terrorist financing purposes. Thus, all the obligations that have been imposed on other actors in the financial system have to apply also to mobile money payments service providers.

⁹⁴ Recommendation 21.

Apart from setting the standards on money laundering and terrorist financing, the FATF also conducts research studies to identify new ways in which money is being laundered. These are called money laundering typologies. In 2006, the FATF conducted a typology on the susceptibility of new payment methods to money laundering.⁹⁵ This typology report was followed by the 2010 report called *Money Laundering Using New Payment Methods* (NPMs). It analysed three types of NPMs. These are prepaid cards, Internet payment services and mobile payment services. This follow-up typology report was necessitated by the growing use of NPMs and an increased awareness of associated money laundering and terrorist financing risks.⁹⁶

Of particular relevance to this paper are the mobile payment services.

2.5 Conclusion



As can be seen from the discussion above, the global legal regime aimed at combating money laundering, terrorist financing and proliferation of weapons of mass destruction has evolved rapidly over the years. At the inception of this global fight, the focus was on combating the laundering of the proceeds of the drug-trafficking trade. This is exemplified by the provisions of the 1988 Vienna Convention. Later, the authorities realised that there were proceeds from other criminal activities which were being laundered using the global financial system. Hence, a need arose to expand the predicate offences for money laundering. Thus, all serious offences were included in the list of predicate offences for the crime of money laundering.

⁹⁵ FATF typology on Money Laundering Using New Payment Methods, (October, 2010).

⁹⁶ Executive Summary (2010).

The attacks on the Twin Towers of the World Trade Centre and the Pentagon in September 2011 alerted world authorities to the need to monitor the financial system so as to prevent and combat terrorist financing. The fight against money laundering and terrorist financing thus became one. Later, this would be extended to the fight against proliferation of weapons of mass destruction.

The global financial system has become so heavily regulated that it has become risky for criminal elements to use it for money laundering, terrorist financing and proliferation without detection by regulatory, supervisory and law enforcement agencies. This has forced criminals to look to other means of laundering the proceeds their crimes, financing terrorism and sponsoring the proliferation of weapons of mass destruction. One such new medium which has the potential of affording criminals an opportunity to achieve the above without strict scrutiny is mobile money payments. This was unearthed by the FATF's 2006 and 2010 typology reports on NPMs.



The FATF standards have addressed the vulnerability of NPMs to money laundering, terrorist financing and proliferation of weapons of mass destruction by way of Recommendations 14, 15 and 16. The FATF provides merely a guide on the measures to be implemented, and it is up to individual countries to decide exactly how they are going to implement such recommendations.

The next chapter will look at how the mobile money payments are regulated under Malawian law. It will compare also how they are regulated in other jurisdictions such as Kenya. It will also discuss and pinpoint the vulnerability of these products to misuse for money laundering, terrorist financing and proliferation of weapons of mass destruction.

Chapter Three

The Legal Regime Regulating Mobile Money Payments in Malawi

3.1 Introduction

This chapter will discuss the various pieces of legislation which regulate mobile money payments and the AML/CFT laws that touch on mobile money payments in Malawi.

Furthermore, it will discuss the relevant authorities that have been tasked with the job of supervising and regulating mobile money payments and the role each plays. The chapter will consider also the vulnerability of mobile money payments to money laundering and terrorist financing due to the enforcement deficit and gaps in the AML/CFT with regard to mobile money payments. The chapter will compare how mobile money payments services in other jurisdictions, for example Kenya, are regulated and how the responsible authorities in those jurisdictions have handled the threat of such services being utilised for money laundering and terrorist financing purposes. In addition the chapter will engage the need to strike a balance between the regulation of mobile money payments to reduce their susceptibility to money laundering and financial inclusion of the masses who are underserved by the formal financial system. Lastly, the chapter will examine the extent to which the responsible authorities responsible for supervising and regulating mobile money payments adhere to international AML/CFT standards in the execution of their functions.

As discussed above, Malawi was affected by a financial scam in 2013, which led to the loss of 13 Billion Kwacha from the state coffers. Since then, several people have been convicted of laundering the proceeds emanating from that scam. This means that Malawian courts have dealt only with money laundering cases involving the proceeds of corruption and

public theft laundered through the formal financial system. They have not dealt with a case of proceeds laundered through mobile money payments. Be that as it may, it does not eliminate the fact that mobile money payments can be abused by criminals to launder money. As of 2014-15, it was estimated that 10 per cent of Malawian mobile phone subscribers were registered customers of mobile money accounts.⁹⁷ This percentage translated into 0.4-0.5 million mobile money account holders, an estimated figure which was projected to grow considerably owing to the partnerships which the mobile money payments service providers were forging with banks and micro finance institutions (MFI).⁹⁸ The potential of mobile money presenting a lucrative opportunity to criminals to launder the proceeds of their criminal enterprises is addressed below.

3.2 Laws and Institutions Regulating Mobile Money Payments in Malawi

There are several pieces of legislation that have a bearing on the functioning of mobile money payments in Malawi. These include the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act (Money Laundering Act, 2006)⁹⁹ and the regulations made pursuant to that Act (AML Regulations, 2011),¹⁰⁰ the Reserve Bank of Malawi Act,¹⁰¹ the Mobile Money Guidelines issued by RBM pursuant to section 4(e) of the RBM Act, the Financial Services Act¹⁰² and the Communications Act.

In addition to the above-mentioned enactments, there are several authorities that provide supervisory and regulatory services for mobile money payments in Malawi. These include

⁹⁷ Buckley R, Greenacre J and Malady L 'The Regulation of Mobile Money in Malawi' *Washington University Global Studies Law Review* 14(3) (2015) 451.

⁹⁸ Buckley *et al* (2015: 450).

⁹⁹ Chapter 8:07 of the Laws of Malawi.

¹⁰⁰ Money Laundering, Proceeds of Serious Crime and Terrorist Financing Regulations, 2011.

¹⁰¹ Chapter 44:02 of the Laws of Malawi.

¹⁰² Act No. 26 of 2010 of the Laws of Malawi.

the Malawi Communications Regulatory Authority (MACRA), the Reserve Bank of Malawi (RBM) and the Financial Intelligence Unit (FIU). The RBM is the primary regulator of mobile money payments in Malawi.¹⁰³

3.2.1 The Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act and the Regulations Pursuant to that Act

This Act is the main law dealing with anti-money laundering and the combating of the financing of terrorism. Part of the objectives of this Act is obligate financial institutions to adopt measures aimed at combating money laundering and terrorist financing.¹⁰⁴ The obligations under this Act apply also to mobile money payments since they are included in the definition of financial institutions covered by the Act. Mobile money payments are defined as financial transactions under the category of money transmission services.¹⁰⁵

Arguably, they are also covered under the category of institutions issuing and administering means of payment.¹⁰⁶



The Act replicates the key FATF Recommendations on anti-money laundering and counter-financing of terrorism. Firstly, the Act obligates financial institutions, including mobile money payments service providers, to ascertain and verify independently the identity of the customers with whom they enter into a business relationship, conduct a transaction or suspect of engaging in money laundering. The identification need not only be done prior to the inception of the business relationship, but also during the relationship.¹⁰⁷ This requirement enables financial institutions to know exactly the type of person, legal or

¹⁰³ Buckley *et al* (2015: 451).

¹⁰⁴ Long title of the Money Laundering Act.

¹⁰⁵ Section 2 of the Money Laundering Act.

¹⁰⁶ Section 2 of the Money Laundering Act.

¹⁰⁷ Section 24(1) of the Money Laundering Act.

natural, with whom they are entering into a business relationship so as to be able to determine whether or not such person poses a money laundering or terrorist financing risk.

Secondly, financial institutions are obligated to report to the FIU and not to proceed with processing an attempted transaction where insufficient evidence has been adduced to establish a satisfactory identification of a customer.¹⁰⁸ Failure to comply with this requirement results in the commission of an offence under the Act, the punishment of which is two years' imprisonment and a fine of K100, 000 in the case of a natural person and a K500,000 fine and loss of a business licence in the case of a company.¹⁰⁹

The Act also requires financial institutions to maintain accounts in the clients' true names.¹¹⁰

Thus, they are prohibited from establishing and maintaining anonymous accounts or accounts in the fictitious names of their clients.

In addition, the Act compels financial institutions to establish and maintain customer records which should include such information as the customer's identity, transactions conducted and their accompanying correspondence, as well as enquiries made to the FIU relating to suspicious transactions and money laundering and terrorist financing in respect of such customer.¹¹¹ This helps financial institutions to construct a customer profile for their clients which is not only helpful in assessing the ML/TF risk of a client, but which assists law enforcement authorities as an evidentiary source should the need to investigate and prosecute arise.

¹⁰⁸ Section 25(2) of the Money Laundering Act.

¹⁰⁹ Section 25(2) of the Money Laundering Act.

¹¹⁰ Section 26 of the Money Laundering Act.

¹¹¹ Section 27 of the Money Laundering Act.

Section 28 of the Money Laundering Act imposes perhaps one of the most crucial obligations in the fight against money laundering and terrorist financing on financial institutions. It obligates them to report suspicious transactions to the FIU whenever they suspect that a transaction exceeds the designated threshold or suspect that it involves the commission of a money laundering offence. This enables the FIU to analyse such transactions, and if they establish any irregularity, transmit such intelligence to law enforcement or supervisory authorities for investigation or prosecution.¹¹² Whenever a suspicious transaction report (STR) is filed with the FIU by a financial institution, such institution or its personnel are prohibited from notifying the person against whom an STR has been filed that it has been filed.¹¹³ Contravention of this obligation is an offence under the Act.



Moreover, the Act requires financial institutions to establish and maintain internal reporting procedures. These include employing a compliance officer, setting up mechanisms for conducting CDD and KYC requirements, keeping and retaining transaction records, reporting STRs and acquainting employees with AML/CFT laws and regulations.¹¹⁴

The Act requires financial institutions and money transmission service providers to record also originator information and other related messages on all electronic funds transfers.¹¹⁵

This helps in establishing the true identity of the person initiating the transaction and its purpose.

¹¹² Section 11(2) of the Money Laundering Act. The FIU is established under section 11(1) of the Money Laundering Act and is 'responsible for receiving, requesting, analysing and disseminating to competent authorities disclosures of financial information as required under this Act, in order to counter money laundering and financing of terrorism'.

¹¹³ Section 30 of the Money Laundering Act.

¹¹⁴ Section 32 of the Money Laundering Act.

¹¹⁵ Section 33 of the Money Laundering Act.

Lastly, the Act empowers the FIU to obtain court orders to enforce financial institutions' compliance with obligations imposed under sections 24, 25, 26, 27 and 28 whenever it is of the view that the obligations have been breached.¹¹⁶ Such court orders are crucial as they are an effective manner of ensuring that the AML/CFT obligations are enforced.

Most of the obligations imposed by the Money Laundering Act are replicated in the AML Regulations of 2011 except that the Regulations provide specific details and clarification on how financial institutions should go about implementing the obligations punctiliously.¹¹⁷

3.2.2 The Reserve Bank of Malawi Act (RBM Act)

The Reserve Bank of Malawi is the central bank of the land tasked with the function of regulating commercial banks and overseeing the financial and monetary policies of Malawi.¹¹⁸ It is established under section 3 the RBM Act.

The RBM is one of the main actors in the regulation of mobile money payments in Malawi. It is obligated to promote excellent co-operation with banks and other financial institutions in order to guarantee high standards of conduct in the financial system and the proper implementation of policies of national interest.¹¹⁹ Its mandate is to ensure that financial institutions such as mobile money payments service providers offer their services with the highest standards of financial integrity so as to safeguard the financial system, and in the spirit of the national interest, to make sure that their products are not used for money laundering and terrorist financing. In trying to fulfil this mandate, the RBM has led efforts to

¹¹⁶ Section 43 of the Money Laundering Act.

¹¹⁷ ESAAMLG '4th Progress Report on Anti-Money Laundering and Combating the Financing of Terrorism Republic of Malawi' 20, available at www.esaamlg.org, (Accessed on 20 December 2016).

¹¹⁸ Section 4 of the RBM Act.

¹¹⁹ Section 47(b) and (c) of the RBM Act.

bring together participants and regulators in the mobile money payments service industry under the banner of the Mobile Money Consultative Group (MMCG).¹²⁰

In addition, the RBM is tasked with the obligation to supervise banks and other financial institutions. Thus, it has to make sure that they are solvent and act in accordance with monetary regulations under the RBM Act.¹²¹ The MMCG is comprised of the two Mobile Network Operators in Malawi, donors, regulators and banks, and its main objective is to fortify the use of mobile money payments in Malawi by heeding the recommendations and concerns of all the stakeholders involved in the provision of mobile money payments services.¹²²

The RBM has signed a memorandum of understanding with two other regulatory bodies, namely, MACRA and the FIU, in order to create a secure and favourable operating environment for mobile money payments service providers in Malawi.¹²³



Furthermore, the RBM's mandate to supervise and regulate mobile money payments is derived from section 4(e) of the RBM Act.¹²⁴ This section empowers the RBM to promote and manage payment systems in Malawi.¹²⁵ Pursuant to section 4(e), the RBM issued the Guidelines for Mobile Payment Systems (Mobile Guidelines) to regulate mobile money payments in Malawi. They were issued in March 2011. According to Buckley *et al*, these Guidelines represent the dominant regulator of mobile money payments in Malawi.¹²⁶

¹²⁰ Buckley *et al* (2015: 453).

¹²¹ Section 48(1) of the RBM Act.

¹²² Buckley *et al* (2015: 454).

¹²³ Buckley *et al* (2015: 455).

¹²⁴ Buckley *et al* (2015: 452).

¹²⁵ Buckley *et al* (2015: 452).

¹²⁶ Buckley *et al* (2015: 457).

3.2.3 Guidelines for Mobile Payment Systems

The Mobile Guidelines define a Mobile Network Provider as ‘a mobile phone company licensed by the Malawi Communications Regulatory Authority or any other body with authority in Malawi’.¹²⁷ They define a Mobile Financial Payment Service Provider as ‘a company that is authorised to provide services that enable the process of money transfer and exchange of money for goods and services between two parties using a mobile phone’.¹²⁸ The Mobile Guidelines were issued pursuant to the RBM’s mandate to oversee payment systems in Malawi under section 4(e) of the RBM Act.¹²⁹

The objective of the Mobile Guidelines is to promote a stable and sound financial structure that enables mobile money payments.¹³⁰ The Mobile Guidelines state explicitly that they shall apply only to non-bank based mobile money payments models. These are models where the service is provided by a non-bank entity, such as a mobile network operator (MNO).¹³¹



The Mobile Guidelines provide that any entity wishing to provide mobile money payments services must apply in writing to the RBM for a licence.¹³² Some of the most crucial requirements to be included in the application include the certificate of incorporation as a registered company,¹³³ a copy of the licence to operate mobile telecommunications services

¹²⁷ Definitional section of the Mobile Guidelines.

¹²⁸ Definitional section of the Mobile Guidelines.

¹²⁹ Paragraph 2.0 of the Mobile Guidelines.

¹³⁰ Paragraph 3.0 of the Mobile Guidelines.

¹³¹ Paragraph 4.0 of the Mobile Guidelines.

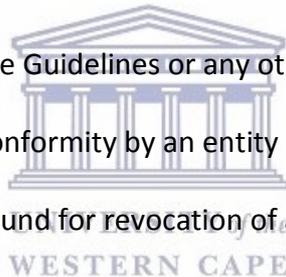
¹³² Paragraph 5.0 of the Mobile Guidelines.

¹³³ Paragraph 5.1 of the Mobile Guidelines.

from MACRA,¹³⁴ a description of the mobile financial payment service,¹³⁵ and conditions for recruiting network agents and a standard copy of the service level agreement.¹³⁶

Where the RBM is satisfied with the entity's application, it may require the entity to conduct a pilot trial of the product. If the RBM is satisfied that the product is safe and viable, it must issue a letter of no objection to the entity's commencement of business and one copy of such letter must be furnished to MACRA.¹³⁷

Even where a licence has been issued by the RBM, it retains authority to revoke it.¹³⁸ Some of the reasons for revocation which are very relevant to this paper include a situation where the RBM is of the view that the mobile money payments service provider does not operate in the interest of the public¹³⁹ and where the mobile money payments service provider violates the provisions of the Mobile Guidelines or any other laws and regulations related to them.¹⁴⁰ It follows then that non-conformity by an entity providing mobile money payments services with AML/CFT laws is a ground for revocation of a licence issued by the RBM.



The Mobile Guidelines address the critical issue of agents who are utilised by mobile money payments service providers in the provision of their services.¹⁴¹ They require mobile money payments service providers to enter into contracts with agents according to which they must exercise reasonable control over the agents.¹⁴² Before establishing a business relationship with the agents, the service providers must identify independently the agents

¹³⁴ Paragraph 5.2 of the Mobile Guidelines.

¹³⁵ Paragraph 5.3 of the Mobile Guidelines.

¹³⁶ Paragraph 5.4 of the Mobile Guidelines.

¹³⁷ Paragraph 6.0 of the Mobile Guidelines.

¹³⁸ Paragraph 7.0 of the Mobile Guidelines.

¹³⁹ Paragraph 7.3 of the Mobile Guidelines.

¹⁴⁰ Paragraph 7.4 of the Mobile Guidelines.

¹⁴¹ Paragraph 11.0 of the Mobile Guidelines.

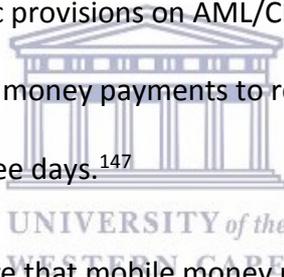
¹⁴² Paragraph 11.7 of the Mobile Guidelines.

and verify such identity. Where the agent is an individual, the following particulars must be identified: the name, address, signature and/or bio-data.¹⁴³

If the agent is a registered business, the following documents must be furnished and verified: the certificate of incorporation; board approval to operate a mobile money payments service; and physical address of head office and list of branches.¹⁴⁴

The service providers are obligated also to train the agents to ensure that they execute their responsibilities effectively.¹⁴⁵ The agents on their part are required to report suspicious transactions to the mobile money payments service providers to whom they account as their principals.¹⁴⁶

The Mobile Guidelines have specific provisions on AML/CFT. They obligate all institutions carrying out the business of mobile money payments to report all transactions from agents or subscribers to the FIU within three days.¹⁴⁷



Lastly, the Mobile Guidelines require that mobile money payments service providers adhere to the Money Laundering Act (2006) and Regulations issued by the FIU from time to time.¹⁴⁸

All the above-mentioned provisions ensure that mobile money payments are operated with integrity and at a reduced risk of being utilised for money laundering and terrorist financing purposes.

¹⁴³ Paragraph 11.1 of the Mobile Guidelines.

¹⁴⁴ Paragraph 11.2 of the Mobile Guidelines.

¹⁴⁵ Paragraph 11.5 of the Mobile Guidelines.

¹⁴⁶ Paragraph 11.8 of the Mobile Guidelines.

¹⁴⁷ Paragraph 13.1 of the Mobile Guidelines.

¹⁴⁸ Paragraph 13.2 of the Mobile Guidelines.

3.2.4 The Financial Services Act (2010)

This Act is an important enactment in the regulation of financial institutions, of which mobile money payments are a part. To be sure, the Act itself does not recognise mobile money payments as being part of financial institutions in its definitional section, but since they do have a bearing on the integrity and stability of the financial system they thus fall under the control of the Act by extension in the broader definition of the term financial institution.¹⁴⁹ The Act designates the Governor of the RBM as the Registrar of financial institutions and bestows upon him or her regulatory and supervisory authority over the financial services industry.¹⁵⁰ Thus if a mobile money payments service provider is not registered in accordance with this Act, it cannot operate such business. The specific procedures for registration are provided for under the Act.¹⁵¹

Under Section 10 of the Act, the Registrar is obligated to execute his supervisory duties in order to achieve the highest standards of business conduct by financial institutions¹⁵² in the interests of guaranteeing the stability of the financial system¹⁵³ and deterring the commission of financial crimes in financial institutions.¹⁵⁴

What is more, the Act requires the Registrar to consult and to enter into arrangements with other governmental departments when performing his or regulatory and supervisory functions over the financial industry.¹⁵⁵ A good example of this is the MOU signed by the

¹⁴⁹ Madise S 'Payment Systems and Mobile Money in Malawi: Towards Financial Inclusion and Financial Integrity', available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2531319 (Accessed on 20 January 2017).

¹⁵⁰ Sections 8(1) and (2) of the Financial Services Act.

¹⁵¹ Sections 23 and 24 of the Financial Services Act.

¹⁵² Section 10(b) of the Financial Services Act.

¹⁵³ Section 10(d) of the Financial Services Act.

¹⁵⁴ Section 10(e) of the Financial Services Act.

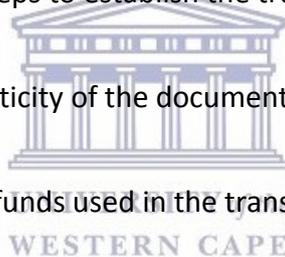
¹⁵⁵ Section 19 of the Financial Services Act.

RBM, MACRA and the FIU to create an environment conducive to the operation of mobile money payments, discussed above.

As far as AML/CFT obligations are concerned, the Act requires financial institutions to demand and record proof of identity whenever dealing with clients, whether occasionally or on a regular basis, more especially when it concerns large cash transactions.¹⁵⁶ It further obligates financial institutions to make STRs to the FIU whenever suspicion of ML/TF arises in a transaction.¹⁵⁷

It is an offence under the Act for a financial institution to permit a transaction, including the opening of an account, to go through when its employee, officer or director:

- (a) does not take reasonable steps to establish the true identity of the client;
- (b) has doubts as to the authenticity of the documentation furnished by the client; and
- (c) knows or suspects that the funds used in the transaction are proceeds of an illegality.¹⁵⁸



3.2.5 The Communications Act

This is Act that regulates communication services in the country. It establishes the Malawi Communications Regulatory Authority (MACRA) under section 3. One of the main functions of MACRA is to license mobile network operators to carry out their business in the country.¹⁵⁹ Thus, if an MNO is not issued with a licence by MACRA under this Act, it cannot

¹⁵⁶ Section 100(1)(a).

¹⁵⁷ Section 100(1)(b).

¹⁵⁸ Sections 100(3)(a), (b) and (c).

¹⁵⁹ Section 5(2)(g)(i) of the Communications Act.

engage in the business of providing mobile money payments services in Malawi.¹⁶⁰ MACRA is listed as one of the oversight bodies with regulatory functions over mobile money payments services under the Mobile Guidelines.¹⁶¹ Under the same Mobile Guidelines, the RBM must withdraw automatically an MNO's licence to provide mobile money payments services in Malawi in the event of MACRA withdrawing the service provider's telecommunications licence for whatever reason.¹⁶² All this signifies that MACRA is an important governmental body in the regulation and supervision of mobile money payments services in the country.

3.3 Gaps in the Regulation and Operation of Mobile Money Payments Services and the Potential Risk of ML/TF in Malawi

Mobile money payments services have been touted as agents that foster economic development because they help the poor and underprivileged who are under- or unbanked to have access to financial services.¹⁶³ This mobile money revolution has swept many countries worldwide, but nowhere on the planet has it flourished and taken hold so extensively as in Africa's sub-Saharan rural areas.¹⁶⁴ Malawi has not been bypassed by this mobile money payments services revolution. Currently, Malawi has two MNOs which offer mobile money services to the nation. These are Telekom Networks Malawi (TNM) and Airtel Malawi.¹⁶⁵

¹⁶⁰ Buckley *et al* (2015: 458).

¹⁶¹ Definitional section of the Mobile Guidelines.

¹⁶² Paragraph 7.4 of the Mobile Guidelines.

¹⁶³ Kersop M and Du Toit S F 'Anti-Money Laundering and the Effective Use of Mobile Money in South Africa Pt (1)' *Potchefstroom Electronic Law Journal* (2015) 18(5) 1603 and 1604.

¹⁶⁴ Kersop M and Du Toit S F (2015) 1603.

¹⁶⁵ Buckley *et al* (2015: 449).

There is ample evidence suggesting that mobile money is crucial for reducing poverty.¹⁶⁶ However, the potential of this important technological innovation to be abused by criminals for money laundering and terrorist financing purposes can never be underestimated. The FATF, through its New Payment Methods Report of 2006 and the Money Laundering Using New Payment Methods typology of 2010, which are discussed above, echoes the sentiments that mobile money payments have the potential of being abused for money laundering and terrorist financing.¹⁶⁷ It thus is of great importance for authorities to make sure that the quest to reduce poverty and increase financial inclusion of those under-served by the formal financial system should not be pursued at the expense of weakening effective AML/CFT measures.¹⁶⁸

As illustrated above, Malawi has a quite elaborate legal framework regulating financial institutions on the AML/CFT front. Mobile money payments services providers are a part of these financial institutions which fall under the regulation and supervision of this elaborate legal framework. Despite the existence of this detailed legal framework, there remain gaps and challenges that have the potential of exposing mobile money payments to the risk of being abused for money laundering and terrorist financing purposes. This section of the paper will highlight and discuss these gaps and challenges. The first part of this section will discuss gaps and challenges which are distinctive to the Malawian situation whilst the second part will discuss those common to all mobile money payments systems.

¹⁶⁶ Buckley *et al* (2015: 439). See also Marina S and Zerzan A 'Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks' GSMA DISCUSSION PAPER (2010) 4.

¹⁶⁷ FATF Money Laundering Using New Payment Methods (2010: 20).

¹⁶⁸ Kersop M and Du Toit S F (2015: 1608).

3.3.1 Lack of National Identity Cards

Malawi does not have a fully-fledged national identification card system.¹⁶⁹ The only other documents that are relied upon to identify clients are a driver's licence and a passport, both of which are hardly accessible to most Malawians.¹⁷⁰ In November 2016, the government rolled out a pilot national identification card scheme.¹⁷¹ Under this pilot trial, only 5,000 Malawians have national identity cards out of a population of close to 17 million people.¹⁷² Until the system is rolled out to cover the whole citizenry, it will remain difficult for financial institutions to obtain and verify the identity of their clients. For example, non-Malawians have in the past exploited this flaw to obtain Malawian citizenship. This may result eventually in undermining Malawi's efforts to combat ML/TF and it also increases the risk of mobile money payments being used for ML/TF purposes since the service providers have no reliable documentation on which to base their verification of a client's identification. This is further compounded by the fact that a large segment of the Malawian population has no verifiable home addresses.¹⁷³



¹⁶⁹ Malawi FIU 'Money Laundering Typologies in Malawi' (2016) 12 Para 26. See also Nkhoma G B (2012: 34), and Buckley *et al* (2015: 451).

¹⁷⁰ Malawi FIU (2016: 12).

¹⁷¹ Embassy of the Republic of Malawi Addis Ababa (2016), 'Ethiopia 5,000 Malawians to get national IDs by August', available at <http://malawiembassy-addis.com/5000-malawians-to-get-national-ids-by-august/>, (Accessed on 11 December 2016). See also Hughes N 'UK donates \$11M to help Malawi launch national ID card, available at <https://oneworldidentity.com/2016/10/27/uk-donates-11m-to-help-malawi-launch-national-id-card/>, (Accessed on 11 December 2016).

¹⁷² Embassy of the Republic of Malawi Addis Ababa (2016).

¹⁷³ Madise S 'Payment Systems and Mobile Money in Malawi: Towards Financial Inclusion and Financial Integrity', available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2531319 (Accessed on 20 January 2017). 85 percent of Malawians live in rural areas and their households have no postal codes or formal residential addresses: See Buckley *et al* (2015: 447).

3.3.2 Non-Registration of SIM Cards on Purchase

Under Malawian law, there is no requirement for a subscriber to have his or her SIM card registered when purchasing it from MNOs or their agents. Non-registration of SIM cards, coupled with the lack of national identification cards, encourages anonymity and may lead to a situation where a potential money launderer can purchase several SIM cards and use them to open several mobile money payments accounts, using several fraudulent identities, thereby widening the scheme and speed at which he can launder the proceeds from his criminal enterprises.¹⁷⁴ This is possible despite the fact that the terms and conditions of both MNOs in Malawi stipulate that a client may open only one mobile money payments account.

3.3.3 Malawi is a Largely Cash-Based Economy

Malawi is a cash-based economy.¹⁷⁵ In Malawi, cash is the dominant form of money used in commercial transactions. This exposes mobile money payments to the greater risk of being utilised for ML/TF purposes because both Airtel and TNM allow their clients' transaction on their accounts to be funded using cash. This is very attractive to criminals because it is very difficult to trace cash. It leads to a situation where there are no or insufficient paper trails regarding the funding transaction and the origin of the funds.¹⁷⁶ All one needs to do is go to a registered agent and give him cash, which is then converted to stored e-value which can then be transferred to another person or used to purchase goods. Thus, it becomes difficult for financial institutions such as mobile money payments service providers to differentiate

¹⁷⁴ Money Laundering Using New Payment Methods (2010: 25 Para 73).

¹⁷⁵ Malawi FIU (2016: 11 Para 25).

¹⁷⁶ Money Laundering Using New Payment Methods (2010: 27 Para 83).

between legal and illegal or unusual transactions.¹⁷⁷ This problem is exacerbated by the fact that TNM and Airtel do not require the inclusion of originator information from the initiator of a mobile money payments transaction. This loophole enables criminals to launder the proceeds of their crimes through mobile money payments.

3.3.4 Employment of Generic AML/CFT Procedures by Staff of Financial Institutions

One of the challenges in the AML/CFT campaign is that most financial institutions put in place and implement generic AML/CFT measures just to be seen to be in conformity with the requirements set by regulatory and supervisory authorities, without doing more to achieve the intended objectives of those requirements. The RBM has noted that most Malawian financial institutions conduct only generic AML/CFT measures. It noted that financial institutions had enormous deficits and were falling seriously short in customer identification and verification processes, record keeping of client information, ongoing monitoring of customer transactions, ML/TF risk assessment of customers, products and services, delivery methods and geographical locations.¹⁷⁸ It has noted further that financial institutions conduct limited and generic AML/CFT staff training which does not cover all legislative requirements and specialised business areas.¹⁷⁹

The same applies to agents, who are not trained to conduct proper and thorough AML/CFT measures. Some of them are more concerned with making a commission and choose purposely to ignore conducting AML/CFT procedures as required of them by the Mobile Guidelines discussed above. The situation becomes even worse where agents are not subject to any strict AML/CFT obligations. All these obligations rest on the principal service

¹⁷⁷ Malawi FIU (2016: 11 Para 25).

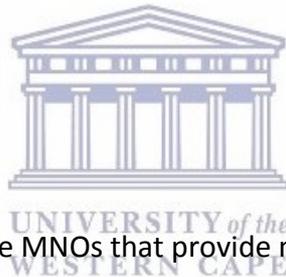
¹⁷⁸ Reserve Bank of Malawi (2014).

¹⁷⁹ Reserve Bank of Malawi (2014).

providers. This is troublesome because all the liability for not carrying out AML/CFT measures falls squarely on the principal. This does not create an incentive for agents to follow the AML/CFT measures. For instance, under the Mobile Guidelines agents are obligated only to send STRs to mobile money payments service providers.¹⁸⁰ This is risky because agents are the ones involved mainly in the registration of clients on behalf of the service providers. Thus, there is a possibility that they can register clients without verifying their true identity, thereby exposing the products to the danger of being exploited for ML/TF.

Having considered the gaps and challenges which are specific to Malawi, the discussion will now focus on the challenges that are common to mobile money payments services in general.

3.3.5 Absence of Credit Risk



This issue concerns situations where MNOs that provide mobile money payments services have no incentive to obey AML/CFT obligations strictly, because all the funds used to make the transactions on the service are prepaid.¹⁸¹ Since the funds are prepaid by the clients using the service, the MNOs do not have any credit risk. They operate on the assumption that they have nothing to lose, therefore do not see the need to obtain full and accurate information about the customer and the nature of the business relationship.¹⁸²

¹⁸⁰ Paragraph 11.8 of the Mobile Guidelines.

¹⁸¹ Money Laundering Using New Payment Methods (2010: 21 Para 61).

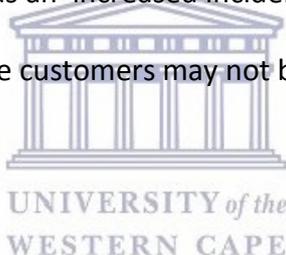
¹⁸² Money Laundering Using New Payment Methods (2010: 21 Para 61).

3.3.6 Speed of Transactions

New payment methods such as mobile money payments are designed in such a way that the transactions are conducted rapidly. Funds are transferred with utmost speed and are converted from one form to another with ease. This is attractive to money launderers and presents a challenge to supervisory and law enforcement agencies in tracing and investigating the proceeds of crime.¹⁸³

3.3.7 Non-Face to Face Business Relationship

Some mobile money payments are designed in such a way that there is no face to face interaction between the clients and the providers. This increases the threat of ML/TF in the mobile money payments products as an increased incidence of impersonation raises the risk of fraud being perpetrated since customers may not be who they say they are.¹⁸⁴



3.4 Financial Inclusion

Financial inclusion is another major issue that features prominently in the discourse on mobile money payments. It has been defined as 'ensuring access to appropriate financial products and services at an affordable cost in a fair and transparent manner'.¹⁸⁵ This access has to be provided to the financially excluded who are also referred to as the unbanked.¹⁸⁶

The problem of financial exclusion cropped up as a result of reluctance on the part of banks to provide banking arrangements and financial services to poor and low income

¹⁸³ Money Laundering Using New Payment Methods (2010: 21 Para 61).

¹⁸⁴ Money Laundering Using New Payment Methods (2010: 21 Para 61).

¹⁸⁵ The FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion Para 17. See also Buckley *et al* (2015: 439), Merritt C 'Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments' Retail Payments Risk Forum White Paper Federal Reserve Bank of Atlanta (2010) 4.

¹⁸⁶ FATF Guidance: AML and Financial Inclusion Para 17.

communities. The reason for this unwillingness has to do with the fact that the high transaction costs and poor returns for the banks.¹⁸⁷ As a consequence, people are excluded from the formal financial system. In 2015, there were 2.5 billion adults worldwide who were officially excluded from the formal financial system.¹⁸⁸ This is a figure of epic proportions. The situation of excluded people is dire as they cannot be cushioned from economic shocks which, in turn, perpetuates the cycle of poverty.¹⁸⁹ Therefore, the initiative to achieve financial inclusion has developed into a vital international policy in the fight against the scourge of poverty.¹⁹⁰ This effort is exemplified by the fact that organisations and forums such as the G20 summits, the Global Policy Forum (GPF) of Alliance for Financial Inclusion (AFI), Better than Cash Alliance (BTCA), FATF and the Basel Committee on Financial Inclusion have all championed the importance of inclusion in the fight against poverty.¹⁹¹

Mobile money has been hailed as an important medium through which financial inclusion of the global unbanked adult population can be achieved.¹⁹² This is so because the mobile phone technology has been adopted by a huge portion of the world's population. It is the most widely adopted form of modern technology in history.¹⁹³ Besides, in 2006 the mobile phone achieved the milestone of being the first piece of communications technology to



¹⁸⁷ Buckley *et al* (2015: 439).

¹⁸⁸ The Imperative of Financial Inclusion, UNITED NATIONS SECRETARY GENERAL'S ADVOCATE FOR FINANCIAL DEVELOPMENT, available at <http://www.unsgsa.org/financial-inclusion> (Accessed on 5 January 2017).

¹⁸⁹ Buckley *et al* (2015: 440).

¹⁹⁰ De Koker L 'Aligning Anti-money Laundering, Combating of Financing of Terror and Financial Inclusion: Questions to Consider when FATF Standards are Clarified' (2011) *JFC* 362.

¹⁹¹ Buckley *et al* (2015: 441).

¹⁹² Alexandre C and Eisenhart L C 'Mobile Money as an Engine of Financial Inclusion and Lynchpin of Financial Integrity' *WJLTA* (2013) 287.

¹⁹³ GSMA, available at <http://www.m4dimpact.com/data/sectors/mobile-industry> (Accessed on 11 January 2017).

have more users in developing countries than in the developed world.¹⁹⁴ The mobile phone enables even those situated in inaccessible rural areas to gain access to financial services through mobile money payments services.¹⁹⁵ The reason is that the acquisition of a mobile phone does not require the user to install as a prerequisite new technological infrastructure since it utilises the already existing infrastructure.¹⁹⁶ Once the people in the rural areas begin accessing these financial services through mobile phones, they become enticed to join the formal financial system, hence achieving the goal financial inclusion.¹⁹⁷

3.4.1 Balancing AML/CFT Obligations and Financial Inclusion

Despite mobile money payments being promoted as catalysts for financial inclusion, some have argued that the possibility of these services being utilised by criminals for purposes of money laundering and terrorist financing should not be overlooked.¹⁹⁸ It has been asserted that there should be a balance between the two, by which is meant that, in order not to stifle the potential for financial inclusion, regulators have been asked to strike a balance in addressing the AML/CFT risks which have the potential of plaguing the mobile money payments industry and promoting innovation.¹⁹⁹

It has been argued also that financial inclusion and the need to protect mobile money payments services from being used for money laundering and terrorist financing purposes

¹⁹⁴ Chatain P *et al* World Bank Working Paper No 146: Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing (2008), available at http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf, (Accessed on 11 January 2017).

¹⁹⁵ Chatain P *et al* (2008: xiii).

¹⁹⁶ Chatain P *et al* (2008: viii).

¹⁹⁷ Buckley *et al* (2015: 441).

¹⁹⁸ Marina S and Zerzan A (2010: 4).

¹⁹⁹ Khaonarong T 'Oversight Issues in Mobile Payments', IMF Working Paper 14/123 (2014) 18, available at <https://www.imf.org/external/pubs/ft/wp/2014/wp14123.pdf>, (Accessed on 10 January 2017).

need to be viewed as complementary and not competing objectives, if the balance between the two is to be achieved by mobile money payments regulators.²⁰⁰

In order to strike a balance between these two financial sector policy objectives, it has been argued that mobile money regulators should adopt a two-pronged approach. The regulators are urged to adopt an enabling and proportionate approach to the regulation of mobile money payments services. Each of these two concepts is explained below.

(a) Enabling Approach

An enabling approach is an approach where the regulator is not only tasked with the duties to achieve financial stability, integrity and consumer protection, but also with the obligation to achieve financial inclusion of those under-served by the formal financial system. Thus, regulators must produce regulatory initiatives that are essential for the development and flourishing of mobile money payments services.²⁰¹



(b) Proportionate Regulation

This second part of the two-pronged approach hinges on the contents of the regulatory instruments relied upon by the regulator. It is the duty of the regulator to ensure that the costs that incurred by both financial institutions providing mobile money payments services and customers are commensurate to the risks that are being addressed, especially when regard is had to the benefits that are expected from the product.²⁰² The justification for proportionality is that excessive regulation, including AML/CFT regulation, over-burdens

²⁰⁰ Marina S and Zerzan A (2010: 8).

²⁰¹ Buckley *et al* (2015: 443).

²⁰² Buckley *et al* (2015: 445).

financial institutions, thereby stifling business and economic growth.²⁰³ Thus, the proportionate regulation of mobile money payments services safeguards the mobile money payments products from AML/CFT risks and helps create an environment conducive to innovation and healthy business which, in turn, fosters economic growth.

3.5 The Regulation of Mobile Money Payments Services in Kenya: The Case of M-PESA

The most successful implementation of a mobile money payments service is that of M-PESA. This is a Kenyan mobile money payments service system that was launched in 2007 by the Vodafone Group and Kenya's leading mobile network operator, Safaricom, after a successful pilot trial in 2005.²⁰⁴ It has been hailed as one of the most successful mobile money payments service in the world. This assertion is backed by the sheer number of clients registered to the service and the number of transactions conducted through it.²⁰⁵ Although launched only in 2007, by May 2008 the service had two million registered customers.²⁰⁶ This figure rose to more than six million registered customers in 2009.²⁰⁷ The number of registered active users of the service more than doubled, to reach 15.2 million in 2011.²⁰⁸



²⁰³ Kabor S E 'The Role of Anti-Money Laundering Law in Mobile Money Systems in Developing Countries', *Washington Journal of Law, Technology and Arts* 8(3) (2013) 305.

²⁰⁴ Buku M W and Meredith M W 'Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity', *Washington Journal of Law, Technology and Arts* 8(3) (2013) 378.

²⁰⁵ Buku M W and Meredith M W (2013: 389).

²⁰⁶ Buku M W and Meredith M W (2013: 390).

²⁰⁷ Williams I 'Regulatory frameworks and Implementation patterns for Mobile Money in Africa: The case of Kenya, Ghana and Nigeria', (2013) 4, available at http://s3.amazonaws.com/academia.edu.documents/42068100/Regulatory_frameworks_and_Implementation20160204-17000-9tcws1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1485341002&Signature=27kgM3ORPY4%2Fc5Nuz7NYo81gm44%3D&response-content-disposition=inline%3B%20filename%3DRegulatory_frameworks_and_Implementation.pdf (Accessed on 20 January 2017).

²⁰⁸ Buku M W and Meredith M W (2013: 390).

Statistics show that in 2013 over 2 million transactions were conducted over the M-PESA service every day,²⁰⁹ and this translated to US\$4.98 billion worth of transactions conducted in a year.²¹⁰ In a span of five years since the launch of the M-PESA service in Kenya, over US\$1.4 trillion in peer to peer transactions have been transferred through the service.²¹¹ It has been averred that this means that 'M-PESA processes more transactions domestically than Western Union does globally'.²¹²

It goes without saying that a service that has a high number of registered users and conducts transactions of this magnitude on a daily basis will be on the radar of regulatory authorities and raise AML/CFT risk concerns. The section below discusses how the regulatory authorities in Kenya control the mobile money payments service of M-PESA.

In 2007, when the M-PESA service was launched, the Kenyan regulatory authorities adopted the strategy of regulating mobile money payments services in the same way as banks had been traditionally regulated. They did this by merely extending the pre-existing regulations which are applicable traditionally to banks to mobile money payments services.²¹³ The measures employed to control money laundering and conduct AML/CFT procedures such as KYC, CDD, STR and mandatory record keeping were contained in generally applicable criminal law statutes.²¹⁴ This position changed in 2009 with the passage of the Proceeds of Crime and Anti-Money Laundering Act, which imposed more rigorous AML/CFT regulations and made all the FATF Recommendations applicable to and mandatory for all financial

²⁰⁹ Buku M W and Meredith M W (2013: 390).

²¹⁰ Buku M W and Meredith M W (2013: 391).

²¹¹ Buku M W and Meredith M W (2013: 391).

²¹² Mas I and Radcliffe D 'Mobile Payments Go Viral: M-PESA in Kenya' 32 *Journal of Financial Transformation* (2011) 169. See also Buku M W and Meredith M W (2013: 391).

²¹³ Buku M W and Meredith M W (2013: 394).

²¹⁴ Buku M W and Meredith M W (2013: 395).

institutions.²¹⁵ Thus Safaricom is also covered. In 2011, the Kenyan legislature passed the National Payment Systems Act, which imposes the same obligations on mobile money payments and traditional banking institutions.²¹⁶

The registration of customers and protection of the service from being abused by identity fraudsters for money laundering and terrorist financing purposes has been aided greatly by the fact that Kenya has a functioning national identity system.²¹⁷

Despite having rigorous AML/CFT regulations and a fully established national identity system, the safeguarding of the M-PESA from money laundering has also to a large extent depended on the establishment of and compliance with voluntary internal AML/CFT procedures and programmes by Safaricom. These procedures have centred on three key areas, namely, (a) agent training, (b) internal KYC procedures and (c) strict transaction monitoring.²¹⁸

(A) Agent Training



Safaricom has invested huge effort and expended considerable resources to train agents for its M-PESA mobile money service in the observance of AML/CFT controls.

Agents are made to undergo an intensive training, covering the entire operating scheme and Safaricom's own AML/CFT and KYC procedures.²¹⁹ This type of training is also undergone by members of staff at all levels of the establishment and is audited annually to check for

²¹⁵ Muthiora B 'Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution' GSMA (2015) 22. See also Buku M W and Meredith M W (2013: 395).

²¹⁶ Buku M W and Meredith M W (2013: 396).

²¹⁷ Makin P 'Regulatory Issues Around Mobile Banking: *New initiatives to bank the poor are straining the world's financial regulatory systems*', available at <http://www.oecd.org/ict/4d/43631885.pdf>, (Accessed on 13 January 2017).

²¹⁸ Buku M W and Meredith M W (2013: 397).

²¹⁹ Buku M W and Meredith M W (2013: 397).

compliance deficiencies and areas that require improvement by the Vodafone Group Money Laundering Reporting Office.²²⁰

(B) Internal KYC Procedures

Under the M-PESA mobile money payment service, both customers registered on the service and agents who play a crucial role in its functioning are subject to in-depth KYC procedures.²²¹

In addition, Safaricom has adopted an automated screening mechanism used to screen people who are politically exposed and those who are on the international sanctions or terror list. This is done to reduce the risk of its mobile money service being used for money laundering and terrorist financing purposes.²²²

(C) Strict Transaction Monitoring



In its quest to reduce the risk of its mobile money service being utilised for money laundering and terrorist financing purposes, Safaricom has placed limits on transactions and has implemented a policy of conducting on-going monitoring of transactions in relation to customers who are still utilising the service.²²³

It bears noting that, despite a rigorous regulatory legal regime being in place, Safaricom has gone to great lengths to reduce the risks of its mobile money service being utilised by criminals for money laundering and terrorist financing purposes.²²⁴ By and large, this has helped make M-PESA a considerably secure service. This shows that, for the fight against

²²⁰ Buku M W and Meredith M W (2013: 397).

²²¹ Buku M W and Meredith M W (2013: 397).

²²² Buku M W and Meredith M W (2013: 397).

²²³ Buku M W and Meredith M W (2013: 398).

²²⁴ Buku M W and Meredith M W (2013: 396).

money laundering and terrorist financing to be successful, it is essential that all the stakeholders play a substantial role in the bigger scheme of things.

3.6 Conformity to FATF Standards by Malawian Regulatory Authorities and Mobile Money Payments Service Providers

As discussed above, Malawi has made great strides in order to conform to the FATF AML/CFT international standards by enacting the Money Laundering Act, other pieces of legislation and guidelines addressing the area of economic criminality. However, going by the 2014 RBM Annual Report which stated that most financial institutions have established and apply only generic AML/CFT procedures in relation to customer identification, record keeping of client information, ongoing monitoring of customer transactions and ML/TF risk assessment of customers, products and services, delivery methods and geographical locations, then, at best, Malawi is only partially compliant with AML/CFT international standards.



It is worrying that Malawian financial institutions spend only limited resources to train their staff in comprehensive AML/CFT procedures - training which has been labelled by the Central Bank as generic. Apart from this, there is no concrete evidence showing that mobile money payments service providers have set aside substantial resources to train agents who are essential players in the functioning of mobile money payments services. Despite all the above-mentioned shortcomings, the regulatory authorities have refrained from imposing sanctions against defaulters or reprimanding them.

All these shortfalls in the enforcement of AML/CFT international standards need to be remedied because they expose mobile money payments products to a high risk of being misused for money laundering and terrorist purposes.

3.7 Conclusion

Mobile money payments are a relatively a new phenomenon in Malawi as they were introduced only in 2012. They present a unique opportunity to enhance the financial inclusion of Malawi's unbanked population which is worryingly under-served by the formal financial system. This is so because most Malawians have access to a mobile phone and hence MNOs do not have to establish an expensive information technology infrastructure to bring their mobile money payments services to the doorsteps of the unbanked population.

Thus, the mobile phone serves to cut the operational costs of providing financial services to the unbanked.



Despite being flaunted as a crucial mechanism for financial inclusion of the unbanked, there are gaps and challenges which expose mobile money payments to the high risk of being misused by criminals for money laundering and the financing of terrorism. The gaps and challenges include the country's having no national identification system, non-registration of SIM cards on purchase, funding mobile money payments transactions using mainly cash, the employment of generic AML/CFT procedures by financial institutions and their staff and the partial compliance with FATF international standards by the general financial sector and the regulatory bodies.

The partial compliance with the FATF international standards occurs despite the fact that Malawi has in place a comprehensive AML/CFT regulatory legal framework. It is therefore

imperative that the responsible authorities formulate deliberate executive policies and an action plan to address the challenges highlighted above. Such an initiative would go a long way to reduce the risk of mobile money payments being used for purposes of money laundering and terrorist financing. In order to achieve this goal, the responsible authorities can borrow a leaf or two from their counterparts in Kenya as regards the evolutionary process they followed to regulate the M-PESA service efficiently.



Chapter Four

Conclusions and Recommendations

4.1 General Conclusions

Criminals and terrorist financiers have become wary of using the formal financial system to launder the proceeds of their criminal enterprises or to bankroll terrorist organisations. This state of affairs has been brought about by the concerted global efforts aimed at eradicating money laundering and terrorist financing.²²⁵ Thus, criminals and terrorist sponsors have turned to alternative methods which do not involve the formal financial system to launder their proceeds and fund terrorist organisations.²²⁶ One such alternative method involves laundering money using mobile money payments. This paper has discussed the potential which mobile money payments have to be used by criminals in order to clean the proceeds of their crimes so as to create a gulf between themselves and the predicate offence, or by terrorist financiers to finance terrorist organisations who are hell-bent on carrying out terrorist attacks around the globe. The paper has also highlighted the loopholes which increase the risk of Malawian mobile money payments being exploited by criminal elements for money laundering and terrorist financing purposes.

The following are the recommendations which the author believes, if adopted, would go a long way in reducing the risk of mobile money payments being used to launder criminal proceeds or to finance terrorist groups.

²²⁵ McSkimming S 'Trade Based Money Laundering: Responding to an Emerging Threat', 15(1) *Deakin Law Review* (2010) 37.

²²⁶ McSkimming S (2010: 37).

4.2 Establishing a National Identification System

As pointed out above, Malawi does not have a national identity card issued to its citizens. This makes it difficult to identify Malawians properly. It thus becomes cumbersome for financial institutions such as mobile money payments service providers to differentiate between Malawians and non-Malawians. It is also hard to establish the authenticity of a person's identity in the absence of a national identity card. The alternative documents which are relied upon by Malawian authorities and financial institutions to establish the true identity and verify a person's personal details are passports and driver's licences. The problem with these alternative documents of identification is that they are not accessible easily to all Malawians. They are costly, which means only a privileged few Malawians can afford to obtain them. These documents are also ones that an ordinary Malawian will endeavour to have only if the need arises. Accordingly, when no need exists to have a driver's licence or passport, an average Malawian has no incentive to come into the possession of such documents. The problem is exacerbated by the fact that there is no central automated bio-data storage centre. The establishment of an efficient national identification system would be hugely helpful for mobile money payments service providers in carrying out their AML/CFT obligations of customer identification and verification.

4.3 Extending all AML/CFT Obligations Imposed by Law to Agents

Agents are crucial players in the functioning efficiency of mobile money payments. They perform most of the essential functions, such as registration of customers and the execution of most transactions initiated by customers through the service. At present, not all the AML/CFT obligations are imposed on agents. According to the Mobile Guidelines, agents are

required to report only suspicious transactions to their principal, who in this case happens to be the MNO providing the mobile money payments service. If all the AML/CFT obligations were extended to the entire spectrum of agents, this would reduce greatly the risk of mobile money payments being utilised for purposes of money laundering and terrorist financing.

4.4 Adoption and Application of Comprehensive AML/CFT Procedures by Financial Institutions

Financial institutions need to endeavour to adopt and apply robust internal AML/CFT measures in the provision of their services to their customers. These measures should cover areas such as customer identification and verification, staff and agent training, record keeping, on-going transaction monitoring and product risk assessment. This assists much in giving effect to the applicable laws. Currently, financial institutions are criticised by the Central Bank for applying purely generic AML/CFT measures.



4.5 Registration of SIM Cards on Purchase

Subscribers should be legally compelled to register with the MNO whenever they purchase a SIM card. This would help combat anonymity and the risk of criminals using fraudulent identities to open several mobile money accounts to be used to launder their criminal proceeds. Under Malawian law as it currently stands, it is not a requirement to register a SIM card with an MNO upon purchase.

4.6 Investment in Information Communication Technology (ICT)

Malawi lags behind in the use of ICT in its quest to meet its international AML/CFT obligations. The bulk of information is stored manually. This affects the quality of the records which financial institutions are required to keep under the FATF standards. Investment in proper ICT infrastructure would go a long way to remedy this deficiency. ICT would also help financial institutions to monitor transactions automatically by cross-checking their clients against international sanctions or terror list data bases, thereby reducing the risk of their products being abused for ML/TF purposes and saving time.

4.7 Conducting National and Product Risk Assessment

Recommendation 1 of the FATF international standards requires countries to conduct national risk assessments in order to identify areas which are vulnerable to be exploited for ML/TF purposes. The outcome of the Malawi national risk assessment that started in 2013 is yet to be published. The country is thus still operating in the dark as to which areas are susceptible to ML/TF purposes.

The FATF's Recommendation requires financial institutions also to assess the ML/TF risks of their products. A national and product risk assessment would assist in establishing the exact extent to which mobile money payments are prone to be utilised as vehicles for money laundering, and a risk assessment would help also to determine the amount of resources to be used to mitigate such risks.

The recommendations made in this paper are essential for the proper functioning of the mobile money payments industry in Malawi. They will serve to eliminate all the gaps and

challenges that make the financial sector and the economy in general vulnerable to economic criminals. Moreover, adopting effective measures would promote the integrity and stability of the financial system, which would help advance the drive towards financial inclusion of the financially excluded population.



BIBLIOGRAPHY

Primary Sources

International and Regional Instruments

1. Council Directive 2001/97 EC of the European Parliament and of the Council of the European Union of 4 December 2001.
2. Council Directive 2005/60/EC of the European Parliament and of the Council of the European Union on the Prevention of the Use of the Financial Systems for the Purposes of Money laundering and terrorist Financing of 26 October 2005.
3. Council Directive 91/308 ECC of the European Parliament and of the Council of the European Union on Prevention of the Use of the Financial System for the Purpose of Money Laundering of 10 July 1991.
4. Council Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, And Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC
5. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds from Crime (1990). Adopted in September 1990, came into force on 1 April 1991.
6. United Nations Convention against Corruption of 2003 (Merida Convention). Adopted by the United Nations General Assembly resolution A/58/422 on 31 October 2003, came into force on 14 December 2005.

7. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988). Adopted on 19 December 1988, came into force on 11 November 1990.
8. United Nations Convention against Transnational organised Crime of 2000 (Palermo Convention). Adopted by resolution A/RES/55/25 of 15 November 2000 at the fifty-fifth session of the General Assembly of the United Nations and came into force on 29 September 2003.

Malawian Legislation

1. Communications Act (Cap 68:01 of the Laws of Malawi).
2. Births and Deaths Registration Act (Cap 24:01 of the Laws of Malawi).
3. Financial Services Act of 2010 (Malawi) Act No. 26 of 2010 of the Laws of Malawi.
4. Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act (Cap 8:07 of the Laws of Malawi).
5. Reserve Bank of Malawi Act (Cap 44:02 of the Laws of Malawi).

Official Reports

1. Baker Tilly *Report on Fraud and Mismanagement of Malawi Government Finances: Covering transactions and controls in the six month period 1 April 2013 – 30 September 2013* (21 February 2014), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/28

5877/20140221 National Audit Office Malawi - Forensic Audit Report - FINAL ISSUED.pdf (accessed on 28 September 2016).

2. Embassy of the Republic of Malawi Addis Ababa (2016), 'Ethiopia 5,000 Malawians to get national IDs by August', available at <http://malawiembassy-addis.com/5000-malawians-to-get-national-ids-by-august/>, (Accessed on 11 December 2016).
3. ESAAMLG '4th Progress Report on Anti-Money Laundering and Combating the Financing of Terrorism Republic of Malawi' 20, available at www.esaamlg.org, (Accessed on 20 December 2016).
4. FATF and ESAAMLG (2008) Mutual Evaluation Report on Malawi, available at http://www.esaamlg.org/evaluationreports/Malawi_Report.pdf (accessed 12 March 2016).
5. FATF *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (16 February 2012), available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (accessed on 27 March 2016).
6. FATF *Typologies Report on Money Laundering Using New Payment Methods* (October 2006) FATF-GAFI: Paris, available at <http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusingnewpaymentmethods.html>, (Accessed on 12 March 2016).



7. FATF typologies Report on Money Laundering Using New Payment Methods- October (2010) FATF-GAFI: Paris, available at <http://www.fatf-gafi.org> (Accessed on 12 April 2016).
8. Introductory note to the FATF recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism Proliferation (16 February 2012). Available at [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf) (accessed on 1 September 2016).
9. Malawi FIU 'Money Laundering Typologies in Malawi' (2016), available at www.fiumalawi.gov.mw (Accessed on 16 December 2016).
10. Methodology for Assessing Compliance with FATF + 9 Recommendations (2004), available at <http://www.fatf-gafi.org/media/fatf/documents/reports/methodology.pdf> (accessed on 28 September 2016).
11. Reserve Bank of Malawi 'Financial Institutions Supervision Annual Report (2014)', available at [https://www.rbm.mw/Supervision/BankSupervision/?activeTab=BASUDirectivesand Guidelines](https://www.rbm.mw/Supervision/BankSupervision/?activeTab=BASUDirectivesandGuidelines), (Accessed on 16 April 2016).
12. The FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, available at <http://www.fatf-gafi.org> (Accessed on 17 January 2017).



13. The Imperative of Financial Inclusion, UNITED NATIONS SECRETARY GENERAL'S ADVOCATE FOR FINANCIAL DEVELOPMENT, available at <http://www.unsgsa.org/financial-inclusion> (Accessed on 5 January 2017).
14. United Nations Economic Commission for Africa and The African Union Commission Report of the High Level Panel on Illicit Financial Flows from Africa, "Track it, Stop it and Get it: Illicit Financial Flows" (26 February 2015), available at http://www.uneca.org/sites/default/files/PublicationFiles/iff_main_report_26feb_en.pdf (accessed on 6 April 2016).

Secondary Sources

Books

1. De Willebois *et al* (2011) *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It* World Bank: Washington DC.
2. Durrieu R (2013) *Rethinking Money Laundering and Financing of Terrorism: Towards a New Global Legal Order* Martin Nijhoff Publishers: Boston.
3. Houghton D *Money Laundering: A Concise Guide for All Businesses* (2 ed) 2009. Gower publishing Co.: Farnham.
4. Beare M E and Schneider S (2007) *Money Laundering in Canada: Chasing Dirty and Dangerous Dollars* University of Toronto Press: Toronto.
5. Mugarura N (2012) *The Global Anti-Money Laundering Regulatory Landscape in Less Developed Countries* Ashgate Publishing Company: Farnham Surrey.

6. Muller WH Kalin CH and Goldsworth JG (eds) (2007) *Anti-Money Laundering: International Law and Practice* John Willey & Sons: West Sussex.
7. Muthiora B (2015) *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution* GSMA, available at https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/2015_MMU_Enabling-Mobile-Money-Policies-in-Kenya.pdf (Accessed on 19 December 2016).
8. Scher D (2005) *Asset Recovery: Repatriating Africa's Looted Billions* Institute for Security Studies: Pretoria.
9. Stessens G (2000) *Money Laundering: A New International Law Enforcement Model* Cambridge International Press: New York.
10. Turner JE (2011) *Money Laundering Prevention: Detering, Detecting and Resolving Financial Fraud* John Wiley & Sons: New Jersey.
11. Unger B (2007) *The Scale and Impacts of Money Laundering* Edward Elgar: Cheltenham.
12. Yikona S, Slot B, Geller M et al (2011) *Ill-Gotten Money and the Economy: Experiences from Malawi and Namibia*.

Chapters in Books

1. Unger B (2007) "Implementing Money Laundering" in Masciandaro D et al *Black Finance: The Economics of Money Laundering* Edward Elgar: Cheltenham.

Journal Articles

1. Alexandre C and Eisenhart 'Mobile Money as an Engine of Financial Inclusion and Lynchpin of Financial Integrity' *Washington Journal of Law, Technology and Arts* (2013)
2. Buckley R, Greenacre J and Malady L 'The Regulation of Mobile Money in Malawi' 14(3) *Washington University Global Studies Law Review* (2015).
3. Buku M W and Meredith M W 'Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity', 8(3) *Washington Journal of Law, Technology and Arts* (2013).
4. De Koker L 'Aligning Anti-money Laundering, Combating of Financing of Terror and Financial Inclusion: Questions to Consider when the FATF Standards are Clarified' *JFC* (2011).
5. Gill M and Taylor G 'Preventing Money laundering or Obstructing Business?' *British Journal of Criminology* (2004).
6. Gordon R K 'Anti-Money Laundering Policies- Selected Legal, Political, and Economic Issues' in *International Monetary Fund; Legal Department; Current Developments in Monetary and Financial Law* (1999) (1).
7. Hameiri S and Jones L 'Regulatory Regionalism and Anti-Money Laundering in Asia' 69(2) *Australian Journal of International Affairs* (2015), available at <http://dx.doi.org/10.1080/10357718.2014.978737> (Accessed on 20 December 2016).
8. Ionescu L 'Money Laundering Directives and Corruption in the European Union', 4(2) *Contemporary Readings in Law and Social Justice* Volume (2012).



9. Kersop M and Du Toit S F 'Anti-Money Laundering and the Effective Use of Mobile Money in South Africa Pt (1)' 18(5) *Potchefstroom Electronic Law Journal* (2015).
10. Kersop M and Du Toit S F 'Anti-Money Laundering and the Effective Use of Mobile Money in South Africa Pt (2)' 18(5) *Potchefstroom Electronic Law Journal* (2015).
11. Kobor S E 'The Role of Anti-Money Laundering Law in Mobile Money Systems in Developing Countries', 8(3) *Washington Journal of Law, Technology and Arts* (2013).
12. Mas I and Radcliffe D 'Mobile Payments Go Viral: M-PESA in Kenya' in 32 *Journal of Financial Transformation* (2011).
13. McSkimming S 'Trade Based Money Laundering: Responding to an Emerging Threat' 15(1) *Deakin Law Review* (2010).
14. Nguyen C 'Criminalisation of Money Laundering in the International Anti-Money Laundering Regime and its Adoption by Vietnam' 14(1) *Australian Journal of Asian Law* 14(1) (2013).
15. Nkhoma G B 'Transnational Threats: The Problem of Illegal Immigration in Northern Malawi' 1(2) *Southern African Peace and Security Studies* (2012).
16. Serafini J 'Money Laundering' 41 *American Criminal Law Review* 887 (2004), available at <http://www.lexisnexis.com.ezproxy.uwc.ac.za/hottopics/lnacademic/?shr=t&csi=168966&sr=TITLE%28Money+Laundering%29+and+DATE+IS+2004> (accessed on 31 March 2016).



17. Sharman J C 'The Global Anti-Money Laundering Regime and Developing Countries: Damned if they Do, Damned if they Don't?' *Government and International Relations University of Sydney, NSW* (2006).
18. Stewart D P 'Internalising the War on Drugs: The UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances' *18 Denver Journal of International Law and Policies* (1990).
19. Unger B and Van Waarden F 'How to Dodge Drowning in Data? Rule- and Risk-Based Anti-Money Laundering Policies Compared' *5(2) Review of Law and Economics* (2009).

Electronic and Internet Sources

1. Airtel Money Cross Boarder Transfer, available at http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/malawi/airtel_money/home/airtel-money-cross-border, (Accessed on 16 April 2016).
2. Airtel Money Terms and Conditions, available at http://africa.airtel.com/wps/wcm/connect/AfricaRevamp/Malawi/Airtel_Money/Home/Personal/Terms-and-Conditions, (Accessed on 31 March, 2016).
3. Babu R R 'The United Nations Convention against Corruption: A Critical Overview', available at <http://ssrn.co/abstract=891898> (accessed on 11 September 2016).
4. Carr I & Goldby M *The UN Anti Corruption Convention and Money Laundering*. International Conference of the Institute of the International Economic Relations, Athens, Greece 6-7 September 2008 1, available at [idec.gr/iier/new/CORRUPTION CONFERENCE/The UN Anti-corruption convention and money laundering-INDIRA CARR.pdf](http://idec.gr/iier/new/CORRUPTION_CONFERENCE/The_UN_Anti-corruption_convention_and_money_laundering-INDIRA_CARR.pdf) (accessed on 11 September 2016).

5. Chatain P *et al* World Bank Working Paper No 146: Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing (2008), available at http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf, (Accessed on 11 January 2017).
6. GSMA, available at <http://www.m4dimpact.com/data/sectors/mobile-industry>, (Accessed on 11 January 2017).
7. Khiaonarong T 'Oversight Issues in Mobile Payments', IMF Working Paper 14/123 (2014) 18, available at <https://www.imf.org/external/pubs/ft/wp/2014/wp14123.pdf>, (Accessed on 10 January 2017).
8. Madise S 'Payment Systems and Mobile Money in Malawi: Towards Financial Inclusion and Financial Integrity', available at  https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2531319 (Accessed on 20 January 2017).
9. Makin P 'Regulatory Issues around Mobile Banking: *New initiatives to bank the poor are straining the world's financial regulatory systems*', available at <http://www.oecd.org/ict/4d/43631885.pdf>, (Accessed on 13 January 2017).
10. Mandiwa M 'Access to Financial Services in Malawi: Policies and Challenges', available at http://unctad.org/meetings/en/Presentation/ciem6_2014_Malawi_en.pdf_p6 (Accessed on 10 April 2016).

11. Marina S and Zerzan A 'Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks' GSMA DISCUSSION PAPER (2010), available at <https://www.ifc.org/wps/wcm/connect/3093368049585f389f52bf19583b6d16/7.3.i+GSMA+Methodology+Assessing+AML+Risk.pdf?MOD=AJPERES> (Accessed on 13 April 2016).
12. Mpamba Terms and Conditions available at <http://www.tnm.co.mw/index.php/tnm-mpamba.html>, (Accessed on 31 March 2016).
13. Merritt C 'Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments' Retail Payments Risk Forum White Paper Federal Reserve Bank of Atlanta (2010)
14. Schott P A (2006) Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: Second Edition and Supplement on Special Recommendation IX. Washington, DC: World Bank, available at <https://openknowledge.worldbank.org/handle/10986/6977> (Accessed 28 September 2016).
15. Van Duyne P C 'Money laundering policy'. Fears and Facts (2003) 69, available at <http://petrusvanduyne.nl/files/Witwassen%20Fears%20and%20Facts.pdf> (Accessed on 23 September 2016).
16. Williams I 'Regulatory frameworks and Implementation patterns for Mobile Money in Africa: The case of Kenya, Ghana and Nigeria' (2013) 4, available at http://s3.amazonaws.com/academia.edu.documents/42068100/Regulatory_framework

[orks and Implementation20160204-17000-9tcws1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1485341002&Signature=27kgM3ORPY4%2Fc5Nuz7NYo81gm44%3D&response-content-disposition=inline%3B%20filename%3DRegulatory_frameworks_and_Implementatio](#)
[n.pdf](#) (Accessed on 17 January 2017).

Newspaper Articles

Hughes N 'UK donates \$11M to help Malawi launch national ID card', available at <https://oneworldidentity.com/2016/10/27/uk-donates-11m-to-help-malawi-launch-national-id-card/>, (Accessed 11 December 2016).





UNIVERSITY *of the*
WESTERN CAPE