

**TOWARDS ANTI-MONEY LAUNDERING LEGISLATION IN KENYA: A
Case Study of the Mobile Telephony Money Transfer System**

**A Dissertation Submitted in Partial Fulfillment of the Requirement for the Bachelor of
Laws Degree LL.B.Submitted to the University of Nairobi, School of Law**

By

EVETTE ACHIENG OCHODO

G34/1887/2006

**UNIVERSITY OF NAIROBI LIBRARY
P. O. Box 30197
NAIROBI**

Supervisor:

William Musyoka

2010

TABLE OF CONTENTS

| | |
|--|------|
| Declaration..... | ii |
| Dedication..... | iii |
| Acknowledgement..... | iv |
| List of Abbreviations..... | viii |
| List of Cases..... | ix |
| List of Statutes & Treaties..... | x |
| | |
| 1.0 CHAPTER ONE: INTRODUCTION | |
| 1.1 Introduction..... | 1 |
| 1.2 Background..... | 1 |
| 1.3 Statement of the Problem..... | 2 |
| 1.4 Research Questions..... | 5 |
| 1.5 Research Justifications..... | 6 |
| 1.6 Theoretical Framework..... | 6 |
| 1.6.1 Reward-Risk Model of Criminal Behaviour..... | 6 |
| 1.7 Conceptual framework..... | 8 |
| 1.7.1 Concept of Money Laundering..... | 8 |
| 1.7.2 Concept of Money Transfer..... | 10 |
| 1.7.3 Anti Money Laundering Regulation of Mobile Money Transfer..... | 12 |
| 1.8 Literature Review..... | 16 |
| 1.8.1 Defining Money Laundering..... | 16 |
| 1.8.2 Effects of Money Laundering..... | 17 |
| 1.8.3 Regulation of Money Laundering & Emerging Technologies..... | 18 |
| 1.9 Research Methodology..... | 20 |
| 1.10 Summary of Chapters..... | 20 |
| | |
| 2.0 CHAPTER TWO: THE MONEY LAUNDERING LEGAL FRAMEWORK | |
| 2.1 Introduction..... | 22 |
| 2.2 Definition of Money Laundering..... | 22 |
| 2.2.1 Principal Offenders..... | 24 |
| 2.2.2 Mobile Telephone Operators..... | 24 |
| 2.2.3 Shortcomings of Section 8..... | 25 |
| 2.2.4 Inchoate offences..... | 26 |
| 2.3 Definition of Predicate Offences..... | 26 |
| 2.3.1 Recommendation..... | 29 |
| 2.4 Reporting Institutions..... | 29 |
| 2.4.1 Recommendation..... | 31 |
| 2.5 Customer Due Diligence & Record Keeping..... | 32 |
| 2.5.1 Recommendation..... | 35 |
| 2.6 Supervision & Enforcement Agencies..... | 36 |
| 2.6.1 Recommendation..... | 37 |
| | |
| 3.0 CHAPTER THREE: MOBILE MONEY TRANSFER BUSINESS MODELS | |
| 3.1 Introduction..... | 38 |
| 3.2 Business Models..... | 38 |

| | | |
|------------|---|----|
| 3.2.1 | Bank- Based Model..... | 38 |
| 3.2.2 | Non-Bank Based Model..... | 40 |
| 3.3 | Rationale For The Trust Accounts and Central Bank's Role..... | 42 |
| 4.0 | CHAPTER FOUR: FACTORS AFFECTING THE SUCCESSFUL PROSECUTION OF MONEY LAUNDERING AS AN OFFENCE | |
| 4.1 | Introduction..... | 45 |
| 4.2 | Offences..... | 45 |
| 4.2.1 | Money Laundering..... | 45 |
| 4.2.1.1 | Knowledge of illegal proceeds..... | 46 |
| 4.2.1.2 | Proceeds of crime..... | 48 |
| 4.2.2 | Failure to Report Suspicious Transactions..... | 48 |
| 4.2.3 | Tipping Off, Misrepresentation and Malicious Reporting..... | 48 |
| 4.2.4 | Failure to establish and maintain customer records and failure To verify customer identity..... | 49 |
| 4.3 | Criminal and Civil Asset Forfeiture..... | 49 |
| 4.4 | International Cooperation..... | 50 |
| 4.5 | Intra-Agency and Inter-Agency Co-ordination..... | 51 |
| 4.6 | Impediments to Successful Prosecution..... | 52 |
| 4.6.1 | Prosecutorial Powers vest in Attorney General..... | 52 |
| 4.6.2 | Differentiating between 'clean' and 'dirty' money..... | 54 |
| 4.6.3 | Trust Companies/Trust Account Holders..... | 54 |
| 4.6.4 | Lack of Universal Criminalization of Money Laundering..... | 55 |
| 4.6.5 | Corruption and Overlap with the Anti Corruption and Economic Crimes Act 2003..... | 55 |
| 4.6.6 | False Identities..... | 56 |
| 5.0 | CHAPTER FIVE: SUMMARY OF FINDINGS AND RECOMMENDATIONS | |
| 5.1 | Introduction..... | 57 |
| 5.2 | Findings..... | 57 |
| 5.3 | Recommendations..... | 58 |
| 5.3.1 | Establish a Supreme Financial Regulator..... | 58 |
| 5.3.2 | Introduction of Risk Based Customer Due Diligence..... | 60 |
| 5.3.3 | Directive on Predicate Offences..... | 60 |
| 5.3.4 | Granting Prosecutorial Powers to an Independent Body..... | 60 |
| 5.3.5 | Tougher Transaction Monitoring and Reporting Guidelines..... | 60 |
| 5.3.5.1 | Transaction Volume..... | 61 |
| 5.3.5.2 | Transaction Velocity..... | 61 |
| 5.3.6 | Inclusion of Trust Account Holders/Trust Companies as Reporting Institutions..... | 61 |
| 5.3.7 | Omission or Amendment of Section 8..... | 62 |
| 5.3.8 | Clarification of Overlap with Anti-Corruption Legislation..... | 62 |
| 5.3.9 | AML Training for law Enforcement Agencies..... | 63 |
| 5.3.10 | Customer Identification System..... | 63 |
| 5.3.11 | Provision for Inchoate Offences..... | 64 |

LIST OF CASES

Da Silva [2006] EWCA Crim 1654, 11/7/06

Jopley Constantine Oyieng v Republic Criminal Appeal Number 45 of 1988

Manifest Shipping v Uni-Polaris [2001] UKHL 1

R v Saik [2006] 2 W.L.R. 993, HL

R v Rollins [2009] EWCA Crim 1941

R v McInerney [2009] WLR (D) 294

Richard Kimani and M Maina v Nathan Kahara High Court criminal (revision) case number 11 of 1983

LIST OF STATUTES AND TREATIES

Kenyan Legislation

Anti Corruption and Economic Crimes Act 2003

Banking Act CAP 488 Laws of Kenya

Central Bank of Kenya Act

Central Bank of Kenya Prudential Guidelines on Proceeds of Crime and Money Laundering (Prevention)

Narcotics and Psychotropic Substances (Control) Act No.4 of 1994

Mutual Legal Assistance Bill

Proceeds of Crime and Anti Money Laundering Act 2009

International Treaties

European Communities Convention on Laundering, Search Seizure and Confiscation of the Proceeds from Crime

UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (i.e the Vienna Convention) of 1988

United Nations Convention Against Corruption (UNCAC)

Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime i.e. the Strasbourg Convention

UK Legislation

Money Laundering Regulations 2007(the Third Regulations) of the United Kingdom (UK,)

Proceeds of Crime Act 2002 (POCA)

Financial Services and Markets Act 2000 (FSMA)

South African Legislation

Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (RICA),

1.0 CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

Mobile money transfer has made a significant contribution to the Kenyan economy and has neutralized the monopoly enjoyed by banks and other remittance agencies in so far as remittances and payments are concerned. Mobile money transfer has revolutionized how business is carried out in Kenya thus regulation is paramount. Furthermore, the fact that mobile money transfer is a key enabler of financial services exposes it to the risk of money laundering.

It is therefore extremely essential to ensure that adequate anti-money laundering laws are enacted and enforced to ensure that the gains achieved by mobile money transfer are not lost.

1.2 BACKGROUND

Money transfer has been practiced since money came into existence. Initially money transfer took place through personal delivery of the money to the recipients. As time moved on money remittances were done by post offices due to their wide distribution networks. However this process was too slow. As time progressed, banks and specialized money transfer agencies such as Western Union began offering money transfer services. In as much as these services are faster, banks do not have a wide distribution network and as such a large number of the world's population can be categorized as "unbanked"

With the dawn of mobile telecommunication services, mobile service providers have been able to build an extremely wide distribution network. Mobile phone penetration is growing faster than the traditional banking infrastructure such as branches and automated teller machines (ATMs)¹. Today, mobile operators have the largest distribution network in any developing economy and hence are in a better position to remit money from one location to another². According to the Global System for Mobile Communications (GSM) Association, fewer than 1 billion out of 6.5 billion people worldwide have bank accounts.

¹ PPT: Sonia Arenaza: End User Benefits Enabled Applications to Financial Services: Regulatory Policies on Universal Access. 8th September, ITU Geneva

² www.mobilein.com/MobileMoneyTransfer

At the same time, the penetration of mobile subscribers in emerging markets is increasing rapidly – with 85% of the next billion subscribers expected to come from areas such as Africa, Latin America and East Asia³.

Due to the increasing penetration of mobile phones, mobile payment schemes could bring formal financial services to the “unbanked.”⁴ Consequently, there is a convergence of telecommunications and financial services. The mobile handset is becoming a key enabler in financial services. Thus many entities with a global development focus have turned to the mobile phone as a potential platform for delivering development services⁵.

Kenya has not been left behind in offering mobile money transfer services. Currently, three out of the four mobile network operators in the country offer the service. Safaricom’s service popularly known as M-Pesa was launched in March 2007 and now has over 7 million subscribers. Zain’s service is known as Zap while the most recent entrant is called yuCash by Obopay which is a service offered by Essar Telecom Kenya which operates under the brand Yu, in conjunction with Obopay. In addition, mobile money transfer services are being used to make utility payments. For example, in Kenya, mobile payments (m-payments) for electricity, water, cable television bills among other bills can be paid via M-Pesa or Zap

1.3 STATEMENT OF THE PROBLEM

Mobile money transfer (MMT) is a recent technological development in Kenya and globally that has revolutionized the provision of financial services. Due to the wide distribution network that mobile network operators have, this service has reached people who ordinarily do not have access to the conventional financial services. However, just like any other financial service, mobile money transfer is susceptible to misuse by criminals for money laundering and terrorist financing. When mobile network operators (MNO) decide to offer mobile money transfer (MMT) services, they are first confronted

³ http://www.gsmworld.com/our-work/mobile_lifestyle/mobile_money/mobile_money_transfer/index.htm

⁴ Indran Medhi, S.N Nagasema Gaulana, Kentara Toyama: A Comparison of MMT Uiss for Non-Literate and Semi Literate Users

⁵ Donne J, Research Approaches to Mobile Use in the Developing World: A Review of the Literature. *The Information Society* 24(3)2008

with Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) regulation. It applies mostly in situations where cash is paid in or out as part of an MMT service⁶.

The vulnerability of financial systems has been recognized globally. In fact, the United Nations Security Council passed *Resolution 1617* United Nation under Chapter VII of the UN Charter and therefore binding on all member countries. Resolution 1617 'Strongly urges all Member States to implement the comprehensive, international standards embodied in the FATF Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing. In addition, the European Commission issued *Directive 2005/60/EC* of the European Parliament and of the Council of October 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. This directive applies to member states of the European Union.

At present the regulatory framework for the provision of the MMT service is at its infant stage and is therefore easy to manipulate. With regard to money laundering, the Kenyan parliament recently enacted the Proceeds of Crime and Anti Money Laundering Act 2009. However, questions are still being raised if this law accommodates mobile money transfer considering its peculiar features.

The future of mobile money transfer is dependent on the regulatory environment in various countries. According to William Gilmore⁷ in *Money laundering: the international aspect* there is a need to strengthen both criminal and financial laws He asserts "Out of the (increasing recognition of the negative impact which vast flows of dirty money can have on the financial sector) a twin track solution to the problem has gradually emerged. On the one hand it calls for the strengthening of the criminal law since it is widely acknowledged that the principal burden must be carried by invoking

⁶ GSM A ssociation: An introduction to the MMT Regulatory Environment PDF Document

⁷ William C Gilmore, "Money laundering: the international aspect", in David Hume Institute, *Money Laundering* (Hume papers on Public Policy, vol 1, No 2) Edinburgh, Edinburgh University Press, 1993, 1 at 2

penal means. On the other hand, it is now generally accepted that the financial system can and must play an effective preventative role.”

Therefore, whereas mobile money transfer is making an effective contribution to the economy, if it is discovered that it is being used for money laundering, this may result in either the cessation of the service or introduction of extremely stringent regulations which could hurt the growth of the service and destroy the gains attained by the use of the service by the “unbanked.” Therefore, effective regulations and controls must be put in place to prevent and detect money laundering.

Until recently, the only Kenyan statute that addressed money laundering is the Narcotics and Psychotropic Substances (Control) Act No.4 of 1994⁸. However, this Act only dealt with the proceeds of crime. It did not make provisions for the prevention and detection of money laundering activities. Furthermore, this Act only applied in so far as the proceeds of crime related to narcotics trafficking and related offences as stipulated by the Act. Therefore, proceeds from crimes such as Illegal arms sales, smuggling, computer fraud among others which can be laundered using mobile money transfer and other financial services were not regulated under the Act.

Whilst complying with anti-money laundering (AML) regulation is standard practice for banks, these rules are not something mobile operators are traditionally familiar with. The Central Bank of Kenya (CBK) has Prudential Guidelines which apply to all banks and financial institutions operating in Kenya. These guidelines were made pursuant to Section 33 of the CBK Act which empowers the bank to enact regulations that apply to all financial institutions. These guidelines require these institutions to adhere to strict guidelines on customer due diligence (CDD), Know Your Customer (KYC) and Anti-money laundering regulations.

The CBK Guidelines on Prevention of Money Laundering make money laundering a criminal offense. The only problem with these regulations is that in as much as they are

⁸ Section 49

meant to apply to all financial institutions, they are tailor made for the banking industry yet the risks that affect banks and mobile money transfer services are different. The risks that attach to mobile money transfer operators are of a lower threshold as compared to the risks that attach to banks. Therefore it is not fair to subject mobile operators to the same stringent regulations. There is an urgent need for proportionate risk based regulations.

In addition there is confusion on the rightful regulatory authority for mobile money transfer services. Since mobile money transfer is a convergence of telecommunications and financial services, which existing regulatory authority between the Communications Commission of Kenya (CCK) and the Central Bank of Kenya (CBK) is the supreme authority?

The vacuum in regulating money laundering in Kenya necessitated the government to draft legislation. Consequently, the Proceeds of Crime and Anti-Money Laundering Act, 2009 was passed by Parliament in December 2009. The Act applies to all financial institutions. Mobile network operators that provide mobile money transfer services are financial institutions within the meaning of reporting institutions provided for by the Act. The Act also introduces the concept of E-money and establishes a regulatory body among other provisions.

1.4 RESEARCH QUESTIONS

1. Does the Proceeds of Crime and Anti- Money Laundering Act adequately regulate money laundering activities in the mobile money transfer services?
2. Can the current Kenyan banking laws and regulations be adopted for mobile money transfer services?
3. Is there a need to establish a body mandated to regulate mobile money transfer services?
4. What are the impediments to the prosecution of money laundering and related crimes? And does the proposed law provide any remedies?

1.5 RESEARCH JUSTIFICATIONS

Money laundering poses one of the biggest threats to the integrity and credibility of financial systems worldwide. Consequently due to the significant contribution that mobile money transfer services have made to the ‘unbanked’ population, it is extremely important to ensure that the gains attained by the service are not watered down through money laundering activities.

Accordingly, this study seeks to establish how effective the recently enacted Proceeds of Crime and Anti Money Laundering Act, 2009 is in regulating mobile money transfer considering that it is a recent technological development in financial services and that the transactions involved are not the conventional transactions regulated by traditional anti money laundering legislation.

Furthermore, due to the transnational nature of money laundering and the introduction of cross border mobile money transfer by various service providers, mobile money transfer services are further exposed to higher risks of money laundering. Considering that countries have different AML laws, conflicts between the laws could affect the regulation and enforcement of the Kenyan AML law.

1.6 THEORETICAL FRAMEWORK

1.6.1 Reward-Risk Models of Criminal Behaviour

In *Crime and Human Nature*⁹, political scientist James Q Wilson and psychologist Richard Herrnstein claim that people choose preferred courses of action and that their behaviour is governed by its consequences. They argue that if the rewards of crime are great and its risks small and if the rewards of a non criminal way of life are comparatively small and its risks relatively great people will choose to violate the law. Accordingly, with respect to money laundering, the rewards run into billions of dollars for successful launderers.

⁹ James Q Wilson and Richard J Hernstein. *Crime and Human Nature*. New York: Simon and Schuster, 1985

The International Monetary Fund(IMF) (2003,2001), and the World Bank estimate that 2-4% of the world's gross domestic product (GDP) stems from illicit (criminal) sources or from money laundering activities. With such returns it is no wonder that many individuals globally are willing to risk the stringent anti-money laundering legislations in order to achieve their objectives. According to Wilson and Herrnstein (1985:44), "The larger the ratio of net rewards of crime to the net rewards of non-crime, the greater the tendency to commit crime."

The reward-risk model can trace its origin to the classical school of thought which stressed the role of reason and free-will in human affairs. According to Jeremy Bentham¹⁰, in *The Principles of Morals* "the principal control over the unfettered exercise of free will is fear of pain. That punishment is the chief way of creating fear in order to influence the will and thus control behaviour." This position was supported by Beccaria Cesare, a protest writer who in his book *Crime and Punishment*¹¹, stated that punishment should be:

- 1 Proportionate to the harm done
- 2 Should not be too severe so as to lose the good and thus become tyrannical
- 3 Prompt
- 4 Certain

It is based on such arguments that the Proceeds of Crime and Anti Money Laundering Act 2009 was enacted. As Ringguth pointedly observes in *Money Laundering- The Criminal Dimension*¹², "if you can take the profit motive out of acquisitive crime, then that is a positive way of tackling criminality generally." The Act provides for various penalties for different offences. These penalties are meant to be proportionate to the offence committed. For example failing to report suspicion regarding the proceeds of crime carries a different penalty from malicious reporting¹³. Therefore, whereas a natural person guilty of failing to report his suspicion regarding proceeds of crime is liable to

¹⁰ Jeremy Bentham. *The Principles of Morals & Legislation* (1789) Ch1. p.1

¹¹ Cesare Beccaria, *Of Crimes and Punishment*, R. Bell MDCCLXXVIII (1778)

¹² Ringguth J, Money Laundering-The Criminal Dimension, Paper presented at the "Stop Money Laundering" Conference, 26 February 2002 London

¹³ Section 6

imprisonment of a term not exceeding seven years or a fine not exceeding two million or both, a natural person guilty of malicious reporting is liable to an imprisonment term not exceeding two years or a fine not exceeding one million or to both. In addition, there are different penalties for natural and fictitious persons.

1.7 CONCEPTUAL FRAMEWORK

1.7.1 Concept of Money Laundering

Money laundering is the “process by which one conceals the existence, illegal service or illegal application of income and then disguises that income to make it appear legitimate.”¹⁴ Simply put money laundering is the process of “cleaning up dirty money. The money is “cleaned” or laundered through legitimate means and as a result the proceeds lose their existing criminal identity and appear to have originated from a legitimate source¹⁵.

An even broader definition of money laundering includes the fact that criminals use this process to further criminal activities. Accordingly, money laundering consists of “All activities to disguise or conceal the nature, source of, or entitlement to money or property, or rights to either, when the money or property or rights are acquired from serious crime, as well as all activities to disguise or conceal money or property that is intended to be used in committing or facilitating the commission of serious crime¹⁶. This is captured in Article 1 of the 1990 *European Communities Convention on Laundering, Search Seizure and Confiscation of the Proceeds from Crime* defines money laundering as “ The conversion or transfer of property knowing that such property is derived from serious crime for the purpose of concealing or illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action and the concealment or disguising of the true nature, source,

¹⁴ President’s Commission on Organized Crime, *The Cash Connection, Organized Crime, Financial Institutions and Money Laundering* 7(1984)

¹⁵ www.iba

¹⁶ George Kegoro, “Profiling Money Laundering in Eastern and Southern Africa,” an Overview of Capacity: Volume One Chapter 5 “Money laundering Patterns in Kenya, , Institute for Security Studies Monograph 90

location, disposition, movement rights with respect to or ownership of property knowing that such property is derived from serious crime.”

The proceeds of money laundering can be used to facilitate organized crimes such as drug trafficking, arms smuggling, corruption. Among the key factors that have contributed to money laundering in Kenya are corruption and a poor record of law enforcement.

Money laundering is carried out in the following ways¹⁷.

1. Smurfing: this involves the use of multiple cash deposits each smaller than the minimum cash reporting requirement.
2. Misinvoking of exports and falsification of import letters of credit and customs declaration can conceal cross-border transfers say the proceeds of drug trafficking
3. Barter: stolen property (e.g. antiques) can be exchanged across national borders or domestically for illegal substances
4. Parallel credit transactions can be used to avoid the formal economy except for the final use made of the net proceeds of illegal activity to purchase legally marketed goods or services
5. Inter-bank wire transfers may not be subject to reporting on money laundering, bribery of bank officials can thus make it easier to conceal large illegal transfers between accounts
6. Derivatives that replicate insider trading opportunities (e.g. a synthetic version of a company stock subject to merger or take over) can be used to avoid detection of an unusual change in a listed stock price.

Money laundering affects every business or institution that handles money. Banks, insurance companies, real estate agents, stock brokerage firms are just a few examples of institutions that are affected by money laundering. Added to this list are mobile network operators that offer mobile money transfer. Mobile money transfer involves the remittance of money from one person to another through a mobile telephone. When

¹⁷ Peter J Quirk: Money Laundering- Mudding the Macroeconomy: *Finance & Development* 1997

mobile network operators engage in mobile money transfer they expose themselves to the risk of money laundering and terrorist financing.

Increased international efforts to criminalize money laundering have placed increased regulatory burdens on commercial banks and other financial institutions which are then passed on to consumers through higher fees or lower interest rates.

There is growing concern about money laundering and terrorist financing as the world views the effects of these criminal activities on the integrity and functioning of financial systems, good governance, financial stability and economic development¹⁸. One major organization that has steered the development and implementation of anti-money laundering and counter –terrorist financing legislation is the Financial Action Task Force. FATF¹⁹

The Financial Action Task Force (FATF) has focused its anti-money laundering legislation efforts on financial institutions because of the ease with which criminal groups have used financial institutions to transmit the proceeds of their illicit activities and because of the threat that money laundering poses to the systemic stability of financial systems²⁰.

1.7.2 Concept of Mobile Money Transfer

Mobile money transfer refers to services whereby customers use their mobile device to send and receive monetary value—or more simply put, to transfer money electronically from one person to another using a mobile phone. Both domestic transfers as well as international or cross-border, remittances are money transfer services²¹.

Mobile phone based financial services have proved to be an important vehicle in promoting financial inclusion in developing countries where a large segment of the

¹⁸ <http://www.worldbank.org/amlcft>

¹⁹ FATF is an intergovernmental body which sets standards and develops and promotes policies to combat money laundering and terrorist financing. <http://www.fatf-gafi.org>

²⁰ FATF-VIII Money Laundering Typologies Exercise Public Report, Organization for Economic Co-operation and Development (OECD) 5 February 1997

²¹

population is either un-banked or under-banked. The un-banked people are those without formal bank accounts who operate in a cash economy²². In developing countries, the mobile handset provides the un-banked segment of the population the potential to access all types of financial services; transactional and informational²³. Mobile money transfer therefore makes a significant contribution to economic growth. Accordingly, all necessary steps must be taken to minimize money laundering which has devastating economic consequences. Fighting it should be a priority for all countries and is not incompatible with financial market liberalization²⁴

The growth of mobile money transfer has been spurred on by several factors some of which include: ease of use and mobility. This is the mobile experience²⁵. Mobile money transfer has made the money transfer market more competitive and the mobile phone has offered an alternative, convenient and cheaper way to remit money almost instantly in the palm of your hand. Traditionally, banks and other remittance institutions have charged high commission rates and at times bank to bank transfers could take more than a day²⁶. Thus mobile money transfer has revolutionized the whole system of cash remittances.

In addition, the high penetration of mobile telecommunication services and the increased migrant remittances have also significantly contributed to the success of mobile money transfer. There were over 3.3 billion phone users in 2007²⁷ and close to 60% subscribers live in developing countries²⁸. Thus, many entities with a global development focus have turned to the mobile phone as a potential platform for delivering development services.²⁹ Mobile money transfer enables migrant workers to send money home at lower transactional costs than traditional money transfer services and enable friends and family

²² Porteous D "The Enabling Environment for Mobile Banking in Africa, London :DFID (2006)

²³ Address by Prof. Njuguna Ndung'u, Governor of the Central Bank of Kenya at the official launch of the International Money Transfer Service, Nairobi, 13th October, 2009.

²⁴ Peter J Quirk: Money Laundering- Mudding the Macroeconomy: *Finance & Development* 1997

²⁵ www.gsmworld.org/mmt

²⁶ www.mobile-money-transfer.com/globalsummit

²⁷ ITU ICT Eye <http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx>

?ReportName=WTI/CellularSubscribersPublic & RP_intYear=2007&RP_intLanguageID=1

²⁸ UNCTAD, Information Economy Report 2007-2008 Science & Technology for Development. The New Paradigm of ICT, Geneva: United Nations Conference on Trade & Development 2008.

²⁹ Donne J. Research Approaches to Mobile Use in the Developing World: A Review of the Literature. *The Information Society* 24(3) (2008)

at home and without bank accounts to access the money. The World Bank estimates that recorded remittances by some 200 million migrants from developing countries reached US\$ 283 billion up from US\$240 in 2007³⁰.

The rapid growth of mobile money transfer has therefore necessitated the need to establish a regulatory framework for the service. In particular there is an urgent need for anti-money laundering (AML) and counter-terrorism financing (CFT) regulation.

1.7.3 Anti Money Laundering Regulation of Mobile Money Transfer

Money-laundering poses one of the biggest threats to the financial sector: it not only economically destabilizes an economy but also exposes it to terrorist attacks, threatening the integrity and sovereignty of the nations concerned. It conceals the huge, illegal profits generated by unscrupulous organized criminal groups in various fields of crime. Due to the serious effects of money laundering there has been a significant growth in enacting legislation both at the national and international level to regulate financial services.

As a general rule, the more a mobile network operator becomes involved in the provision of financial services, the heavier the burden of financial regulation. This is because any weaknesses in the provision of financial services are prone to exploitation by criminals who can use the systems to engage in money laundering and terrorist financing. It is worth noting that mobile money transfer has made a significant contribution in ensuring access to financial services by persons who have been traditionally excluded by banks. Consequently, this has spurred on economic growth. It is therefore imperative that the gains brought about by mobile money transfer services are not eroded thus denying those who need the service access to it. Accordingly, the future of mobile money transfer will greatly depend on regulation.

A risk-based approach by financial regulators with regard to regulation of MMT services is crucial for the up take of MMT services. This is because the business model for MMT

³⁰ http://siteresources.worldbank.org/INTROSPECTS/Resources/334934-1110315015165/MD_Brief5.pdf

services is based on high volumes of low value transactions thus the thresholds of risks for MMT are lower than that of banks and other financial institutions.

The anti money laundering legislation in Kenya does not adequately cater for mobile money transfer. This is because apart from being a new technology, experts have not been able to satisfactorily decide whether MMT can be categorized as deposit taking institution within the meaning of the Banking Act Cap 489 Laws of Kenya. If indeed MMT could fall under a deposit taking institution, then it would be deemed to be banking business thus the AML, Know Your Customer (KYC) and Customer Due Diligence(CDD) regulations applicable to banks would easily have been extended to mobile network operators offering mobile money transfer services.

The situation is a bit more complex. Mobile network operators have circumvented the application of the Banking Act by establishing trusts and appoint trustees to manage the funds. Bank accounts in the names of the trustees are opened with licensed banks in Kenya and the funds are held in trust for customers of the mobile companies³¹. Therefore in essence, the money is never received by or paid to the order of the mobile network operator. The mobile network operator only provides the technical services to facilitate transfer of funds and is never at any time a custodian of the funds.

At the international level, the first significant piece of anti money laundering legislation is the *UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (i.e the Vienna Convention) of 1988*. The purpose of the Convention as provided under Article 2(1) is to provide co-operation among the contracting states so that they may address more effectively the aspects of illicit traffic in narcotic drugs and psychotropic substances having an international dimension. The convention required states to criminalize money laundering, to co-operate in money laundering investigations and related proceedings and to pass laws facilitating the tracing, seizing and forfeiture of proceeds of crime. It is on these grounds that Baldwin and Munroe in *Money Laundering*

³¹ Anne Kiunuhe: Business Daily, *Mobile Banking Laws Should not Restrict Capital Inflows* Wednesday December 30th 2009

*Asset Forfeiture and International Crimes*³² remarked that “the convention established a basis for placing international controls on money laundering thus setting the standard for international anti money laundering efforts.”

Other developments were by the *Basle Committee*³³ and by the *Financial Action Task Force (FATF)*. The Basle Committee is a supervisory body for the banking industry which exists in order to improve banking supervision and strengthen prudential standards in member and increasingly non-member countries.. The Basle Committee established the Basle principles (*Statement of Principles on the prevention of the criminal use of the banking system for the purpose of money laundering*) which suggest policies and procedures in four areas to curb money laundering. They include:

1. customer identification
2. compliance with law
3. co-operation with law enforcement agencies
4. Adherence to the statement.

The FATF established 40 recommendations and 9 special recommendations that deal with counter terrorist financing (40+9). The 40 recommendations and the greater co-ordinating ability of the FATF superseded the statement. The FATF is the primary international coordinator for strengthening anti-money laundering laws. The FATF aims to develop and promote policies to combat money laundering policy nationally and internationally. The 40 recommendations call on countries to criminalize money laundering (not just its predicate acts), to enact legislation that prioritizes law enforcement over bank secrecy and to require their financial institutions to implement anti money laundering controls. In addition, financial institutions are obliged to file suspicious activity reports with a regulator if the movement of funds by their clients raises reasonable questions as to their legitimacy.

³² Fletcher N Baldwin, Jr & Robert J Munroe, eds *Money launderers, asset forfeiture and international financial crimes* (3 vols), New York: Oceana Publications, 1993

³³ Consists of representatives from central banks and supervisory authorities of the G-10 group of industrialized nations.

According to the GSM Association the main anti-money laundering obligations for financial institutions and designated non-financial institutions include:

1. Identification Procedures (provide satisfactory evidence of identity of customers, take into account the greater risk of money laundering when customer is not physically present when identified)
2. Record Keeping Procedures (keep copy of identification data for at least 5 years on record) ; money service operator has to register with the relevant authority (this in turn gives the authority the power to inspect the premises, order access to recorded information and to impose penalties)
3. Systems & Training to prevent money laundering (train employees establish procedures of internal control and communication which are appropriate to prevent money laundering)

Until recently, the anti-money laundering legislation in Kenya was not comprehensive. The only laws that dealt with money laundering were the Narcotic Drugs and Psychotropic Substances (Control) Act No. 4 of 1994 which dealt with the proceeds of drug trafficking activities and the Central Bank of Kenya Prudential Guidelines on Proceeds of Crime and Money Laundering (Prevention) which are not comprehensive enough as they were drafted while having the banking industry in mind. The guidelines were enacted pursuant to Section 33 of the CBK Act and therefore have the force of law,

This gap in legislation prompted the Kenyan government to enact the Proceeds of Crime and Anti-Money Laundering Act (2009). This Act complies with the FATF 40+9 special recommendations that provide measures for combating money laundering and terrorist financing. The recommendations set the minimum standards of compliance and cover all the measures that national systems should have in place within their criminal justice and regulatory systems, the preventive measures to be taken by financial institutions and certain other businesses and professions and international co-operation³⁴. The provisions of the Proceeds of Crime and Anti Money laundering Act will be analyzed in greater detail in subsequent chapters.

www.fatf-gafi.org/fatfrecommendations.pdf

1.8 LITERATURE REVIEW

1.8.1 Defining Money Laundering

The way in which money laundering is defined will have a significant impact on the regulation of money laundering.

According to Elena Madalina Busuioc³⁵ *Predicate Offences –The Achilles’ Heel of Anti-Money Laundering Legislation*, From a legal point of view, the Achilles’ heel in defining and criminalizing money laundering relates to the so called ‘predicate offences’ understood as the criminal offences which generated the proceeds thus making laundering necessary. Hiding or disguising the source of certain proceeds will of course not amount to money laundering unless these proceeds were obtained from a criminal activity (i.e. predicate crime). For example in Germany tax evasion is not a predicate offence to money laundering while in Greece and Switzerland, tax evasion is not even a crime and therefore, the hiding or concealing of such proceeds does not amount to money laundering because the first requirement of the crime of money laundering, the criminal origin of the proceeds is not met.

However, for purposes of this study, money laundering as defined by Shantamu Jugtawat in *Money Laundering- To Disguise its illegal Origin*³⁶ refers to the practice of moving illegally acquired cash through financial and other systems so that it appears to be legally acquired. This definition is also contained In *Blacks Law of Lexicon* where the term laundering is referred to as investment or other transfer of money flowing from racketeering , drug transactions, and other sources (illegal sources) into legitimate channels so that its original source cannot be traced.

Money laundering is difficult to discover, investigate and prosecute, thus allowing vast sums of ill gotten gains to move through the international financial system without fear of

³⁵ Elena Madalina Busuioc, *Predicate Offences- The Achilles Heel of Anti-Money Laundering Legislation*, ” Chapter 2 in Brigette Unger *The Scale and Impacts of Money Laundering*.” Edward Elgar Cheltenham, UK. Northampton, MA, USA 2007

³⁶ Shantamu Jagtawat, “*Money laundering-To disguise its illegal origin*,” National Law Institute University

retribution by the wrongdoers.³⁷The process of money laundering involves three stages: placement, Layering and Integration. The UN General Assembly³⁸ defines these stages as follows:

Placement: the initial entry of funds into the financial system serves the purpose of relieving the holder of large amounts of actual cash and positioning these funds in the financial system for the next stage. Placement is the most vulnerable stage of the process as the chance of discovery of the illicit origin of the money is greatest at the beginning.

Layering: this is the next stage. It describes a series of transactions designed to conceal the money's origin. At this level, money is often sent from one country to another and then broken up into a variety of investments which are moved frequently to evade detection.

Integration: This is the final stage. At this stage funds have been fully assimilated into the legal economy where they can be used for any purpose.

1.8.2 Effects of Money Laundering

Money laundering has significant short-term and long-term negative economic effects. A conservative estimate puts the figures at between 2% to 4% of the Global Gross Domestic Product (GDP). That translates to between US \$ 500 billion and US\$1 trillion³⁹. John McDowell and Gary Novis in *Economic Perspectives*⁴⁰ state that money laundering presents the world community with a complex and dynamic challenge. They believe that the nature of the problem calls for global standards and international cooperation to

³⁷ Dept of Treasury(Treasury) The National Money Laundering Strategy for 2000, (March 2000), at <http://www.treas.gov/press/releases/docs/ml2000.pdf>

³⁸ UN General Assembly, *Special Session on the World Drug Problem*, Fact Sheet 5: Money Laundering (June 8-10,1998) available at <http://www.un.org/ga/2ospecial/presskit/themes/moeny-5.htm>

³⁹ www.cgd.com The CGD Bills Digest/July 2007

⁴⁰ John McDowell & Gary Novis, "The Consequences of Money Laundering & Financial Crime," *Economic Perspective, an IIP Electronic Journal*(May 2001)

reduce the ability of criminals to launder their proceeds and carry out their criminal activities.

In order to capture the magnitude of the negative effects caused by money laundering, the US Money Laundering Strategy 2000⁴¹ lists the following negative consequences.

1. undermining public trust in the integrity of financial institutions
2. posing a challenge to the legitimate authority of national governments
3. corrupting officials and professionals
4. facilitating the looting of national treasures and IMF/World Bank funds of capital poor developing countries
5. Creating an inherent danger to the financial and economic stability of nations
6. Diminishing the efficiency of global interest rate markets
7. causing a routine violation of legal norms, property rights and human rights
8. Facilitating other crimes such as drug trafficking, tax evasion, bribery and terrorism.

It is these negative consequences that have necessitated both international and national regulation to stem the growth of money laundering.

1.8.3 Regulation of Money Laundering and Emerging Technologies

It is worth noting that available literature on money laundering and its regulation have primarily focused on traditional forms of money laundering. There is very little if any literature on regulating money laundering through emerging technologies such as mobile money transfer.

Both authorities and the money launderer seem to permanently change their behavior when trying to hunt and escape money laundering. Money laundering techniques change in reaction to change in regulation. Consequently as a result of increased stringent and watertight regulation in the banking sector, money launderers have sought to use other channels such as electronic financial systems to continue their illegal activities. Agarwal and Agarwal in *Money Laundering, New Forms of Crime Victimization*(Current

⁴¹ Money Laundering Strategy for 2000, *supra* note 28

Trends and Modus Operandi)⁴² opine that while the emergence of electronic finance has on one hand benefited growth, development and inter-regional trade, on the other hand it has made the possibility to trace movements of suspect funds and in identifying the real ownership of suspicious assets behind shell companies or offshore bank facades an enormously difficult task for the enforcement bodies, the intelligence agencies and the government.

The emergence of electronic financial systems has enabled the creation of deceptive laundering techniques which prevent law enforcement officers from tracing the funds and determining the masterminds behind the criminal acts. Linda Davis in *Nest of Vipers*⁴³ captures the essence of the current nature of the money laundering problem. She writes that, "The money screamed across the wires, its provenance fading in a maze of electronic transfer which shifted it, hid it, broke it up into manageable wads which would be withdrawn and redeposited elsewhere, obliterating the trail."

Due to the problems caused by electronic financial systems formulating the appropriate legislation required to effectively deal with money laundering has been quite a challenge. For example e-payments have certain characteristics which clearly distinguish them from traditional financial systems. At present, mobile money transfer is characterized by low value high volume transactions in comparison to the high value low volume transactions that characterize traditional bank transactions

The Annex to the FATF report on Money laundering Typologies summarizes the differences between traditional systems and modern day systems. This is clearly outlined in Annex 1

⁴² J.D Agarwal & Aman Agarwal, Keynote address on *Money Laundering: New Forms of Crime Victimization (Current trends and Modus Operandi)* National Workshop on "New Forms of Crime Victimization with reference to Money Laundering", organized by the Indian Society of Victimology, Department of Criminology, University of Madras, Chepauk, Chennai, INDIA, on 18th November 2006.

⁴³ Linda Davis, *Nest of Vipers* (Reed Business Information Inc, 1995

It is therefore reasonable to conclude that due to the distinguishing attributes of modern technologies, there is a need to enact legislation to suit them. The same reasoning applies to mobile money transfer. Extending traditional legislation to modern technological developments is counter-productive.

1.9 RESEARCH METHODOLOGY

This study will adopt a descriptive research design because it will describe the state of the anti money laundering legal framework

Data collection will be mainly through secondary sources of data such as scholarly works, journals and the internet. It is worth noting that mobile money transfer is a recent development hence the literature in this area is limited

1.10 SUMMARY OF CHAPTERS

Chapter 1

This is the introductory chapter which highlights the background of the study, statement of the problem, conceptual and theoretical framework, literature review, research justification and research methodology.

Chapter 2

In this chapter, the provisions of the recently enacted Proceeds of Crime and Anti Money Laundering Act 2009 will be critically analyzed. The definition of money laundering, the obligations imposed, the enforcement mechanisms and the institutions established will all be analyzed to determine how suitable they are to regulate money laundering in mobile money transfer services. The Chapter will also seek to explain why the current banking anti-money laundering regulations cannot be applied to mobile money transfer.

Chapter 3

This chapter will give an analysis of the various models adopted by mobile service operators in offering mobile money transfer services. In addition, this chapter will seek to

determine how adaptable the current Kenyan laws are to the various mobile money transfer models.

Chapter 4

This chapter will seek to discuss the impediments to the successful prosecution of the crime of money laundering in Kenya and identify ways in which the impediments can be remedied in order to ensure successful prosecution of the crime of money laundering.

Chapter 5

This will be the final chapter and it will contain a summary of findings and proposed recommendations.

2.0 CHAPTER TWO

THE MONEY LAUNDERING LEGAL FRAMEWORK

2.1 INTRODUCTION

This chapter will review certain provisions of the Proceeds of Crime and Anti Money Laundering Act 2009 with the aim of determining how effective the Act will be in preventing and regulating money laundering in mobile money transfer. The identified areas of analysis include: The definition of money laundering, predicate offences and reporting institutions. The Customer due diligence provisions and the supervision and enforcement mechanisms will also be reviewed

2.2 DEFINITION OF MONEY LAUNDERING

In order for an activity to be considered a crime it must be defined and categorized as a crime by law. In Kenya, section 3 of the Judicature Act clearly provides for the sources of law in Kenya. It is the existence of such laws that provides a basis of legitimacy for state agencies to investigate, prosecute and punish individuals for the commission of an offence.⁴⁴ Accordingly, the basic principle of legality is summarized in the ancient maxim, *nulla poena sine lege* (“no punishment without law”)

The technical definition of money laundering varies from jurisdiction to jurisdiction. The United Nations Global Programme Against Money Laundering highlights the elements of an effective money laundering scheme, “...a process which disguises illegal profits without compromising the criminals who wish to benefit from the proceeds. It is a dynamic three stage process that requires first moving the funds from direct association with the crime, second disguising the trail to foil pursuit and third making the money available to the criminal once again with the occupational and geographic origins hidden from view.”

In Kenya, the Proceeds of Crime and Anti Money Laundering Act takes a broad definition of money laundering and question arises if money laundering with regards to

⁴⁴ Criminal Justice 2nd Edition, Steve Uglow, London, Sweet and Maxwell, 2002

mobile money transfer has properly been captured by the Act. Money laundering is defined as an offence committed under Section 3, 4, 5 and 8 of the Act. These sections provide as follows:

3. *A person who knows or who ought reasonably to have known that property is or forms part of the proceeds of crime and—*

- (a) *enters into any agreement or engages in any arrangement or transaction with anyone in connection with that property, whether such agreement, arrangement or transaction is legally enforceable or not; or*
- (b) *performs any other act in connection with such property, whether it is performed independently or with any other person,*

which has or is likely to have the effect of—

- (i) *concealing or disguising the nature, source, location, disposition or movement of the said property or the ownership thereof or any interest which anyone may have in respect thereof; or*
- (ii) *enabling or assisting any person who has committed or commits an offence, whether in Kenya or elsewhere to avoid prosecution; or*
- (iii) *removing or diminishing any property acquired directly, or indirectly, as a result of the commission of an offence,*

commits an offence.

4. *A person who knows or ought reasonably to have known that another person has obtained the proceeds of crime, and who enters into any agreement with anyone or engages in any arrangement or transaction whereby—*

- (a) *retention or the control by or on behalf of that other person of the proceeds of crime is facilitated; or*
- (b) *such proceeds of crime are used to make funds available to that other person or to acquire property on that person's behalf or to benefit that person in any other way*

commits an offence.

5. *A person who—*

(a) *acquires*

(b) *uses; or*

(c) *has possession of*

property and who, at the time of acquisition, use or possession of such property, knows or ought reasonably to have known that it is or forms part of the proceeds of a crime committed by another person, commits an offence.

8. *A person who, knowingly transports, transmits, transfers or receives or attempts to transport, transmit, transfer or receive a monetary instrument or anything of value to another person, with intent to commit an offence, commits an offence*

In the case of MMT, the persons likely to commit money laundering are the sender, recipient and the mobile telephone operator. In order to determine how suitable the

definition is in capturing these three persons (natural and juristic) as possible money launderers, the analysis will be broken down in terms of,

- i. the principal offenders i.e the sender and recipient and
- ii. the mobile telephone operator

while at the same time taking note if the three stages of money laundering (layering, placement and integration) have been clearly captured.

2.2.1 The Principal Offenders

In the event of prosecuting a person for sending or receiving, proceeds of crime, the most suitable sections to charge the persons are section 3, 4 and 5. This section clearly provides the requisite *mens rea* that is *knowing that the property forms part of the proceeds of crime*. It is worth noting that this *mens rea* is extremely important at all three stages of money laundering.

Money laundering is a crime of intent thus without properly defining the necessary mental element, a person cannot be charged for money laundering. Furthermore, this intent must exist in both the sender and recipient and this is clearly captured because section 3 requires the existence of an agreement. Thus if such knowledge is only available to the sender, the recipient cannot therefore be guilty of an offence.

2.2.2 Mobile Telephone Operators

In so far as the mobile telephone companies are concerned, they can be charged under all sections that criminalize money laundering. However, of significance is section 3 and 4 which put criminal responsibility on the person (person means both a natural and juristic person) who enters into an arrangement or transaction that facilitates the use, control or concealment of proceeds of crime. Thus if the mobile telephone company knows that money in a customer's account constitutes proceeds of crime and without reporting the transaction, it processes it, it facilitates the use or control of the proceeds of crime, and thus commits an offence under s. 4. Section 45 imposes an obligation to reporting institutions to continuously monitor and report suspicious transactions. Failure to report is an offence. Section 6 makes it an offence to willfully fail to report unusual transactions as

provided under S.45 (2). The penalty for this offence is a fine not exceeding ten million shillings or the amount of the value of the property involved in the offence, whichever is the higher.

The Act however provides a defence under section 7 for mobile telephone companies that proceed to transfer the funds so long as they report the suspicious transaction. It is worth noting that this defence has no effect since the reporting obligations imposed by the Act is USD 10,000, an amount that cannot be transferred using mobile money transfer. This means that in essence, should mobile network operators be charged under section 3 or 4 they are denied the statutory defence by the same statute. Special provision should therefore be made for mobile money transfer transactions.

On the other hand assuming that a reporting threshold is enacted for MMT, there will still be a loophole in the regulatory framework. The statutory defence makes it sufficient to report a suspicious transaction. Thus if the MNO proceeds with the transaction and reports it, it has a defence in law for its action. This leaves an opportunity for money launderers to conspire with these companies. There is a need to amend the provision and indicate that the transaction must be approved. In the UK for instance, disclosure of suspicious transactions is not enough for financial institutions to proceed with a transaction, they must receive authorized consent from the regulatory body. This system should be adopted in Kenya in order to seal the loophole. The only problem is that due to the speed with which MMT services operate, such approval might cause delays. It is however worth noting that the terms of use provided for by the MNOs and which are incorporated in the standard form contracts; delays in service provision are allowed

2.2.3 Shortcomings of Section 8

Section 8 makes it an offence of money laundering for anyone who transfers or transmits money with intent to commit an offence. This section therefore implies that it is immaterial which crime is to be committed by such funds such a transaction automatically becomes one of money laundering. Thus if the funds are meant to pay off a

contracted assassin or a thief, the person initiates the transaction will be guilty of money laundering.

If the definition remains as is, it will cause serious problems at the point of prosecution. The defence will argue that the definition does not meet the character of money laundering since intent to conceal or disguise the funds as legal proceeds is absent. If indeed the funds are used to facilitate a crime the funds retain their criminal nature.

2.2.4 Inchoate Offences

The Act does not create inchoate offences thus all offenders regardless of their level of involvement will be charged for the full crime. Thus aiders and abettors of the crime face the same charges as the principal offenders.

2.3 DEFINITION OF PREDICATE OFFENCES

According to Article 2(h) of the United Nations Convention Against Corruption (UNCAC), "predicate offences shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 23 of the convention." Article 23 defines money laundering. This definition is also used in the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime i.e. the Strasbourg Convention.

Therefore, disguising or concealing the source of certain proceeds will not amount to money laundering unless these proceeds were obtained from a criminal activity (predicate offence). For example some countries do not categorize tax evasion as a crime for example in Switzerland tax evasion is a misdemeanor and not a crime. So if money laundering was committed in Kenya with tax evasion funds from Switzerland, Kenya cannot prosecute for money laundering unless Switzerland decides to list tax evasion as a predicate offence.

Defining predicate offences is extremely important in so far as law enforcement is concerned. However, defining what constitutes a predicate offence has been a serious

challenge for legislators globally resulting in different countries adopting different approaches with regard to defining predicate offences. According to the FATF⁴⁵, countries should apply the crime of money laundering to all serious offences with a view to including the widest range of predicate offences. The FATF has in its forty recommendations outlined the various approaches which countries can adopt in defining predicate offences. Predicate offences may be described⁴⁶

- i. By reference to all offences (the all crimes approach)
- ii. By reference to a threshold linked either
 - a. To a category of serious offences or
 - b. To the penalty of imprisonment applicable to the predicate offence
- iii. A combination of the two

UNIVERSITY OF NAIROBI LIBRARY
P. O. Box 30197
NAIROBI

Whereas the FATF recommendations are not binding, they have been recognized by the International Monetary Fund (IMF) and World Bank as the international standards for combating money laundering and the financing of terrorism.

The Kenyan approach to defining predicate offences is the all crimes approach. Section 2 of the Act defines an "Offence"

"means an offence against a provision of any law in Kenya, or an offence against a provision of any law in a foreign state for conduct which, if it occurred in Kenya, would constitute an offence against a provision of any law in Kenya;"

Under the all crimes approach, all activities which constitute crimes under Kenyan law are predicate offences. This is unlike the approach of having a limited category of crimes that qualify as predicate offences. Furthermore, the Kenyan law requires for dual criminality. This means that an act has to be an offence in both the country where the act was committed and in Kenya where the monetary proceeds are received. The dual criminality requirement greatly reduces the effectiveness of combating money laundering. Given the transnational nature of money laundering, the effectiveness of the all crimes approach is diminished where other countries adopt the threshold approach or a limited category of crimes. This is because if the act is committed in a country where it is

⁴⁵ The FATF is an inter-governmental body which sets standards and develops and promotes policies to combat money laundering and terrorist financing.

⁴⁶ FATF recommendation 1, Scope of the criminal offence of money laundering.

not a crime; the proceeds are not proceeds of crime within the definition of the Proceeds of Crime and Anti Money Laundering Act. The Kenyan courts cannot therefore prosecute the persons involved.

Accordingly, this loophole can be misused by criminals in order to conduct money laundering through mobile money transfer services and other financial institutions. With regard to MMT in Kenya, M-Pesa offered by Safaricom and Zap offered by Zain offer MMT services across the Kenyan border. In so far as M-Pesa is concerned, it has only expanded its operations to the United Kingdom (UK). It is worth noting that UK has enacted the Proceeds of Crimes Act 2002 which also adopts the all crimes approach thus the effectiveness of the Kenyan law is not diminished. However with regard to Zap, Zain has extended this service to several African countries some of which do not have money laundering legislation.

Of great concern is the crime of terrorism. Whereas terrorism is not strictly speaking a predicate offence because it is not a crime from which dirty proceeds are obtained and which subsequently need to be laundered. Rather, terrorism involves reverse money laundering. Unlike money laundering, it does not purport to avoid detection of dirty money of past crimes but instead to primarily avoiding detection of clean money to be used for future crimes.⁴⁷ However, terrorism financing uses similar channels and exploits the same weaknesses in the financial system as money laundering in its aim of concealment. It is in this connection that FATF listing of terrorism as a predicate crime to money laundering can be understood.⁴⁸

The problem with terrorism as a crime is that it does not have a uniform universal definition. The United Nations definition is different from that adopted by the Arab

⁴⁷ Elena Madalina Buuioic, *Predicate Offences- The Achilles Heel of Anti-Money Laundering Legislation*, "Chapter 2 in Brigette Unger *The Scale and Impacts of Money Laundering*." Edward Elgar Cheltenham, UK. Northampton, MA, USA 2007

⁴⁸ Elena Madalina Buuioic, *Predicate Offences- The Achilles Heel of Anti-Money Laundering Legislation*, "Chapter 2 in Brigette Unger *The Scale and Impacts of Money Laundering*." Edward Elgar Cheltenham, UK. Northampton, MA, USA 2007

League, African Union and other national laws. Furthermore very few countries have enacted domestic legislation criminalizing terrorism. Thus in determining the criminality, a country which has not yet enacted counter terrorism legislation has to rely on international treaties which as earlier explained do not have a uniform universal definition. Kenya follows the British transformation doctrine whereby treaties must be ratified and enacted by Parliament to become law⁴⁹. In this case Kenya has not domesticated counter terrorist treaties. Furthermore, international law is not expressly recognized as a source of law by the Judicature Act (Cap 8) Laws of Kenya.⁵⁰

The lack of a clear legal framework to deal with terrorism is a major setback in the fight against money laundering and terrorist financing in Kenya.

Accordingly, criminals can launder funds using MMT services in order to finance terrorist cells. The fact that there is a ceiling on the amount to be sent via MMT services is not an impediment since terrorists operate using cells and one individual is part of an elaborate scheme. Furthermore the individuals are not necessarily connected. Therefore MMT services can be used to pay different terrorists over a long period of time.

2.3.1 Recommendation

In order to remedy this, it is recommended that a directive be issued to the effect that MNOs can only extend MMT services to countries which have enacted money laundering legislation and which adopt the all crimes approach.

With regards to terrorism, it is imperative to enact a terrorism legislation so as to clearly identify which activities constitute terrorism activities.

2.4 REPORTING INSTITUTIONS

Another question to determine is whether MNOs are reporting institutions within the meaning of the Act. Reporting institutions include financial institutions and designated

⁴⁹ DJ Harris, Cases and Materials on International Law, London: Sweet & Maxwell, 1998

⁵⁰ Section 3

non-financial businesses or professions. Under the Act financial institutions have a broad definition. The most applicable to MNOs that offer mobile money transfer services is

“financial institution” means any person or entity, which conducts as a business, one or more of the following activities or operations–

(a) accepting deposits and other repayable funds from the public;

This definition is applicable to mobile money transfer at the point of making deposits and withdrawals. The Act does not define the term deposit thus it is highly debatable if the definition in the Banking Act would apply. It is however most likely that the dictionary meaning of the term deposit will be applicable in order to bring in more financial institutions within the jurisdiction of the Act.

However as a means of payment, it has been argued that the following definition is most suitable since it brings in the concept of electronic money:

(e) issuing and managing means of payment (such as credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money);

Mobile telephone operators provide the technological facilities necessary to conduct mobile money transfer as well as making utility payments. Therefore it can be concluded that these operators issue and manage a means of payment within the meaning of the Act.

Electronic money is still a new concept in Kenya, and has not been defined by any existing piece of legislation. Accordingly, whether mobile money transfer constitutes electronic money is highly debatable. The European Union (EU) has made attempts to define electronic money and according to its Directive Proposal of 9.10.2008, electronic money is “a monetary value as represented by a claim on the issuer which is stored electronically and issued on receipt of funds, for the purpose of making payment transactions (as defined in Article 4(5) of Directive 2007/64/EC) and is accepted by nature or legal persons other than the issuer. Going by this definition, e-money is monetary value that is stored electronically on receipt of funds, and which is used for making payment transactions.

If this is the meaning that Parliament attributed to electronic money then we can rightly say that mobile money transfer is electronic money and therefore regulated by the Act.

The Act also applies to designated non-financial businesses or professions and provides a list of such businesses. The FATF 40 recommendations also make reference to designated non financial businesses or professions. It is of great interest that unlike the Kenyan statute, the FATF recommendations list trust companies as designated non-financial businesses. Acting as a trustee of an express trust is therefore a designated non-financial business.

The business model adopted by mobile telephone companies is such that they establish trusts and appoint trustees to manage the public funds held in the MMT system. These trust account holders are a separate entity from the mobile telephone company. Bank accounts in the names of the trustees are opened with licensed banks in Kenya and the funds are held in trust for customers of the mobile companies. The trustees also deduct any fees levied by the mobile companies in connection with the transfer services, remit the fees to the mobile company and pay the balance to the order of the mobile company's subscriber. At no time are the funds held by or to the order of the mobile company. The mobile companies simply act as a conduit and technological facilitator for the funds.⁵¹ The reason for adopting this business model is so that the act of taking deposits does not make the company a deposit taking institution within the meaning of the Banking Act as this will have the effect of subjecting the company to the stringent banking regulations

The omission of trust companies from the Act is serious considering the trust account holders are the issuers of the funds. Question arises whether the trust companies can be used to facilitate money laundering since the obligations imposed on financial and designated non-financial businesses in so far as customer due diligence and record keeping are not applicable to trust companies. The only time the Act will apply to trust companies is if the Minister upon advice from the Financial Reporting Centre declares trust companies to be designated non-financial businesses.

2.4.1 Recommendations

⁵¹ Anne Kiunuhe, Why Kenya Needs Watertight Laws to Combat Money Laundering, Business Daily, 24th Feb, 2009, pg 9

The Act needs to be amended to include trust companies as designated non-financial businesses as the omission can create a loophole for criminals. Presently, only the mobile telephone operators are reporting institutions subject to the provisions of the Act

2.5 CUSTOMER DUE DILIGENCE AND RECORD KEEPING

The Act makes express provision for customer due diligence (CDD)/ Know your Customer (KYC) requirements to be met by all reporting institutions. CDD is to be carried out when establishing a business relationship and also in the case of continuing business relationships. CDD involves identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information. Where there is a beneficial owner who is not the customer, CDD involves identifying the beneficial owner.

Under the Act, all reporting institutions are required to take all reasonable steps to ascertain the identity of the customer and also maintain proper client records. In so far as ascertaining the clients' identity is concerned, reporting institutions are required to obtain documentation sufficient to identify the client, his physical and postal address⁵². With regards to maintaining client records, reporting institutions are required to maintain the records for at least 7 years before disposing of them⁵³. This is a much longer duration than the 5 years that the FATF prescribes. In addition, the reporting institution is under an obligation under section 48 of the Bill to establish and maintain internal controls and reporting procedures. Moreover the reporting institution is required to identify a reporting officer who will be mandated to monitor transactions and report any suspicious transaction

The Act makes it an offence under Section 12 to fail to comply with Sections 45, 46 and 47. Therefore MNOs will be guilty of an offence if they fail to monitor and report unusual transactions or fails to establish customer identification procedures or fails to create and maintain customer records. The penalty of such an offence is a fine not

⁵² Section 45 and 46

⁵³ Section 47

exceeding five million shillings or the amount of the value of the property involved in the offence, whichever is the higher

A significant weakness in the Act is that the CDD requirements in the Act are general provisions to be applied across the board. Specific CDD requirements that cater for mobile money transfer have been omitted in the following ways:

1. Evidence of Identity

Of great concern is Section 46(7) which provides that in the case of a series of transactions where the applicant has already produced satisfactory evidence of identity, there is no requirement for a customer to provide further evidence of identity. The current MMT procedures by M-Pesa and Zap, require the agents to verify a customer's identity before receiving deposits or making payments to a customer. Question arises if at the point of application for an account the applicant's identity was verified and sufficient in the circumstances, is it in order for the agents to request proof of identity in subsequent transactions when the Act states that will not be necessary?

2. Risk Based Approach

It is worth noting that the Kenyan Act does not provide for a risk sensitive approach to CDD unlike the Money Laundering Regulations 2007(the Third Regulations) of the United Kingdom (UK,). In Kenya all reporting institutions are subjected to the same level of CDD irrespective whether the nature of their business has a high risk or low risk. Section 46 of the Act provides that reporting institutions shall take *reasonable* steps in identifying its customers. Reasonable is a question of fact and extremely ambiguous. It does not clearly indicate the existence of a risk based approach.

Under the UK law, the regulated sector is obliged to satisfy itself, on a risk sensitive basis that it knows with whom it is dealing and to do so with the best information

proportionately available⁵⁴. In the UK, under the JMLSG⁵⁵ Guidance 4.4 the risk based approach overall in terms of any policy that can be applied to individual decisions will

- Recognize that money laundering and terrorist financing threats varies from customer to customer, across jurisdictions and between products and delivery channels
- Allow management to discriminate reasonably between their customers due to the nature of the perceived risk in relation to them
- Let senior management apply its approach to the firm's procedures and controls
- Help produce a most cost effective system

Different levels of CDD are required for individuals and beneficial owners. The UK Money Laundering Directive and the Implementation Measures recognize simplified due diligence (SDD) where it has been assessed that a particular situation poses a low appreciable risk of money laundering or terrorist financing. Furthermore enhanced due diligence (EDD) is recognized in higher than normal risk situations.⁵⁶

In Kenya, all reporting institutions are subjected to the same level of CDD irrespective of the risks involved. In the case of MMT, the transactions are of a high volume low risk nature thus subjecting them to the same level of regulation with high risk reporting institutions is unfair considering non-compliance is an offence under the Act. In addition, the aim of MMT is to reach the unbanked members of society who are in many cases members of the low income bracket. Accordingly such individuals have limited access to formal documentation. For example since very many reside in informal settlements and

⁵⁴Paul Hynes, Richard Furlong, Nathaniel Rudolf, *International Money Laundering and Terrorist Financing : A UK Perspective*, Sweet & Maxwell, 2009

⁵⁵The Joint Money Laundering Steering Group(JMLSG) is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance.

⁵⁶Reg. 13(1) & Reg 14

in the rural area, they cannot produce utility bills as proof of physical address nor do they have postal addresses.

2.5.1 Recommendations

Kenya should therefore amend its law to reflect the risks that affect different reporting institutions. FATF recommendation 5 allows countries to apply 'reduced or simplified' CDD/KYC if risks are low by capping balance & transaction size & therefore account utility for criminal elements⁵⁷. Mobile money transfer in Kenya can therefore be subjected to proportionate risk based CDD as this is allowed.

The use of a capping balance was adopted in South Africa but the law changed in order to assist law enforcement agencies trace criminals. In South Africa, mobile money transfer is offered by MTN in conjunction with a bank and just like Kenya, a large number of people live in informal settlements and do not have access to documents to prove their identity. Until recently, Exemption 17 of the South African, Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (RICA), eliminated the legal requirement to verify a customer's physical address for accounts subject to a minimum balance cap.

Thus if a person has a valid South African identity number and transaction limits are observed, the customer can therefore start using the mobile banking service by transacting small amounts without going to a bank branch to provide an address. However, a recent amendment to RICA has changed this situation. The new RICA provisions prohibit mobile network operators from activating a new SIM card unless they have captured the customer's identity. This includes the person's cellular phone number, full names and surname, identity number and an address (preferably a residential address)⁵⁸.

⁵⁷ *Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance*, CGAP Publication, January 2008

⁵⁸ *Marina Solin, New Regulatory Change in South Africa Affects Mobile Money, August 14th, 2009*

This amendment is clear evidence that the absence of CDD creates a problem. Accordingly it is not recommended that CDD requirements be abolished; on the contrary, some level of proportionate CDD is required.

Adopting a risk based approach does not mean that the law is creating loopholes for criminals to abuse because even extremely strict controls can still be exploited by criminals. The risk based approach fosters rather than stifles innovation. An extremely restrictive regulatory system reduces the incentive for individuals to create. Mobile money transfer is an extremely innovative system that has revolutionized not only financial and telecommunications industries but has changed the lives of the millions of unbanked people. The gains brought by mobile money transfer should therefore not be lost because of extremely restrictive laws.

The risk based approach should be guided by the principle of proportionality which is defined by the **General Principles for International Remittance Services**⁵⁹

“...Proportionality means that the legal and regulatory framework... should not be overly restrictive and burdensome relative to the possible issues it is designed to tackle or the number and value of (transactions) involved...In considering this it is important to realize that the public policy objectives may not always point in the same direction...Proportionality means that any such inconsistencies are recognized and resolved in a way that in light of the country’s overall priorities, achieves an appropriate balance.”

2.6 SUPERVISION AND ENFORCEMENT AGENCIES

In terms of supervision, the Central Bank of Kenya (CBK) is recognized as a supervisory body. The Communications Commission of Kenya is not listed as a supervisory body. We can therefore conclude that in the case of mobile money transfer, the supervisory authority is the CBK. This is consistent with the CBK Act which was recently amended to grant the CBK supervisory authority over all financial institutions.

For purposes of money laundering, the CBK only has supervisory authority over the mobile telephone company and not the trust company/trust account holders. This is

⁵⁹ Jointly developed by the World Bank and the Committee on Payment and Settlement systems of the Bank for international Settlements in Basel, 2007

because if we rely on the earlier argument on reporting institutions, only the mobile telephone operators are financial institutions for purposes of money laundering. This leaves the trust company/trust account holders unregulated which is a serious omission.

In so far as enforcement is concerned, the Act creates a number of bodies while at the same time reinforcing the powers of existing institutions such as the police force. The police force has increased authority to enter, search and seize property which forms part of the proceeds of crime. The bodies established by the Act include:

- i. Financial Reporting Centre: The principal objective of the Centre is to assist in the identification of the proceeds of crime and the combating of money laundering⁶⁰ the functions of the Centre are expansive and are outlined in detail in Section 25
- ii. Anti-Money Laundering Advisory Board: The functions of the Board shall be to advise the Director generally on the performance of his functions and the exercise of his powers under this Act⁶¹.
- iii. Asset Recovery Agency is mandated with recovery of assets which form part of the proceeds of crime. The Act provides for seizing and confiscation orders of assets which form part of the proceeds of crime

The duties assigned to these various institutions are adequate enough to combat money laundering. However, their activities are still limited to the mobile telephone operators since the trust companies/trust account holders are not reporting institutions under the Act.

2.6.1 Recommendations

In order to make these institutions more effective, it is imperative that trust companies/trust account holders be included as reporting institutions.

⁶⁰ Section 24 (1)

⁶¹ Section 51

3.0 CHAPTER THREE

MOBILE MONEY TRANSFER BUSINESS MODELS

3.1 INTRODUCTION

Mobile network operators (MNOs) have adopted different business models in order to facilitate mobile money transfer services. A major setback in the selection of the appropriate business model is the absence of a clear regulatory framework. This is because, the convergence of telecommunication and financial services caught policy makers and regulators ill prepared. However, the absence of a clear regulatory framework has promoted rather than stifled innovation this is extremely unique considering that in sectors such as Capital Markets, the absence of asset based securitization has stifled development while in the Banking Sector, agency banking could only commence once Central Bank issued regulations to that effect. This chapter will therefore seek to analyse the extent to which the existing regulatory framework accommodates the various MMT business models and how the absence of clear regulation has fostered innovation.

3.2 BUSINESS MODELS

The business models used by mobile network operators to offer mobile money transfer can be divided into two categories:

1. Bank-Based
2. Non-Bank Based

The regulatory significance of the distinction between the bank based and non-bank based models lies in the fact that behind every transaction under the bank based model, there stands a licensed prudentially regulated and supervised financial institution⁶².

3.2.1 Bank-Based Model

Under the bank based model, mobile network operators partner with banks to offer mobile money transfer. The MNO provides the technical facilities for carrying out the

⁶² Regulating Transformational Branchless banking: Mobile Phones and Other Technology to Increase Access to Finance, CGAP Publication, January 2008

transaction while the bank is the issuer of the funds. The purpose for this model is so that the MNO can avoid financial regulation under the Banking Act. This is because the Banking Act provides an extremely rigid operational framework while MMT services require flexibility and simplicity in order to thrive. Hence this model provides both the flexibility and regulation security required for the development of a successful, secure and regulated mobile money transfer service.

Under the Banking Act, only institutions licenced as banks by the Central bank of Kenya can accept deposits⁶³. Banking business under the Act constitutes *inter alia*⁶⁴: "the accepting from members of the public of money on deposit repayable on demand or at the expiry of a fixed period or after notice." Therefore if MNOs receive deposits from clients they are conducting banking business and can be construed to be deposit taking institutions and will therefore be subject to the stringent banking regulation yet mobile money transfer is not subject to the traditional risks that face banks and other financial institutions.

For purposes of this research, mobile money transfer will not apply to mobile banking. Mobile banking is a system that allows mobile based accessibility to banking services by bank account holders. Accordingly, under mobile banking, the customer has a direct contractual relationship with a prudentially regulated and supervised bank whereas in mobile money transfer customers have a contractual relationship with the mobile network operator. However, it is worth noting that one of the MNOs in Kenya, Zain has integrated its mobile money transfer service Zap, to the mobile banking service offered by Standard Chartered Bank. This arrangement is strictly available only to the bank's clients with Zain lines. Customers can deposit money from their zap account into their bank account and withdraw money from their bank account into their zap account

As earlier mentioned, under the bank based model, the MNO is a conduit for the service while the bank is the issuer of the funds. For purposes of money laundering it is in order to say that this model is regulated under the Proceeds of Crime and Anti Money Laundering Act 2009. The bank is a financial institution within the meaning of the Act.

⁶³ Section 3; restrictions on carrying out banking business

⁶⁴ Section 2

Furthermore, the bank is bound by the CBK Prudential Guidelines on Money Laundering. In so far as the MNO is concerned, it is a financial institution within the meaning of Section 3 (a) and (e) of the Act⁶⁵.

Accordingly, both the MNO and bank are bound to adhere to the AML& KYC obligations imposed on reporting institutions under the Act. Some of these obligations involve: Record keeping, monitoring and reporting of suspicious transactions, customer due diligence among others.

The Bank Based Model has been adopted in South Africa where MTN partnered with Standard Bank. Under this arrangement, MTN uses Standard Bank licenses and its own outlets to distribute and service the mobile money product. Whilst MTN, the mobile operator, is visible at the customer interface for the mobile money service, Standard Bank is responsible for the regulatory compliance. Customers open their MTN Mobile Money accounts online and the mobile telephone number becomes the customers account number. MTN is able to register clients on behalf of Standard Bank thus agency rules apply to allow a mobile operator to become an agent of a bank⁶⁶.

The South African Model has taken the form of agency banking. Agency banking is now recognized in Kenya following the recent issuing of Agency Guidelines by the Central Bank of Kenya. Accordingly the South African Model will therefore be applicable in the Kenyan economy. However, just like mobile banking, the customers in agency banking contract directly with the bank and not with the mobile network operator since the service is offered at the initiative of the bank.

3.2.2 Non-Bank Based Model

Under this model, the mobile network operator is able to offer mobile money transfer services independently of a bank. Under this model, the MNO has two options:

⁶⁵ Refer to discussion in Chapter 2

⁶⁶ GSMA: Enabling Regulatory Environments for Mobile Money Transfer Services. Public White Paper version 1.0 March 2008.

1. To apply for a banking license thus becoming both the issuer of funds and the infrastructure provider.
2. Create a trust company which is separate from the MNO and takes the role of issuer of the funds.

The first option is not adopted in Kenya as it will attract stringent banking regulations and is an extremely expensive option. The second option is the preferred choice in Kenya. Both Safaricom and Zain have created trust companies or rather have appointed trust account holders to be issuer of the funds. This has the effect of separating the issuers of the funds from the infrastructure providers.

A major problem with this system is that traditionally both the issuer of the funds and infrastructure were provided by one institution. For example banks allow customers to make utility payments and withdraw cash from ATMs while at the same time the banks hold the money to the client's order. Accordingly regulation was easy. However when the function of the issuer of funds is separated, a gap in regulation is clearly evident.

As earlier discussed in chapter two, whereas the mobile network operator is a reporting institution within the meaning of the Proceeds of Crime and Anti Money Laundering Act 2009, the trust account holders are not expressly recognized as reporting institutions. The only available option for regulating the trust account holders/trust company in so far as money laundering is concerned is for the bank to exercise a "watch dog" function over the trust account.

The overriding principle in so far as trust accounts are concerned is that the bank should not be a party to any fraud or misapplication of trust funds. The bank must at all times protect the interests of the person beneficially entitled to the funds. Therefore for example, if a bank acts on payment instructions given by the holder of a trust account with the knowledge that the instructions involve a misapplication of trust money, then the bank will be liable to the beneficiaries as a constructive trustee.

The lack of a clear legislative framework is clearly evident. It is therefore a matter of urgency that the Minister should declare trust companies to be designated non-financial businesses in order to bring them under the express regulation of the Act. The bank's "watch dog" function can only be stretched to a certain limit.

3.3 RATIONALE FOR THE TRUST ACCOUNTS AND CENTRAL BANK'S ROLE

Mobile money transfer requires a flexible and simple regulatory framework in order to achieve its objectives of providing financial accessibility to the "unbanked" population. However, the current legal framework in Kenya is rigid and complex, the exact opposite of the prerequisite regulatory environment. This state of affairs has led to the rapid development of the MMT service in the absence of a clear regulatory framework which exposes the country's economy and financial systems to a serious risk. The available regulation is infantile and accordingly insufficient. It is however worth noting that whereas the traditional school of thought promulgates the belief that the presence of law encourages development and innovation, MMT services have proved to be an exception to this rule since the absence of law has in Kenya's case fostered innovation.

Currently, Central Bank of Kenya regulates the service in conjunction with the Communications Commission of Kenya. Central Bank regulates the financial aspect while CCK, the technical aspect. CBK has been able to extend its authority over the service due to the amendment of the CBK Act which extended its supervisory authority to all financial institutions.

Accordingly, CBK, in regulating MMT, saw it beneficial to separate the MNO's funds from the public funds. The reason for this is to protect the public funds from exposure to third party risks. Third party risks could arise as follows⁶⁷:

- (a) insolvency or similar risks on the part of the operator;

⁶⁷ Advisory Opinion Ian Gaitta Advocate

- (b) risk of loss of customer funds through fraud as a result of poor system controls within the MMT product architecture;
- (c) risk of loss as a result of failure of the person holding the trust account which is why only a licensed bank would be permitted to hold the trust account;
- (d) trustee default risk; or
- (e) loss of funds by means of bank charges and the like.

With regard to the risk identified in paragraph (a) above, this could be mitigated by structuring the mobile payment service such that customer funds are held in a trust account by an independent trustee such that the trust account cannot be affected by the mobile network operator's insolvency. Hence the current practice by the CBK to require operators to maintain trust accounts at which customer funds are held, such trust accounts being controlled by trustees of these funds on behalf of the customers. The CBK also requires frequent audit and reporting by the operator and/or the trustees in relation to the funds held in the trust account.

With regard to the risk identified in paragraph (b) above, the CBK will typically require the applicant to satisfy the CBK that the technical features of the product contain sufficient and robust safeguards against fraud or other means of loss of customer funds. The risk referred to in paragraph (c) is covered by CBK agreeing to the identity of the bank which will hold the trust account and reviewing the legal agreements between the bank and the trustees. As regards the risk identified in paragraph (d) above, this issue is dealt with by ensuring that the only deductions allowed from the trust account are sums which the operator is entirely entitled to deduct, for instances, its commissions or fees for air time purchased by a customer using the MMT Product.

Another risk is money laundering. The CBK is concerned to see that the MMT product's structure and transaction documentation contains sufficient anti-money laundering

safeguards in order to ensure that such services are not used as conduits for transmission of proceeds of crime or other illegally acquired funds.

4.0 CHAPTER FOUR

FACTORS AFFECTING THE SUCCESSFUL PROSECUTION OF MONEY LAUNDERING AS AN OFFENCE

4.1 INTRODUCTION

Successful prosecution of any crime is a key deterrent to future crimes money laundering included. There are several factors that affect the successful prosecution of money laundering. The ability to detect and investigate money laundering through mobile money transfer services sets the foundation for successful prosecution. This chapter will therefore seek to evaluate the extent to which the Act adequately provides for the successful prosecution of money laundering through MMT. Some of the factors to be analyzed include criminal and civil asset forfeiture, intra-agency and inter-agency coordination, international cooperation among others. The impediments to successful prosecution will also be analyzed.

4.2 OFFENCES

The Act creates a number of offences that deal with both natural and juristic persons. It also creates offences that deal with the systems and controls which businesses are required to have as well as offences committed by key individuals within them. Among the offences created include: money laundering, failure to report suspicious transactions, tipping off, malicious reporting, misrepresentation, failure to verify customer identity and failure to establish and maintain customer records.

4.2.1 Money Laundering

The offence of money laundering is created under sections 3, 4, 5 and 8 of the Act. These provisions allow for the prosecution of money laundering in that:

- They allow for both self laundering and where laundering is done by a person other than the author of the principal offence.

This is clearly captured with the requirement that an offender has knowledge or is deemed to have reasonable knowledge that certain property comprises of proceeds of crime or enters into an arrangement with another person who has obtained illegal proceeds and deals with the property in such a manner as to conceal its illegal origin.

Furthermore, acquisition, use or the mere possession of proceeds of crime is an offence and can easily be used to prosecute the end user.

- They allow for prosecution of money laundering at all the three stages i.e placement, layering and integration.

Handling property with the knowledge that it constitutes proceeds of crime is not sufficient to amount to money laundering. For money laundering to occur, these sections make it clear the offender must deal with the property in such a way that has the effect of concealing or disguising the nature, source, location, disposition or movement of the said property or the ownership thereof or any interest which anyone may have in respect thereof.

These activities are captured at the different stages of money laundering

4.2.1.1“Knowledge of illegal proceeds”

The definition of the offence brings into sharp focus the mental element of ‘knowledge that the proceeds were from criminal activities.’

The standard of proof in Kenyan criminal cases is beyond any reasonable doubt. Accordingly, the prosecution has to prove beyond any reasonable doubt that the defendant knew or had reasonable grounds to know that the proceeds have been obtained from a specific crime. The standard of proof in this case can be an impediment to successful prosecution especially where the investigations moved through different jurisdictions. Question therefore arises whether the courts should be satisfied that the proceeds have been obtained from an illegal source or is it extremely necessary to prove the commission and knowledge of a specific crime? In the UK, under the Proceeds of Crime Act 2002, the Crown does not have to identify the type of crime alleged - just that the laundered money is the proceeds of some type of crime.

The mental element requires actual knowledge and not mere suspicion that the proceeds are illegal. As Lord Nicholls in *R v Saik [2006] 2 W.L.R. 993, HL* briefly explained, “a decision to deal with money suspected to be the proceeds of crime is not the same as a conscious decision to deal with the proceeds of crime”. However, in reality, the

difference between suspicion and reasonable knowledge is an extremely thin line. Reasonableness is a question of fact and is not measurable. Should the courts therefore accept suspicion of illegality as a sufficient mental element and what exactly constitutes suspicion?

The United Kingdom for example had for a long time debated on what actually constitutes suspicion however; there have been significant development in the case law to fill in the grey areas. Initially, the courts took the dictionary meaning of the word suspicion and in the case of *Da Silva*⁶⁸, the court of appeal criticized the trial judge's direction to the jury on the meaning of suspicion that "any inkling or fleeting thought that the money being paid into [the defendant's] account might be the proceeds of criminal conduct will suffice for the offence... to be proved". The word inkling and fleeting were held to be misleading.

In *Manifest Shipping v Uni-Polaris*⁶⁹, Lord Scott stated, "In my opinion, in order for there to be blind-eye knowledge, the suspicion must be firmly grounded and targeted on specific facts. The deliberate decision must be a decision to avoid obtaining confirmation of facts in whose existence the individual has good reason to believe. To allow blind-eye knowledge to be constituted by a decision not to enquire into an untargeted or speculative suspicion would be to allow negligence, albeit gross, to be the basis of a finding of privity". As it stands, the courts are more willing to define suspicion as something "grounded and targeted on specific facts."

It is however of great interest that reporting a suspicious transaction where someone is charged with money laundering under sections 3, 4 and 5 is a defence under section 7 of the Act. Therefore, it can be argued that if suspicion is a ground for defence why not a ground for prosecution?

⁶⁸ R v Da Silva [2006] EWCA Crim 1654, 11/7/06

⁶⁹ [2001] UKHL 1

4.2.1.2 Proceeds of crime

The money being laundered must represent a benefit from criminal conduct, either directly or indirectly, in whole or in part, so long as the launderer 'knows' that the money represents such a benefit.

It is of great importance to note that the Act has introduced a retrospective aspect with regard to criminal property in the sense that it applies to proceeds derived from criminal activities committed prior to the commencement of the Act. Furthermore any proceeds that are successfully converted from the time the offence was committed are also covered. Therefore, where the crime was committed and the proceeds successfully disguised before the commencement of the Act, this will still amount to proceeds of crime and a person can be prosecuted for money laundering.

A great impediment to the successful identification of proceeds of crime is the double criminality required by the Act. This is because if proceeds are derived from a country where the act is not a crime but is a crime in Kenya they are not proceeds of crime within the meaning of the Act.

4.2.2 Failure to Report Suspicious Transactions

Failure to report suspicious transactions by a reporting institution as provided for under section 45 of the Act constitutes an offence under section 12. In practice this MNO are highly unlikely to be charged for this offence because the reporting threshold as provided for under the Act is USD 10,000, a limit unlikely to be reached through MMT due to transaction limits. Furthermore, the Act does not expressly provide for what constitutes a suspicious transaction for MMT services. Thus the vacuum in legislation means that defining suspicious transactions is at the discretion of MNO.

4.2.3 Tipping Off, Misrepresentation and Malicious Reporting

It is an offence under section 9 to make a disclosure of information that is likely to prejudice investigations by law enforcement agencies. Legal privilege is not a defence for such disclosure.

There is an overlap as to what constitutes misrepresentation and what constitutes malicious reporting. According to the wording of s.10 and s.11 making a false representation to the financial reporting centre constitutes both offences

4.2.4 Failure to Establish and Maintain Customer Records and Failure to Verify Customer Identity

Establishing and maintaining customer records and verifying customer identity are obligations imposed on financial institutions under sections 47 and 46 respectively of the Act. Failure to do so amounts to an offence under s. 12.

4.3 CRIMINAL AND CIVIL ASSET FORFEITURE

The Act provides for both criminal and civil forfeiture. In addition under criminal forfeiture, the Act provides for the implementation of confiscation orders, restraint orders and for the appointment of receiver. In order to execute these functions, the Act has created the Asset Recovery Agency⁷⁰ to conduct recovery proceedings of property which is in whole or part proceeds of crime. In order for the Agency to carry out its functions effectively, there must be cooperation with the Financial Reporting Centre whose responsibility is to identify proceeds of crime.

It is worth noting that with regards to criminal forfeiture, the Act has made proceedings concerning confiscation and restraint orders civil in nature and the civil procedure rules will be applicable⁷¹. Confiscation orders can only be granted by the court after the defendant is found guilty of money laundering while restraint orders can be granted when investigations are underway i.e at the commencement of criminal proceedings in order to prevent the accused from disposing off the assets. The principle underlying criminal confiscation is that the offender who commits an offence from which he benefits

⁷⁰ Part IV

⁷¹ Section 57

financially will face two consequences. In addition to any punishment for the predicate offence, the government will seek to recover the value of his benefit.⁷²

The Act further establishes a Criminal Asset Recovery Fund⁷³ which is to be administered by the Agency. The Funds will include all property derived from confiscation and forfeiture orders and shall vest in the Government and be disposed off in accordance with the relevant law relating to the disposal of public property.

4.4 INTERNATIONAL COOPERATION

Money laundering is an extraditable offence under the Act. Furthermore, the Act provides for mutual legal assistance and international cooperation in investigation and prosecution of money laundering offenders⁷⁴. The mutual assistance can be in the form of provision of evidence, assistance in investigation, requests for enforcement orders such as confiscation and forfeiture among others. Such assistance is based on reciprocity and mutuality between countries.

These legal provisions conform to the FATF recommendations⁷⁵ that countries should provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecution and related proceedings.

However, a major setback that will affect the effectiveness in the provision of mutual legal assistance is that the Act under section 114 authorizes the attorney general to initiate such a request to the appropriate authority of the other country. The attorney general's office has been a major impediment to obtaining mutual legal assistance in so far as fighting corruption is concerned and this is one of the challenges facing the Kenya Anti Corruption Commission (KACC). The courts have for instance ruled in various Anglo-Leasing cases that KACC is barred from requesting for mutual legal assistance from foreign authorities and that these powers vest in the Attorney General's office

⁷² P.268

⁷³ Part XI

⁷⁴ Part XII

⁷⁵ FATF recommendation 36

The Mutual Legal Assistance Bill does not remedy this situation since the Attorney General's office is the Central Authority under the Act and Competent Authorities can only request for assistance through the central authority and it is only in urgent situations where this requirement can be omitted⁷⁶. Furthermore, the Bill if enacted will further hinder the effectiveness of the Act because under section 11(a) a request for mutual assistance can be refused if in the opinion of the competent authority it relates to the prosecution or punishment of an offence that is not an offence in Kenya. Such a refusal will affect relations between countries in future and combating money laundering will be difficult considering the need for dual criminality in the crime. Mutual legal assistance is extremely necessary.

A major omission in the Act is that it does not expressly provide for which country prosecution will take place whether it is the country where the predicate offence was committed or where placement of the proceeds began or the country where layering or integration of the proceeds took place. This is a major problem that international criminal law has not been able to remedy due to the issues of state sovereignty and territoriality. Silence on this matter means that countries will have to negotiate separate agreements on jurisdiction with regards to prosecution.

4.5 INTRA-AGENCY AND INTER-AGENCY CO-ORDINATION

The Act creates three institutions to deal with the identification, tracing and seizure of the proceeds of crime. These institutions are:

1. The Financial Reporting Centre whose function is to identify proceeds of crime by receiving and analyzing suspicious transactions made by reporting institutions and forwarding the same to the appropriate law enforcement agency⁷⁷
2. The Assets Recovery Agency whose function is to conduct recovery proceedings of the proceeds of crime. These recovery proceedings can be conducted either through criminal or civil proceedings⁷⁸.

⁷⁶ Sections 7(1) & 7(2)

⁷⁷ Section 25

3. The Anti-Money Laundering Board whose function is to advise the Director of the Financial Reporting Centre on the performance of his functions and the exercise of his powers⁷⁹.

In order for these institutions to function effectively they must co-operate at all levels. Furthermore, since prosecutorial powers vest in the Attorney General, there is a need for these institutions to liaise with the police force and Attorney Generals Chambers. It is worth noting that the Act has vested the police force with enormous powers of entry, search and seizure.⁸⁰ Accordingly, there must be cooperation and coordination from the point of investigation to prosecution.

4.6 IMPEDIMENTS TO SUCCESSFUL PROSECUTION

4.6.1 Prosecutorial Powers Vest in the Attorney General

Under the current constitution prosecutorial powers vest in the Attorney General⁸¹. This position was confirmed by the Court of Appeal in *Jopley Constantine Oyieng v Republic*⁸² where it was held that "...only the Attorney General has the right under section 26 of the Constitution to institute criminal proceedings..."

The effect of this is that the shortcomings that have for a long time plagued the prosecutorial function in this country will affect the prosecution of money laundering. Some of the shortcomings include staff shortage, ill trained prosecutors, corruption, and unnecessary adjournments among others. Of great concern especially is the use of police prosecutors who have been criticized as being incompetent and corrupt.

In the United Kingdom, whereas the prosecutorial function vests in the Director of Public Prosecution, recent Court of Appeal decisions conferred upon the Financial Services Authority (FSA) the power to prosecute money laundering offences under the Proceeds of Crime Act 2002 (POCA). Whereas, the FSA is a designated prosecutor for offences under the Financial Services and Markets Act 2000 (FSMA) itself by section 401, the

⁷⁸ Part IV

⁷⁹ Section 52

⁸⁰ Section 107

⁸¹ Section 26(3) Constitution

⁸² Criminal Appeal Number 45 of 1988

FSMA is silent on whether the FSA can prosecute money laundering offences under POCA.

In the cases of *R v Rollins*⁸³ and *R v McInerney*⁸⁴, It was argued on behalf of Rollins and McInerney that the FSA's powers are as conferred by FSMA and do not extend beyond FSMA. Accordingly the FSA had no power to prosecute offences, including money laundering, which are not mentioned in FSMA. The FSA argued that it had the right to prosecute other offences as a private prosecutor. The Court of Appeal agreed with the FSA and held that whilst FSMA confers specific powers on the FSA, it does not limit the FSA's powers to those conferred by or under FSMA. The FSA was therefore entitled to prosecute money laundering offences even though they are not mentioned in FSMA, by virtue of the general right of private prosecution contained in section 6 of the Prosecution of Offences Act 1985 and the FSA's memorandum and articles of association.

Whether this argument can be extended to Kenya is highly debatable. Whereas the right of private prosecution is recognized in section 26(3) (b) of the constitution which empowers the Attorney general to “*take over and continue any such criminal proceedings that have been instituted or undertaken by another person or authority.*” such a right can only be invoked under section 88 of the Criminal Procedure Code which confers the right subject to the permission of any magistrate trying the case. Furthermore, case law imposes certain conditions to be fulfilled by the magistrate. These conditions were stated by the High Court in the case of *Richard Kimani and M Maina v Nathan Kahara*⁸⁵ and include:

1. the magistrate should ascertain whether a report has been made to the Attorney General or police and with what result
2. the magistrate should also ascertain that the complainant has *locus standi*

It is therefore clear that the magistrate does not have absolute discretion on this matter. The fact that the magistrate must ascertain that a report has been made to the Attorney General or police is a major setback in instituting private prosecution. Furthermore,

⁸³ [2009] EWCA Crim 1941

⁸⁴ [2009] WLR (D) 294

⁸⁵ High Court criminal (revision) case number 11 of 1983

unlike the FSA none of the institutions created under the Act have been granted any prosecutorial powers by any existing written law.

Therefore unless the law is changed to vest prosecutorial powers in one of the institutions, prosecuting money laundering offences will be a major hurdle..

4.6.2 Differentiating between 'Clean' and 'Dirty' Money is Difficult

Distinguishing between clean and dirty money is extremely difficult. Exactly when laundered money becomes 'clean'-in the placement, layering or integration phase is unclear. When laundered funds are layered they are likely to become mixed up with legitimate money. Economically speaking, laundered money is diluted like a drop of ink in the flow of finance making it difficult to detect⁸⁶.

Furthermore, the fact that some people conduct both legitimate and illegitimate businesses means that it will be difficult to detect illegal proceeds where such a person infuses the proceeds from his illegal activities into his legitimate business as a way of placing and layering money.

4.6.3 Trust Companies/Trust Account Holders

Trust companies have for a long time created an increased risk in so far as conventional money laundering is concerned because of their capacity to conceal the identities of the beneficial owners.

Accordingly, the fact that neither trust companies nor trust account holders are not reporting institutions within the meaning of the Act and the fact that these are avenues being used by mobile network operators to evade the application of the Banking Act provides an avenue for money laundering using MMT services. Such entities cannot be prosecuted for failure to meet reporting obligations under the Act.

⁸⁶ The Scale and Impacts of Money Laundering , Unger Brigitte,Utrecht School of Economics, Utrecht University, the Netherlands, Edward Elgar Publishing,2007, Cheltenham UK

4.6.4 Lack of Universal Criminalization of Money Laundering

Not all countries have enacted domestic legislation criminalizing money laundering. In addition, even if they have enacted domestic legislation, the approach used in defining predicate offences differs. Whereas Kenya adopts the all crimes approach some countries adopt a selective approach hence not all crimes are predicate offences for purposes of money laundering.

This poses a great risk in so far as combating money laundering since proceeds which would ordinarily be illegal can be used invested in Kenya legally since they do not constitute proceeds of crime. Kenya requires double criminality. In the same way, proceeds from a crime in Kenya can easily be laundered to a country which does not criminalize the predicate offence.

Mobile money transfer is currently operating across borders. Both Safaricom and Zain allow for cross border transactions. It is extremely important to ensure that these companies do not expand to countries which do not have anti money laundering legislation.

4.6.5 Corruption and Overlap with the Anti Corruption and Economic Crimes Act 2003 (ACECA)

Section 47 of ACECA makes it an offence of corruption to deal with property that one believes or has reason to believe is the proceeds of a corrupt act. This overlaps with the Proceeds of Crime and Anti Money Laundering Act which makes it an offence of money laundering to deal with proceeds of crime. The effect of this overlap is that a person charged for corruption under section 47 ACECA will also be charged for money laundering under sections 3,4 or 5 of the Proceeds of Crime and Anti Money Laundering Act. These two crimes carry different penalties. The AML penalties are extremely punitive in nature yet equality of the seriousness of the two offences is highly debatable.

In the 2009 Transparency International Corruption Perception Index, Kenya was ranked 146th out of 180 countries samples. In addition, the Police Force was ranked as the most corrupt public institution with the courts following closely behind despite the fact that we

have enacted anti corruption legislation. The Anti Corruption and Economic Crimes Act 2003 and Public Officers Ethics Act 2003 were enacted to combat corruption but have so far not achieved the expected results.

With such high levels of corruption in the judiciary and police force it is very clear that combating money laundering will be extremely problematic.

4.6.6 False Identities

Presently, mobile network operators only require an individual's national identity card as evidence of identity. Whereas this requirement is premised on the notion that since the aim of mobile money transfer is to reach the unbanked who more often than not live in informal settlements or the rural areas and hence other forms of identification will be difficult to obtain, reliance on the national identity card is extremely risky.

The Kenyan national identity card has often been criticized for being easy to forge furthermore Kenya does not have a centralized identification data base that can easily reconcile the individuals born in Kenya, those taking up identity cards and those who have died. Consequently, the use of identity cards of dead people is extremely common. With such risks posing a serious identification challenge

5.0 CHAPTER FIVE

SUMMARY OF FINDINGS AND RECOMMENDATIONS

5.1 INTRODUCTION

This chapter will seek to summarize the findings and make recommendations on what provisions need to be changed or included in the Act in order to make it effective in combating money laundering through mobile money transfer services.

5.2 FINDINGS

Mobile money transfer services as currently constituted are not easily susceptible to money laundering in so far as the transaction involves the traditional high value transactions this is because, the current transaction limits make it unattractive to money launderers. Safaricom for instance has a transaction limit of Kshs. 35,000 thus laundering larger sums means using several transactions and this will definitely be categorized as suspicious.

However, money laundering can still involve smaller sums a technique commonly referred to as 'Starburst.' This consists of a deposit of dirty money made in a bank with standing instructions to wire it in small, random fragments to hundreds of other bank accounts around the world, in both onshore and offshore financial centers (OFCs)⁸⁷ this strategy can be used with MMT. Thus money laundering. Laundering is still possible especially where the nature or character of money laundering changes. Money launderers do react to changes in laws and regulations thus it will not be surprising if the mobile money transfer service is used to launder smaller amounts over a longer period of time. Furthermore, the increased partnership with the banking sector also poses a significant threat to the increased use of MMT to launder funds.

⁸⁷ See: Patricia Martin, " Un juez investiga pagos a ETA en paraíso fiscales" El periodico, July 12,2006 See also; Donato Masciandaro (2004). Global financial crime : terrorism, money laundering and offshore centres. Aldershot, Hants, England ; Burlington, VT, Ashgate. and Veronique Maurus, " L' argent noir du terrorisme" *Le Monde*. Paris, November 4-5, 2001: 13-18

Additionally, MMT services can further be used as channels for terrorist financing this is because of the following reasons:

1. Unlike money laundering, terrorist financing transactions tend to be smaller and much less observable.
2. Kenya does not have any domestic legislation criminalizing terrorism. The absence of such legislation means that supervising entities are under no obligation to verify such transactions and take the necessary legal action.
3. The lack of a single global definition of terrorism means that the crime has no definition hence cannot be legally deemed to exist.
4. The nature of the crime of terrorism. Terrorists operate in cells. There is a lot of division of labor such that there are a number of people playing different roles yet they do not know each other. Their only link is strict adherence to instructions. Thus MMT can easily fund terrorist activities
5. Weak identification systems which can easily be forged.

So great is the role played by money laundering in financing terrorism that the former President of the USA President Bush stated that he wanted a precise tracing of money in order to fight terrorism. . Much of the terrorist financing for September 11 is thought to have used the same channels as money laundering, including techniques such as “starburst” (deposits are made in small random fragments) and the “boomerang,” where funds are sent on a long journey before returning to the country of origin...⁸⁸

5.3 RECOMMENDATIONS

Based on the analysis of the various provisions of the Act in relation to prevention and punishment of money laundering through mobile money transfer services, the following recommendations can be made:

5.3.1 Establish A Supreme Financial Regulator

The rapid growth of MMT services in both the telecommunication and banking sector and the absence of a clear legislative framework is of great concern since unregulated

⁸⁸ Economist (2001) Getting to them through their money: Terrorist finances. Finance & Economics. Sep 27th. http://Economist.com/displayStory.cfm?Story_ID=798424

financial services can damage the integrity of a country's economy. A major reason for this state of affairs is the immense benefit derived from MMT services. This service has greatly revolutionized the provision of financial services to the unbanked segment of society. In addition, the long process of making laws does not help this situation.

It is therefore recommended that a financial service regulator be created with express authority to enact delegated legislation for the provision of financial services. This can be similar to the Financial Services Authority of the UK which is created under the Financial Services and Markets Act 2000 (FSMA) a regulator for insurance, investment business and banking. Section 2 of the Act outlines the objectives of the FSA as

- (a) Market confidence;
- (b) Public awareness;
- (c) The protection of consumers; and
- (d) The reduction of financial crime.

Due to the rapid growth, of MMT services in the country, there is a need to ensure that regulation is created expeditiously. Having such a body with delegated legislative authority will to a large extent remedy the slow pace of legislation in the country. Furthermore, such a body will have the flexibility needed by MMT services to facilitate growth into other sectors of the economy while at the same time maintaining the integrity of the country's economy.

In addition, extending prosecutorial powers to such an authority for purposes of financial crime will greatly help in the fight against money laundering.

The fact that the Central Bank of Kenya is stretching its supervisory powers to MMT poses a risk that in the event of a court proceeding, it can be declared as having *no locus standi* in the matter since it is acting *ultra vires* to the authority granted to it by statute. Thus having a financial authority will be able to remedy this situation by enacting legislation that gives it the prerequisite powers to effectively regulate MMT.



5.3.2 Introduction of Risk Based Customer Due Diligence

The requirement to conduct customer due diligence is imposed on all reporting institutions. However the costs for conducting this exercise are relatively high. Accordingly, it is not fair to impose the same standard of customer due diligence on both high risk and low risk reporting institutions.

Mobile money transfer is a low risk service and such stiff regulations can act as an impediment to growth of the service. In order to prevent this it is highly recommended that a risk based approach similar to the one in operation in the UK (see Chapter 2) is adopted in Kenya

5.3.3 Directive on Predicate Offences

The double criminality requirement set out in the Kenyan Act is a major impediment to fighting money laundering. It is therefore essential that a directive be put in place that mobile network operators can only extend mobile money transfer services to countries that have not only enacted anti-money laundering legislation but which have also adopted the dual criminality approach to predicate offences

5.3.4 Granting Prosecutorial Powers to an Independent Body

The fight against money laundering will definitely be made more efficient and effective if prosecutorial powers are granted to one of the institutions created under the Act or another independent body. Currently, the attorney-general's office is ill equipped to adequately prosecute such cases due to shortage of trained staff, corruption and backlog of other cases

5.3.5 Tougher Transaction Monitoring and Reporting Guidelines

There is an urgent need to enact special transaction monitoring and reporting guidelines for MMT. The following two key elements must be taken into serious consideration when enacting MMT guidelines:

1. Transaction Volume
2. Transaction Velocity

5.3.5.1 Transaction volume

Currently the reporting threshold for all reporting institutions is USD 10,000. This threshold is too high for MMT and therefore ineffective. This vacuum necessitated MNOs to develop internal transaction limits. For example the transaction limit for M-Pesa is Ksh. 35,000.

The fact that the statutory reporting threshold does not apply means that MNOs are technically exempt from reporting obligations provided for in the Act. Since the Act requires the reporting of suspicious transactions. Furthermore, MNOs are denied the statutory defence provided for under section 7 for persons charged with money laundering under sections 3,4 and 5.

It is therefore important for the Act to be amended or regulations enacted by the Minister providing for transaction volumes for MMT services.

5.3.5.2 Transaction velocity

Clear guidelines need to be enacted regulating transaction velocity. The current practice is unclear and a person can easily be identified as conducting suspicious transactions when in fact he is conducting legitimate business.

The only requirement is that customers observe the transaction limit for each transaction conducted. There is a vacuum in so far as the number of transactions a person can make in a day if for example each transaction conforms to the transaction limit. For example can a person make 10 transactions of Kshs 35,000 each per day? Such grey areas need to be clarified

5.3.6 Inclusion of Trust Account Holders/Trust Companies as Reporting Institutions

Trust companies/trust account holders are not reporting institutions for the purposes of the Act. The current practice is that the Central Bank of Kenya has extended its

supervisory authority to these entities. This is despite the absence of legislation to that effect. CBK is therefore creating powers it is not mandated to exercise. By including these entities as reporting institutions, they will be duty bound to adhere to the reporting obligations set out in the Act. Furthermore, CBK will have authority as a supervisory authority under the Act.

5.3.7 Omission or Amendment of Section 8

Section 8 creates the offence of money laundering for any person who receives or transmits money with intent to commit an offence. What this section does is that financing of any crime or receiving money to commit a crime constitutes money laundering. This goes against the main purpose of money laundering which is to conceal the illegal identity of funds. Financing of any crime does not in any way conceal the illegal identity of funds nor is receiving money in order to commit an offence.

This section should therefore be omitted since the essential ingredients of the crime of money laundering are captured in sections 3, 4, and 5.

5.3.8 Clarification of Overlap with Anti Corruption Legislation

Section 47 of the Anti Corruption and Economic Crimes Act 2003 (ACECA) makes it an offence to deal with proceeds of corruption. Such dealing also constitutes money laundering under sections 3, 4 or 5 of the Proceeds of Crime and Anti Money Laundering Act 2009. This basically means a person charged with corruption under section 47 is also guilty of money laundering. This overlap will cause problems in so far as coordinating investigations and also with regards to prosecution. In so far as coordination is concerned, a problem could arise in so far as determining the jurisdictional boundaries of the Kenya Anti Corruption Commission and the institutions established under the proceeds of Crime and Anti Money laundering Act.

Accordingly, the AML Ac needs to be amended to reflect jurisdictional boundaries in so far as corruption is the predicate offence

5.3.9 AML Training For Law Enforcement Agencies

The institutions created under the Act and the Judiciary will only be effective if they are staffed with staff conversant with preventing, detecting and investigating money laundering. There will therefore be a need for such training. Capacity building is therefore extremely necessary

Furthermore, since the Attorney General's office is tasked with the prosecutorial function, such training should also be extended to the staff. This is because lack of training has been a major impediment to the successful prosecution of technical cases.

5.3.10 Customer Identification System

Customer identification is extremely important in order to facilitate the arrest and prosecution of suspected money launderers.

There is therefore an urgent need for the government to set up a computerized and updated database of all Kenyans in order to facilitate ease of identification. The database can be used to enhance CDD in the sense that it will be relied on to verify data given by clients after they have filled in the activation/account opening forms. Should the information not tally such accounts must either be frozen immediately or monitored closely.

To further reinforce verification of customer identity, the adoption of compulsory SIM card registration of all customers by MNOs will be extremely helpful. Except for a presidential directive which has no legal force, there is no regulation in Kenya to support this exercise. Presently, South Africa is leading in this exercise. Analysts have however argued that compulsory registration will have a negative impact on the uptake of mobile telephone services and also result in a reduction in subscriber numbers. According to a report by IHS Global Insight, an economic forecast group, "The introduction of mandatory registration of SIM cards in at least 10 countries has resulted in a dramatic

UNIVERSITY OF NAIROBI LIBRARY
P. O. Box 30197
NAIROBI

slowdown in subscriber growth and will see the disconnection of millions of unregistered subscribers.”⁸⁹

This decline is however in the short run but in the long run, the situation will stabilize. Hence there is no need to worry that the gains achieved so far by MMT services will be lost by the mandatory SIM card registration.

5.3.11 Provision For Inchoate Offences

The Act is silent on dealing with inchoate offences. Thus aiders and abettors will be charged for the full offence of money laundering. It is highly recommended that provision for inchoate offences be made due to the fact that it is extremely difficult to identify all the offenders especially in the case of international transfers. Thus charging persons for the role they played will ensure more convictions and hence act as deterrence to prospective money launderers.

⁸⁹ Adopted from David Lewis article *SIM Card Rule Threatens Africa Mobile Growth* .Business Daily Friday June 18, 2010 p12

ANNEX 1

Appendix 1 Chart 1: E-money Attributes:

Appendix 1 to Annex 1 of PLEN/19.REV 1

E-MONEY SYSTEMS ATTRIBUTES SOME SIMPLIFIED GENERALIZATIONS FOR DISCUSSION*

| CURRENT PAYMENT SYSTEMS | E-MONEY SYSTEMS |
|---|--|
| High degree of central bank control | Various national views re: control |
| Highly structured supervision/regulation | Highly, technical yet to be designed |
| Large legal and policy literature | Applicability of existing laws/regs undetermined |
| Physical means of payment--checks, currency | Intangible electronic analogs |
| Huge infrastructure established worldwide | Downsized, computer-based |
| Relatively labor intensive | relatively capital intensive |
| High value infrastructure--brick and mortar | Low cost decentralized facilities |
| Bank-dominated wire transfers | Personal computer transfers |
| Check-dominated consumer payments | Cyber currency-dominated |
| Velocity of money is low | Velocity of money is high |
| Bank-dominated intermediaries | Non-traditional intermediaries- |
| Clearing mechanism required | clearing requirements reduced/eliminated |
| Transportation--couriers, land, sea, air | Telecommunications |
| Worldwide use of certain currencies | Easy currency exchange/one currency |
| Serial numbers and bank records | Enciphered messages |

Significant statistical data collection

No methodology for money supply statistics

Economic national borders borders

Amorphous political & economic

Defined jurisdictions

Overlapping, unknown jurisdictions

Generally non-refutable, standard methods of validation

Evolving methods of transaction verification

Fungible

System specific convertibility to cash

Authentication, established structure to verify authenticity

Undetermined, system specific and may involve a third party

*This example refers to the United States and is included for illustrative purposes only:

Source: *Cyberpayments: An Introductory Survey*, FinCEN, September 27, 1995

BIBLIOGRAPHY

Anne Kiunue: Business Daily, *Mobile Banking Laws Should not Restrict Capital Inflows* Wednesday December 30th 2009

Anne Kiunue, *Why Kenya Needs Watertight Laws to Combat Money Laundering*, Business Daily, 24th Feb, 2009, pg 9

Brigitte Unger *The Scale and Impacts of Money Laundering*, Utrecht School of Economics, Utrecht University, the Netherlands, Edward Elgar Publishing, 2007, Cheltenham UK

Dept of Treasury (Treasury) *The National Money Laundering Strategy for 2000*, (March 2000), at <http://www.treas.gov/press/releases/docs/ml2000.pdf>

Donne J, *Research Approaches to Mobile Use in the Developing World: A Review of the Literature*. *The Information Society* 24(3)2008

Economist (2001) *Getting to them through their money: Terrorist finances*. Finance & Economics. Sep 27th. http://Economist.com/displayStory.cfm?Story_ID=798424

Elena Madalina Buuioic, *Predicate Offences- The Achilles Heel of Anti-Money Laundering Legislation*, Chapter 2 in Brigitte Unger *The Scale and Impacts of Money Laundering*. Edward Elgar Cheltenham, UK. Northampton, MA, USA 2007

FATF-VIII Money Laundering Typologies Exercise Public Report, Organization for Economic Co-operation and Development (OECD) 5 February 1997

George Kegoro, "Profiling Money Laundering in Eastern and Southern Africa," an Overview of Capacity: Volume One Chapter 5 "Money laundering Patterns in Kenya," Institute for Security Studies Monograph 90

GSM Association: *An introduction to the MMT Regulatory Environment* PDF Document http://www.gsmworld.com/ourwork/mobile_lifestyle/mobile_money/mobile_money_transfer/index.htm

GSMA: *Enabling Regulatory Environments for Mobile Money Transfer Services*. Public White Paper version 1.0 March 2008

Indran Medhi, S.N Nagasema Gaulana, Kentara Toyama: *A Comparison of MMT Uiss for Non-Literate and Semi Literate Users*

J.D Agarwal & Aman Agarwal, *Keynote address on Money Laundering: New Forms of Crime Victimization (Current trends and Modus Operandi)* National Workshop on "New Forms of Crime Victimization with reference to Money Laundering", organized by the

Indian Society of Victimology, Department of Criminology, University of Madras, Chepauk, Chennai, INDIA, on 18th November 2006

John McDowell & Gay Novis, “*The Consequences of Money Laundering & Financial Crime,*” *Economic Perspective, an IIP Electronic Journal*(May 2001) <http://usinfo.state.govt/topical/econ/groups8/summit01/wwwwh01050101html>

Paul Hynes, Richard Furlong, Nathaniel Rudolf; *International Money Laundering and Terrorist Financing: A UK Perspective*, Sweet & Maxwell, 2009

Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance, CGAP Publication, January 2008

Ringguth J, *Money Laundering-The Criminal Dimension*, Paper presented at the “Stop Money Laundering” Conference, 26 February 2002 London

Sonia Arenaza: *End User Benefits Enabled Applications to Financial Services: Regulatory Policies on Universal Access*. 8th September, ITU Geneva www.mobilein.com/MobileMoneyTransfer PPT:

UN General Assembly, *Special Session on the World Drug Problem*, Fact Sheet 5: Money Laundering (June 8-10,1998) available at <http://www.un.org/ga/2ospecial/presskit/themes/moeny-5.htm>

William C Gilmore, “*Money laundering: the international aspect*”, in David Hume Institute, *Money Laundering* (Hume papers on Public Policy, vol 1, No 2) Edinburgh, Edinburgh University Press, 1993, 1 at