

**SECURITY OF MOBILE MONEY TRANSFER IN
TELECOMMUNICATION INDUSTRY IN TANZANIA**

SECURITY OF MOBILE MONEY TRANSFER IN TELECOMMUNICATION INDUSTRY IN TANZANIA

**By
Shamte Mikumuo**

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Award of the Degree of Master of Science in Marketing Management (MSc-MKT) of Mzumbe University.

2013

CERTIFICATION

We, the undersigned, certify that we have read and hereby recommend for acceptance by Mzumbe University, a dissertation entitled **Security of Mobile Money Transfer in Telecommunication Industry in Tanzania**, in partial fulfillment of the requirements for the award of the degree of Master of Business Administration of Mzumbe University.

.....

Major Supervisor

.....

Internal Examiner

.....

External Examiner

Accepted for the Board of MUDCC

.....

CHAIRPERSON, FACULTY/DIRECTORATE BOARD

DECLARATION

I, Shamte Mikumuo, declare that this dissertation is my own original work and that it has not been presented and will not be presented to any other University for similar or any other degree award.

Signature_____

Date_____

COPYRIGHT

© 2013

This dissertation is a copyright material protected under the Berne Convention, the Copyright Act 1999 and other international and national enactments, in that behalf, on intellectual property. It may not be reproduced by any means in full or in part, except for short extracts in fair dealings, for research or private study, critical scholarly review or discourse with an acknowledgement, without the written permission of Mzumbe University, on behalf of the author.

ACKNOWLEDGEMENTS

Thanks and foremost, I would like to sincerely thanks my supervisor, Mr.Makuru Ngemba for his support especially for his guidance in me, his comments and questions and advice were very beneficial in my completion this study. I learnt from his insight a lot.

I have to thanks my lovely parents Mr. & Mrs Milanzi, my lovely & sweetheart wife Haika Maleko and my beautiful daughter Nureen Milanzi for their love and support throughout my life. Thanks you both for giving me strength to reach for the stars and chase my dreams. My sister and uncle deserve my wholehearted thanks as well.

To all my friends and school mates, thanks you for your understanding and encouragement in the all moment. Your friendship makes my life a wonderful experience. I cannot list all the names here but Zephania, Titus, Mrosso, Tausi and Lillian you will always be on my mind.

Thanks you, Lord, for always being there for me.
This thesis is only beginning of my journey.

DEDICATION

This dissertation is lovingly dedicated to my dad, the late Mwishehe Milanzi- Peace be upon him and my brilliant lovely mom Sadda Ibrahim whose words of encouragement, support, endless love and push for tenacity ring in my ears throughout my life.

This dissertation is also dedicated to my loving and supportive wife, Haika Maleko, our exuberant, sweet, kind-hearted & beautiful little girl, Nureen Milanzi- may you be motivated and encouraged to reach your dreams.

Lastly, this dissertation is dedicated to our new baby boy, Ibrahim Milanzi- may you also be motivated & encouraged to reach your dreams and live in the name of Allah.

ABBREVIATIONS

AML	-	Anti-Money Laundering
BOT	-	Bank of Tanzania
DSTV	-	Digital Satellite Television
EAC	-	East African Community
EPOCA	-	Electronic and Postal Communications Act
IBM	-	International Business Machines
KYC	-	Know Your Customer
MFI	-	Micro Finance Institutions
MMT	-	Mobile Money Transfer
MNO	-	Mobile Network Operators
MP	-	Mobile Payment
PDA	-	Personal Digital Assistant
PIN	-	Personal Identification Number
P2B	-	Personal to Business
P2P	-	Person to Person
SP	-	Service Provider
SMS	-	Short Message Service
STK	-	SIM Tool Kit
SIM	-	Subscriber Identity Module
TCRA	-	Tanzania Communications Regulatory Authority
TING	-	Tanzania Integrated Network Group
TRA	-	Tanzania Revenue Authority
UMMAA	-	Uganda Mobile Money Agents Association
USSD	-	Unstructured Supplementary Service Data
VAS	-	Value Added Service
VTL	-	Vodacom Tanzania Limited

ABSTRACT

This study was done to examine the level of security of mobile money transfer in Telecommunication industry in Tanzania as insecurity resulted to frauds for Mobile money customers and reduce profits for mobile money operators in Tanzania in the years to come.

Despite a lot of efforts done by TCRA and BOT still Mobile Money seemed to have paved an easy way of swindling, causing fraud for Tanzania mobile money consumers. Fraud did not only take place during interactive transfers, but has also expanded towards fake hard, money laundering circulating cash and operating system used in the mobile money sector.

Data were collected by undertaking survey from sample obtained by using primary and secondary data collection method. These instruments enabled to obtain data from various units of enquiry. Collected data were summarized, classified, presented and analyzed using readily technology available to research, MS- Excel, where necessary, specialized software and SPSS were used.

The findings from this study indicated that 79.5% are aware of the electronic money transfer, 46% knows methods used to transfer E-money, 54% know mobile money operating system and 99.5% of respondents were not experience any Fake money in electronic money transfer since they start to use the service.

It was concluded that, despite of little awareness of the mobile money methods and operating systems used in transferring electronics money from one customer account to another, still mobile money transfer is safe to both customers and telecommunication companies that are providing mobile money transfer services.

To enhance security of Mobile Money transfers, the mobile money operators should increase advertisements regarding customer's awareness on the important of not sharing mobile money PIN because 13% of customers are sharing E- money PIN. Also should come up with new systems that accommodate new technology which does not allow any mobile money transactions that are stacking, this means all mobile money customers will be allowed to use STK SIM card instead of normal SIM cards that are delaying in getting notification SMS.

TABLE OF CONTENTS

	Pages
CERTIFICATION	i
DECLARATION.....	ii
COPYRIGHT	iii
ACKNOWLEDGEMENTS.....	iv
DEDICATION.....	v
ABBREVIATIONS	vi
ABSTRACT	vii
TABLE OF CONTENTS.....	viii
LIST OF TABLES	xi
LIST OF FIGURES	xii
 CHAPTER ONE	 1
INTRODUCTION.....	1
1.0 Background Information	1
1.1 Statement of the Problem	2
1.2 Research Questions	2
1.2.1 General Research Question	2
1.2.2 Specific Questions.....	2
1.3 Research Purpose	3
1.3.1 Main Research Objective;	3
1.3.2 Specific Research Objectives;.....	3
1.4 Significance of the Study	3
1.5 Limitation of the Study	4
 CHAPTER TWO	 5
LITERATURE REVIEW.....	5
2.0 Theoretical Literature Review.....	5
2.1 Customers awareness in Mobile Money Transfer.....	5
2.1.1 Customers awareness during Registration	5
2.1.2 Methods used in Transferring Mobile Money	6
2.1.3 Safety in Mobile Money Operating Systems	6
2.1.4 Fake Notes in Mobile Money Services	7
2.2 Empirical Literature Review	7
2.2.1 Growth Pattern & Teledensity (Population Coverage) of Mobile Money	7
2.2.3 Trends of Telephone Subscription in Tanzania	8
2.2.4 Mobile Money Usage integration	9
2.2.5 Financial Inclusion	11
2.3 Conceptual Framework of the Study.....	11
2.3.1 Transfer Methods of Mobile Money	12
2.3.2 Operating systems of Mobile Money	13
2.3.3 Customer Care and Customer awareness	14
2.3.4 Fake money circulation in Mobile money transfer	14
2.3.5 The Mobile Money Transfer Environment and Its Stakeholders.....	14

2.3.5.1	Mobile Network Operators	16
2.3.5.2	Financial Institutions.....	16
2.3.5.3	Responsibility of Mobile Money Agents	17
2.3.5.4	Regulator's role in securing mobile money.....	18
2.4	Research Gap	19
CHAPTER THREE		20
RESEARCH METHODOLOGY		20
3.0	Area of the study	20
3.1	Research Design.....	20
3.2	Population of the Study.....	21
3.3	Sample size and sampling technique	21
3.3.1	Convenient Sampling	22
3.3.3	Cluster Sampling.....	23
3.4	Data Collection Methods and Instruments	23
3.4.1	Data Collection Methods.....	23
3.4.2	Primary Data	23
3.5.3	Secondary Data	25
3.6	Data analysis	25
CHAPTER FOUR.....		27
DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS ...		27
4.0	Introduction	27
4.1	Characteristics of Respondents	27
4.1.1	Respondents by Sex	27
4.1.2	Respondents by Age.....	28
4.1.3	Respondents by Education Level	29
4.1.4	Respondent's Registration to different Mobile money services	30
4.1.5	Understanding of Mobile Money Services	32
4.2	Uses of Mobile Money in transferring E-money	32
4.2.1	Familiarity of the Method Used in Transferring E-Money.....	32
4.2.2	Various Method Used in Transferring E-Money	33
4.2.3	Use of Mobile Money to Transfer Money to Relatives & Friends	34
4.2.4	Frequency of Use of Mobile Money Service	34
4.3	Whether or Not Mobile Money Transfer is Safe Means of Transferring Money	35
4.4	Experienced Mobile Money Security Problem in Transferring E-Money.....	36
4.4.1	Experienced Security Problems by Gender.....	37
4.4.2	Experienced Security Problems by Age Group	37
4.4.3	Experienced Security Problems by Level of Education.....	38
4.5	Mobile Money PIN Sharing	39
4.5.1	With Whom Mobile Money Password/PIN Is Shared	40
4.5.2	PIN Sharing is Hindering Security of Mobile Money	41
4.5.3	Security risks in sharing or exposing MM PIN/Password with other person.....	41
4.5.4	Relationship between PIN sharing and experiencing loss security problems.....	42

4.5.5	E-money stolen/lost in unknown way since started to use Mobile Money transfer service	43
4.6	Understanding of Money Laundering in Mobile Money	44
4.7	Money Laundering Affect Mobile Money Service Security Wise	44
4.8	Mobile Money Operating System	45
4.8	Identification of Mobile Money Transfer Methods	46
4.9	Safety in Mobile Money Procedures.....	47
4.9	Customer Awareness on Mobile Money Security Provided by MMO	48
4.9.1	Deposit Fake money to Mobile Agent	49
4.9.2	Withdrawn Fake Money from Mobile Agent	49
4.9.3	Cause of Fraud in Mobile Money Transfer - company side	50
4.9.4	Causes of fraud in Mobile Money Transfer – customers side	51
4.10	Security of Mobile Money is nowadays increased compared to previous years	52
CHAPTER FIVE.....		53
CONCLUSION AND RECOMMENDATION		53
5.0	Introduction	53
5.1	Summary of the Discussion	53
5.2	Conclusion	55
5.3	Recommendations/ Policy Implication of the Research	55
5.3.1	Mobile Money PIN Sharing	55
5.3.2	Security of Mobile Money Agents	56
5.3.3	Security procedure during E-money withdraw	56
5.3.4	Confirmation during transferring E-money	57
5.3.5	Anti-Money laundering.....	57
5.3.6	Mobile Money operating system.....	58
5.4	Further Study.....	58
REFERENCES.....		59
APPENDICES		62
Appendix 1: Time Schedule and Budget		62
Appendix 2: Questionnaire for determining security level of Mobile Money transfer in Telecommunication Industry in Tanzania.		63

LIST OF TABLES

	Pages
Table 2.1: Tanzania Population Vs Subscriptions.....	7
Table 2.2: Subscribers as at 31st December 2007	8
Table 2.3: SIM card Registration Status as at Dec 2011	9
Table 2.4: The Mobile Money Transfer Environment and Its Stakeholders	15
Table 3.1: Distributions of Respondents per each Telecommunications companies	22
Table 4.1: Respondents by Age	29
Table 4.2: Understanding of Mobile Money Services.....	32
Table 4.3: Use of Mobile Money in Transferring E-money	32
Table 4.4: Familiarity of the Method Used in Transferring E-Money	33
Table 4.5: Use of Mobile Money to Transfer Money to Relatives & Friends.....	34
Table 4.6: Whether or Not Mobile Money Transfer is Safe in Transferring E- Money.....	36
Table 4.7: Experienced Mobile Money Security Problem in Transferring E- Money.....	36
Table 4.8: PIN Sharing In Mobile Money	40
Table 4.9: Relationship in Sharing Mobile Money PIN	40
Table 4.10: E-money stolen in unknown way since started to use MMS.....	43
Table 4.11: Safety in Mobile Money Procedures	48
Table 4.12: Deposit Fake Money to Mobile Agent	49
Table 4.13: Fraud Cause in Mobile Money Transfer - company side	51
Table 4.14: Fraud causes in Mobile Money Transfer – customers side	51

LIST OF FIGURES

	Pages
Figure 2.1: Telephone Lines per Populations (Teledensity)	8
Figure 2.2: Mobile Money Usage integration	9
Figure 2.3: Electronic Money Transfer Process.....	12
Figure 2.4: Security Roles of Mobile Network Operator.....	16
Figure 2.5: Transfer Methods of Mobile Money	13
Table 4.1: Depicts Respondent's Sex.	28
Figure 4.2: Respondents Education Level	30
Figure 4.3: General Service Preference (for all respondents)	31
Figure 4.4: General Service Preference by Gender.....	31
Figure 4.5: Various Methods Used in Transferring E-money	33
Figure 4.6: Frequency of Use of Mobile Money Service	35
Figure 4.7: Experienced Security Problems by Gender	37
Figure 4.8: Experienced Security Problems by Age Group.....	38
Figure 4.9: Experienced Security Problems by Level of Education	39
Figure 4.10: How PIN Sharing Hindering Security of Mobile Money	41
Figure 4.11: Security Risk in Mobile Money PIN Sharing.....	42
Figure 4.12: Relationship between PIN Sharing and Security Problems	43
Figure 4.13: Understanding of Money Laundering in Mobile Money	44
Figure 4.14: Money Laundering Affect Mobile Money Service Security Wise.....	45
Figure 4.15: Money Operating System	46
Figure 4.16: Identification of Mobile Money Transfer Methods.....	47
Figure 4.17: Customer Awareness on Mobile Money Security Provided by MMO	48
Figure 4.18: Withdrawn Fake Money from Mobile Agent	50
Figure 4.19: Security of Mobile Money is Nowadays Increased Compared to Previous Years.....	52

CHAPTER ONE

INTRODUCTION

1.0 Background Information

Mobile Money transfer service started in Tanzania in the year 2008, Vodacom and Zantel being the first telecommunication companies to launch the service famous known as M-Pesa and Ezy-Pesa followed by Airtel-Money and Tigo-Pesa provided by AirTel and Tigo Tanzania respectively. Service has grown rapidly due to huge number of Tanzania population of over 42 million people whereby about a majority of the people still has not got access to banking services.

(<http://www.ippmedia.com/frontend/index.php?l=45351>)

Fraud in Mobile money started to happen when SIM cards were not registered in between the year 2008 to 2009. For security reasons, BOT came up with policy in order avoid fraud and theft of electronic money in the subscriber's accounts and SIM card in general. An administrative order was given by the Tanzania Communications Regulatory Authority (TCRA) that required all SIM cards to be registered by their holders between 1st July 2009 and 31st December 2009 to protect consumers from misuse of communication such as fraud and enable consumers to be identified as they use Value Added Services (VAS) such as mobile banking, mobile money transfer, electronic payments for services such as water and electricity and enhance national security(www.tcra.go.tz/headlines/SimRegPublicNotice).

Despite a lot of transactions, the easy access to finances and a new gateway of trading and effort done by TCRA and BOT still Mobile Money seemed to have paved an easy way of swindling, causing fraud for Tanzania mobile money consumers. Fraud did not only take place during interactive transfers, but has also expanded towards fake hard cash deals and money laundering circulating and operating system used in the mobile money sector.(Gilman, L. & Joyce, M.,2012).

1.1 Statement of the Problem

The main research objective was to examine the level of security of mobile money transfer in Telecommunication industry in Tanzania as insecurity resulted to reduced profits for mobile operators in Tanzania in the years to come (Gilman, L. & Joyce, M.,2012).

Specifically, study was done to examine the transfer method used by telecommunications companies in transferring money in Tanzania in order to know if they were sufficient or not to secure money in mobile money transfer, also examined customers awareness in Mobile money transfer, this helped to understand mobile money customers how familiar they were with the service and if they followed all safety measures to secure E-money. Lastly identified the level at which money operating systems from telecommunication companies were secured as measures to increase security of mobile money transfer in telecommunication industry in Tanzania.

Thus, this study determined clearly the security level of Mobile Money transfer in Tanzania which was not known.

1.2 Research Questions

1.2.1 General Research Question

The main research question was to examine to what extent did Mobile or Electronic money transfers were secured in Telecommunications industry in Tanzania?.

1.2.2 Specific Questions

- (i.) What were the methods used in transferring money in electronic money transfer?
- (ii.) How mobile money operating systems were secured to increase security of mobile money transfer?
- (iii.) What was the level of customer's awareness in Mobile money transfer?
- (iv.) How was fake money circulating in Mobile money transfer?

1.3 Research Purpose

This study aimed at capturing all fraud sources that are used direct or indirect by the users and non users of mobile money services that bring impact to the security of mobile money transfer services.

1.3.1 Main Research Objective;

To investigate level of security of mobile money transfer in Telecommunication industry in Tanzania.

1.3.2 Specific Research Objectives;

- (i.) To examine the transfer method used by telecommunications companies in transferring electronics money.
- (ii.) To identify the level at which money operating systems are secured to increase security of mobile money transfer.
- (iii.) To examine customers awareness in Mobile money transfer service.
- (iv.) To monitor circulating of fake money in Mobile money transfer.

1.4 Significance of the Study

Mobile Money customers and other stakeholders like government and policymakers are interested in supporting similar initiatives that can help in fostering the security of Mobile Money market so that customers can proceed using the service without fear of fraud or any means of losing their electronic money during transfer, withdraw and send money.

Many fraud cases regarding lost of Mobile Money in customers or agents accounts has been reported to various Mobile Money service provider in the last years. An average of about two cases per day has been reported to Vodacom Tanzania Limited (VTL) and Tigo Tanzania respectively for period of December, 2012, this figure indicates there is alarming alert in security of Mobile industry. We real need to understand the root causes of the fraud in order to minimize or eliminate this problem in Mobile Money Market.

1.5 Limitation of the Study

The study involved gathering information from customers who are mobile money transfer users whom are wide distributed in Tanzania. Although the research has reached its aims, but there were some unavoidable limitations;

- (i.) First, because of the time limit; There was insufficient time to conduct research due to the factor that researcher is full time worker thus hindering him to move out of Dar es Salaam city to obtain more research details.
- (ii.) Second, target population; research was conducted on a small size of population in Dar es Salaam city whereby many mobile money customers and operators are available. Therefore, to generalize the results for larger groups, the study should have involved more participants at different regions.
- (iii.) Finally, financial limitation; the researcher had little income to privately sponsoring his studies. Therefore only two hundreds samples were used.

CHAPTER TWO

LITERATURE REVIEW

2.0 Theoretical Literature Review

Mobile phone banking has grown a great deal since in the year 2008. According to data from Future Foundation Research Company, the number of Tanzania users adopting banking by mobile phone has risen from 4.3% in 2008 to 9% in November 2010. In the year 2011 has also seen a rapid increase in this form of banking. Alongside banks, credit card companies, mobile network operators and online payment services have put in place mobile payment/transactional systems. While all these developments enable regular mobile users to save time that they can use for leisure, criminals leverage them to come up with new scams to breach their mobile security and steal their money (Solin and Zerzan, 2012).

2.1 Customers awareness in Mobile Money Transfer

Ninety-five percent of E-money customers are not aware of methods that they use in transferring mobile money whether is STK or USSD also, still some of them are not aware of the risk that can face while you are using mobile money transfers since mobile payment systems are not standard yet, and differ greatly from one service provider to another (Guard, 2012).

2.1.1 Customers awareness during Registration

The mobile security of people using these services is at higher risk than before due to increase of Technology in Mobile money development than customer awareness, some customers are using handset that are using android system which is difficult to operate for illiteracy customers. For someone to be able to use mobile money for the first time, they need to complete two processes—registration and account activation, there is no problem during registration if all presented customer documents are correct, the problem became when customer need to activate mobile money service in his/her handset in which they can need assistance of activation from Mobile money Agent is which the PIN will be known by both customer and Mobile Money

Agent, this is big challenge in which agent can withdraw/transfer E-money from customer mobile money accounts without customers awareness (http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf).

2.1.2 Methods used in Transferring Mobile Money

Many people in emerging economies have to travel far from home to find work and need to be able to send money back to their families so they can pay bills. The cost of money remittance is very high in most of the parts of the world ranging from 3% to as high as 10%. This is the reason why more people depend on informal channels (through friends and family) to remit money or physically deliver the money. Traditionally, this has meant high fees, risky unregulated services, or long expensive trips carrying cash in an unsafe and unpredictable environment. It has been observed that Mobile Money transfer users needed to make fewer trips back home to deliver money and the transaction size also came down with frequent transfers. In contrast with bank, the Mobile Money service is accessible at any time and money can be sent anywhere with reference of Message electronic receipt for security reasons (Morawczynski and Mark Pickens, 2011).

Currently methods used to transfer E-Money are STK and USSD. STK is more efficiency and has easy menu that USSD (Mohit, 2009), but none of these method has elaborate its security in the mobile money transfer.

2.1.3 Safety in Mobile Money Operating Systems

Studies undertaken in several countries, including Brazil, South Africa, Kenya, Malaysia and the Philippines indicate that there are two type of operating system that are used in Mobile Money transfers, these are web interface and direct menu such STK and USSD depending on stakeholder. Web system are mostly used by MNO and Mobile Money Technical support like IBM in controlling financial transactions for customers, Agent and Banks while STK are mostly used by Agents and USSD by customers (Solin and Zerzan, 2012). There is a gap in mobile operating system since there studies did not state why there is distinctive to each mobile stakeholder especially in terms of security.

2.1.4 Fake Notes in Mobile Money Services

Despite the intelligence agencies in India trying their best to unravel the fake currency notes nexus in the country, the unabated circulation of fake notes is severely damaging economic growth and giving a fillip to black economy. Leading economists and thinkers believe the black economy could well touch 50 per cent of the GDP if the situation is not handled on a war footing. "While the actual volume of fake currency notes is low, this money is transacted at high velocity. People circulating it want to get rid of it fast. A lot of it is used for money laundering and to support illegal activities (Rajiv Kumar, 2008).

2.2 Empirical Literature Review

2.2.1 Growth Pattern & Teledensity (Population Coverage) of Mobile Money

While the population of Tanzania is growing at the rate of 3.3% annually, the annual number of Tanzanian subscribing for a Telephone lines grows at an average rate of 48%. Though, the subscription is growing at higher rate than that of population, yet there is still a huge gap as shown in figure 2.1 below.

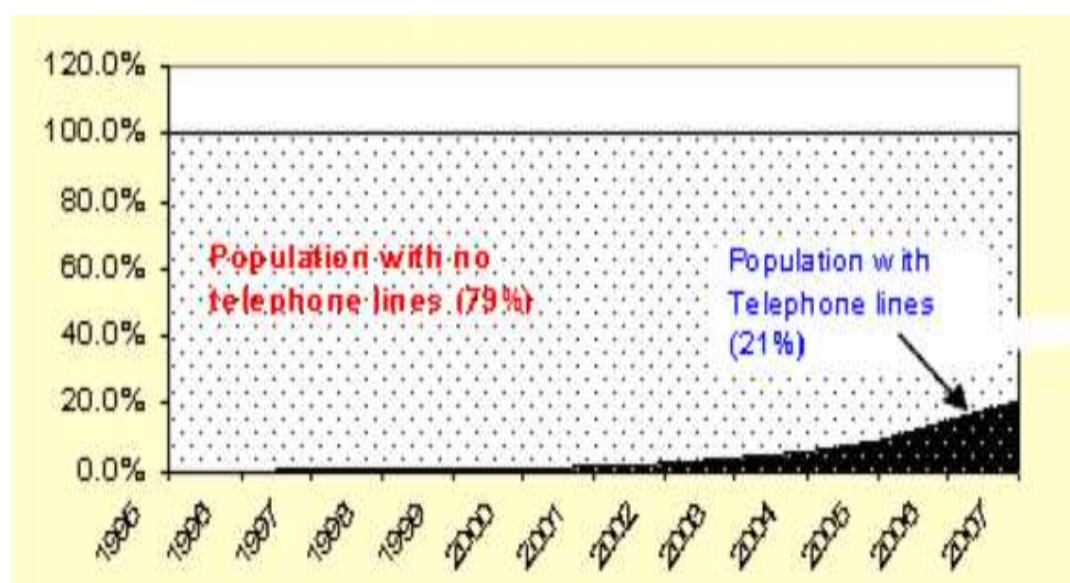
Table 2.1: Tanzania Population Vs Subscriptions

YEAR	POPULATION	SUBSCRIBERS	NON SUBSRCIBERS
1995	29,147,703	90,198	29,057,505
1996	29,963,838	104,200	29,859,638
1997	30,802,826	134,645	30,668,181
1998	31,665,305	157,912	31,507,393
1999	32,551,934	200,320	32,351,614
2000	33,463,388	284,109	33,179,279
2001	33,756,093	453,359	33,302,734
2002	34,161,166	768,449	33,392,717
2003	34,876,231	1,445,006	33,431,225
2004	36,049,581	2,090,360	33,959,221
2005	37,267,530	3,118,157	34,149,373
2006	38,523,907	5,766,566	32,757,341
2007	39,816,363	8,488,774	31,327,589

Source: Gilman, L. & Joyce, M., 2012

Graphical presentation of the underserved population of 31 million people (79%) against telephones lines 8.5 million (21%) as per year 2007 is as depicted below

Figure 2.1: Telephone Lines per Populations (Teledensity)



Source: Gilman & Joyce,2012

2.2.3 Trends of Telephone Subscription in Tanzania

In order to access the Mobile Money service, user must be registered as per TCRA regulation. By 31st December 2007, there were about 8.5 millions voice telephone subscribers. This is an increase of about 47% from 2006. The mobile telecommunication leads the market by having more subscriptions (97%) as compared to fixed line services (3%). For more details see Table 1 below.

Table 2.2: Subscribers as at 31st December 2007

YEAR	FIXED LINES	MOBILE	TOTAL
1995	88,000	2,198	90,198
1996	101,000	3,200	104,200
1997	114,600	20,045	134,645
1998	121,769	36,143	157,912
1999	150,220	50,100	200,320
2000	173,591	110,518	284,109
2001	177,802	275,557	453,359
2002	161,590	606,859	768,449
2003	147,006	1,298,000	1,445,006
2004	148,360	1,942,000	2,090,360
2005	154,420	2,963,737	3,118,157
2006	157,287	5,609,279	5,766,566
2007	236,493	8,252,281	8,488,774

Source: TCRA website 2010

Due to increase the usage of Mobile Money transfer also the number of registered customers has increased rapidly in order to access Mobile Money as means of financing, the table below show the detailed registered as per year 2012.

Table 2.3: SIM card Registration Status as at Dec 2011

	Vodacom	AirTel	Tigo	ZanTel	TTCL	SasaTel	Benson
Subscriber Base	12,317,029	7,664,413	5,613,330	2,347,179	1,048	1,221	1,050
Registered Subscribers	12,301,415	7,289,207	5,509,337	1,203,391	1,048	1,221	1,050
% Registered June 2012	99.873%	95%	98%	51%	100%	100%	100%

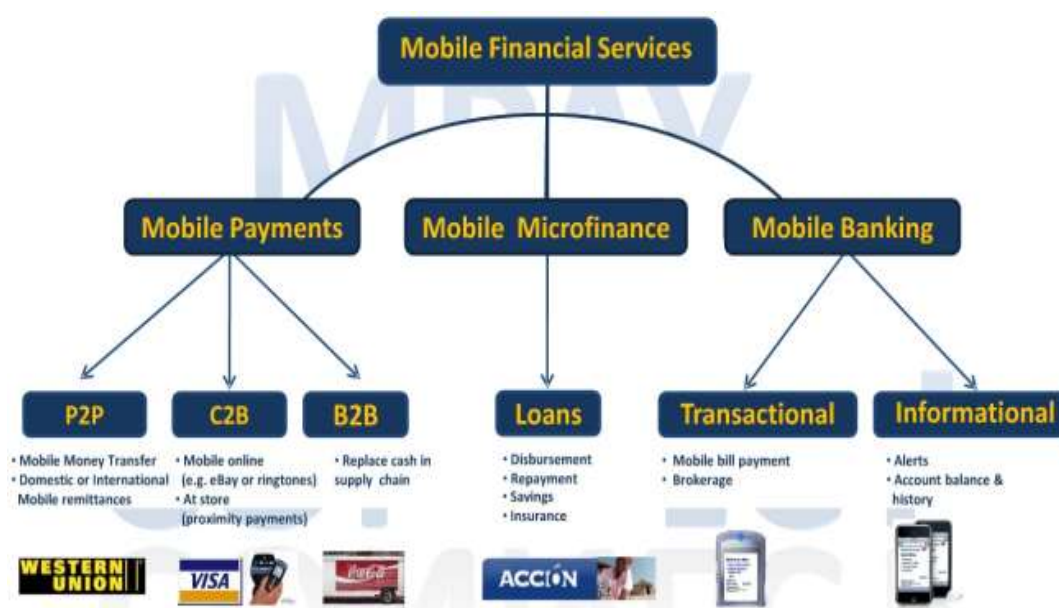
Note: The data of registered SIM Card for ZANTEL is as of March 2012

Source: TCRA website 2012

2.2.4 Mobile Money Usage integration

Terms like mobile money E.g, M-PESA and Tigo-PESA, get tossed around without any real understanding of the differences in systems and outcomes. To help our understanding of these concepts, the diagram below made great presentations on mobile money.

Figure 2.2: Mobile Money Usage integration



Source: Mas, 2009

Mobile money transfer is really mobile financial services, and like traditional financial services, has several parts - mobile payments where money is moved from one account to another, mobile microfinance where money is loaned and expected to be repaid, and mobile banking where money is kept as a safe repository of wealth.

Mobile Money has many benefits, from greater money security to more transparent transactions, but there are two key benefits that we focused on in the Salon.

- (i.) Lowering transaction costs: mPay Connect research shows M-PESA saves 3 hours per day for every Tanzanian subscriber in reduced shoe leather costs - the cost of walking money from place to place. If we multiply 3 hours per day, by 13.2 million subscribers, by 365 days, that's 14.4 billion hours saved per year. Add in the average wage per hour in Kenya, and the time savings start to make you gasp in savings shock.
- (ii.) Increasing business legitimacy: Each business that uses mobile money builds a history of financial activity that they can use for loans, factoring, and even inventory control. It also allows governments to license businesses as such and better estimate and collect taxes. In fact, mobile financial services usually are not creating financial services - many of these systems existed informally through local networks - mobile money is formalizing them and bringing them into the measurable economy.

In India, banks and mobile company are joining forces, while in Bangladesh, BRAC and Grameen Phone have joined to create B-cash, which is promising to be network neutral - that is allow any payment using any mobile operator's system. Overall, there is real convergence - in both payment systems and in the industries that want to participate in them. Recently in Nigeria, 16 companies were given a provisional license to do mobile payments and banking; only 6 are linked to banks and only 1 to a mobile operator (Mas I. & Ng'weno A. 2009).

2.2.5 Financial Inclusion

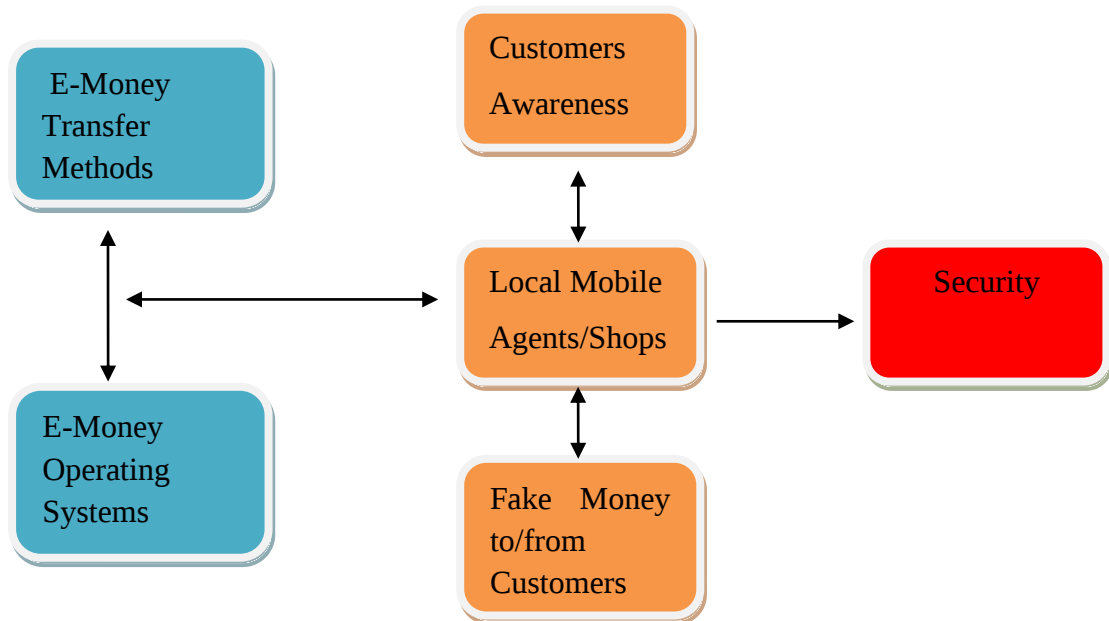
Developing countries are severely constrained by the physical infrastructure of the financial institutions which means that a large part of its population is excluded from the formal banking system. Kenya has just 840 bank branches and 1,510 ATMs that are certainly not sufficient for its 38 million people. M-PESA with its 15k agents is much more accessible to an ordinary Kenyan. M-PESA helped the Micro Finance Institutions (MFIs) to go deeper into remote areas very quickly without substantial increase in the costs.

Financial inclusion has a multiplier impact on the lives of people drawn into the formal financial system which leads to social inclusion. When the poor people get access to financial services, their cash flow management gets better, their financial planning is enhanced and their savings are increased with increased options for providing for themselves for their old age. Mobile Money has brought many unbanked customers under the formal financial system (Camner, G& Sjöblom E, 2009).

2.3 Conceptual Framework of the Study

According to educational researcher (Smyth, 2004), a conceptual framework is a tool researchers use to guide their inquiry; it is a set of ideas used to structure the research, a sort of map that may include the research question, the literature review, methods and data analysis. The influences of customer behavior and Mobile operator in Mobile money transfer in USSD method was used and will help to collect primary and secondary data and analysis the corrected data (M, Chrissy 2011). In this study conceptual frame work has include examination of the transfer method used by telecommunications companies in transferring money, customers awareness in Mobile money transfer, identification of the level at which money operating systems are secured to increase security of mobile money transfer and monitor of circulating of fake money in Mobile money transfer in Tanzania as stipulated in the figure 2.3 below;

Figure 2.3: Conceptual Framework of the Study



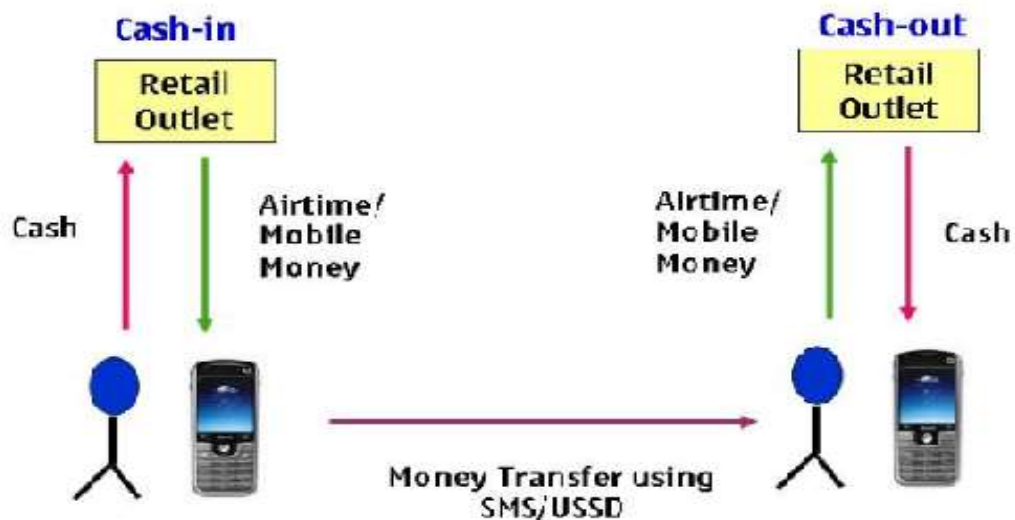
Source: Researcher 2013

2.3.1 Transfer Methods of Mobile Money

As illustrated in the figure 2.5 below, customer can send E-Money via STK or USSD method. STK is more efficiency that USSID, it enable customer to confirm transactions for the recipients number or name or both for long time without expired or time out , this is different from USSD mobile menu. Also to avoid sending money to wrong recipient or getting notification SMS is good to use STK especially for those who use smart phone like that android system.

From a security perspective, if data sent via either USSD or SMS are not encrypted, a transaction is vulnerable to interception. Given that USSD is session based and the server helps to manage the steps, once a USSD session terminates, no data is left on the phone. Conversely, with STK, the SIM helps to manage the steps and creates an SMS sent to the server. SMS is transaction-based and SMS data are stored on the phone, creating vulnerability if the SMS is not deleted and the phone ends up in the wrong hands. All systems rely on the use of a Personal Identification Number (PIN) for transaction authentication (http://www.orange-tkl.co.ke/index.php?option=com_content&view=article&id=224)

Figure 2.4: Transfer Methods of Mobile Money



Source: Mohit, 2009

2.3.2 Operating systems of Mobile Money

Mobile banking, or m-banking currently use USSD platform .Specialized m-banking service providers can cater for anything from balance enquiries to portfolio management and even live stock trading. Essentially, this allows consumers to monitor and manage transactions from anywhere. Great for businesses processes, consumers can also receive real-time SMS alerts via their mobile devices, keeping them informed of any anticipated or even fraudulent transactions as they happen. Platforms can be developed using any number of GSM functions to deliver m-banking to the community. USSD m-banking platforms, for instance, can allow basic phone users to manage their finances without the need for Internet access or multimedia capabilities. One third of the population of South Africa does not have a bank account, but 19% of these people have a pre-paid mobile account. A further 11% have access to the Internet via the phones of friends and family, leading to a high adoption late of Mobile money (<http://www.quirk.biz/resources/mobile101/296/The-Mobile-Wallet>).

2.3.3 Customer Care and Customer awareness

Both mobile money operators and banks run, or outsource, call centres that cater to their existing customers. In principle, then, either is well-positioned to set up this function for a mobile money service—particularly since both banks and operators have found that they train a sub-set of their call-centre staff to deal with mobile money inquiries in order to effectively resolve problems for customers such as suspend customers account once SIM card is lost/stolen, reset Mobile money PIN once customer forget his/her password. Similarly, banks and most operators have experience running walk-in customer care points (branches in the case of banks), and flagship stores or customer care centres in the case of mobile network operators (A, Prasad, 2003).

2.3.4 Fake money circulation in Mobile money transfer

Figure 2.3 above show clearly that fake money can come from either customers or E-Agents or both E-Agent, this implies that customer can request float and give fake money to Agent, also Agent can give fake money to customer during of E-money withdraw or exchange. The security of E-money depend on the customer and Agent awareness during interaction (Rajiv Kumar, 2008).

2.3.5 The Mobile Money Transfer Environment and Its Stakeholders

The following table 2.4 shows that the mobile ecosystem embraces a variety of participants, whose collaboration is necessary for the success of the mobile money network, including the mobile network operators (MNO) financial institutions, airtime agents, telecom retailers, and regulators (Jenkins, 2008). The mobile money environment and its stakeholders help to understand where the fraud were happened and how security was hindered with the mobile money cycle

Table 2.5: The Mobile Money Transfer Environment and Its Stakeholders

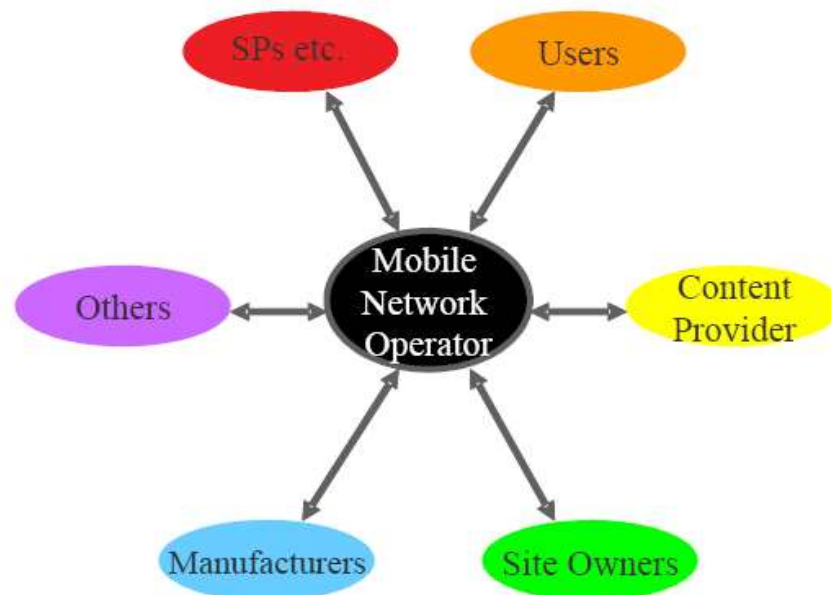
Key players in the mobile money ecosystem Players	Roles	Limitations and Constraints
Mobile network operators	• Provide infrastructure and communications service • Provide agent oversight and quality control • Issue e-money (where permitted by law) • Exercise leadership in drawing mobile money ecosystem together • Advise other businesses (banks, utilities, etc.) on their mobile money strategies	• Regulatory limitations on providing financial services • Shareholder pressure for faster, higher returns • Strategic focus that may not include mobile money
Financial institutions	• Offer banking services via mobile • Hold float or accounts in customers' names • Handle cross-border transactions, manage foreign exchange risk • Ensure compliance with financial sector regulation	• Narrow customer base • Lack of experience with or interest in low-income customers • Stringent regulatory requirements with significant compliance burdens
Agents	• Perform cash-in and cash-out functions • Handle account opening procedures, including customer due diligence • Report suspicious transactions in accordance with AML/CFT requirements • Identify potential new mobile money applications	• Liquidity shortfalls • Basic business skill gaps • Lack of customer trust (in some cases) • Limited ability to partner with large corporations
Regulators	• Provide enabling environment for mobile money • Protect stability of financial system • Demonstrate leadership to encourage and protect behavior change	• Lack of experience with convergence of financial and telecommunications regulatory schemes • Lack of financial and technical capacity
Consumers	• Use mobile money to improve their lives	• Lack of awareness • Limited financial literacy • Cultural and psychological resistance.

Source: Jenkins 2008

2.3.5.1 Mobile Network Operators

The Mobile Money Network (MMN) links the different parts of the chain value (see figure: 2.4). Thus Mobile Network Operator (MNO) have responsibility to take care of party specific (Security) concern while balancing this suitable security solutions to protect MNO infrastructure's and its customers, this is going perpendicular with the vision of adding simplicity to the way people shop by putting the mobile at the heart of the shopping experience (A, Prasad, 2003).

Figure 2.4: Security Roles of Mobile Network Operator



Source: A, Prasad 2003

2.3.5.2 Financial Institutions

In the past several years, both banks and mobile network operators have moved aggressively to offer mobile financial services to the unbanked. For banks, mobile money for the unbanked is a way to serve a vast swathe of customers who would otherwise be out of the reach of costly branch infrastructure; for operators, mobile money represents an opportunity to differentiate themselves from their rivals. To offer mobile money in security, banks and operators need to work together—yet negotiating agreements to do so can be contentious and time-consuming(N, Davidson 2012).

2.3.5.3 Responsibility of Mobile Money Agents

Signing up Mobile Payment agents is the most challenging aspect of the mobile money ecosystem. Technology and applications for mobile financial services are available off shelf all around the world at competitive pricing but agency network which is the Heart of the ecosystem is not available off shelf and it is the most tasking to manage. Providers will require to prospect, train and deploy agents across the length and Breadth of country. Availability and access to a well connected agent network will determine the success of Mobile financial services. In Kenya, MPESA's leadership is under fire from other providers that are clamoring for access into the continent's most extensive Agent network with 22,000 agents in Kenya alone. In MNO driven Mobile financial regime, accessing and getting the right agents is an icing on the cake.

The advantages Mobile Money agents bring to the Table, is the existing customer base which can drive mobile payment transactional services but limited understanding and access to the unbanked using the agency model. The non Bank providers will rely on the goodwill of Commercial Banks and MNOs to reach the critical mass, limited understanding of managing third party outlets and financial services are major hindrances to Go-to-Market (E, Okoegwale 2012).

(i) Airtime Dealers.

Airtime dealers are most suitable to use their existing outlets as Mobile Money agency in Nigeria as they are already active in the low value and high volume business which airtime dealership is. However, Airtime dealers are interested in the agency profitability earlier than independent outlets.

They compare earnings from Airtime sales against Mobile Money for profitability which is clearly below what they earn on their existing airtime business even though they understand the low margin Business, cash handling, security and risk management which are additional burdens of providing mobile payment services alongside airtime.

(ii) Agent Quality

Agent quality is a direct function of the community that produced the agent. There is growing evidence to support the argument that Agents sign on process are not universal and each community presents own unique challenges and opportunities especially in security. Rural Based Agents are concerned about logical security (Fraud), cost of re-balancing and travel cost to nearest Bank Branch while Urban Agents are concerned about physical security (Theft & Robbery) and agency sustainability.

(iii) Training and Support

Potential agents are willing to commit to any provider that can educate them not only on the technology but on the regulatory, trends, risk , cash management and operations .Understanding the process is a huge influence for agents sign up. Agents are attracted to providers that they can understand and address their security and sustainability concerns (<http://mobilemoneyafrica.com/?p=3068>)

2.3.5.4 Regulator's role in securing mobile money

Mobile money does require greater surveillance against fraud and money laundering measures, but it's all fundamentally about secure messaging. From a telecoms regulation point of view, mobile money is another instance of a value added service and those tend to receive a light regulatory treatment. All the specific regulations that pertain to the safety and soundness of mobile money who can issue accounts, conditions of service, data security, privacy standards, and supervisory treatment and consumer protections should be the domain of the banking regulator. In Tanzania, MNO are regulated by BOT and TCRA policies.

There is a risk that MNOs transfer market power from their core market to the emerging retail mobile payments market, in such a way as to effectively shut banks out of mobile payments. In the future, most financial services can be expected to have a mobile component, so such a situation would have severe implications for competition in the financial inclusion space more broadly (CGAP Report, 2012).

2.4 Research Gap

This study investigated the security level of mobile money transfer in telecommunication industry in Tanzania. Several studies exist on mobile money transfer services like *Developing Mobile Money* by Beth Jenkins and *Quarterly Update, GSMA Mobile Money for the Unbanked* by Leishman Paul that explained the mobile money transfer services. However, the existing studies did not focus on security of mobile money transfer at the household level that examine the household effects to make conclusions about security of Mobile Money transfer. This study intended to fill that gap, since it is important for electronic money transfer to have a secure means of transfer.

This study examined the transfer methods used by telecommunications companies in transferring money in Tanzania in order to know if they are efficient or not to secure money in mobile money transfer, also examined customers awareness in Mobile money transfer, this helped to understand on mobile customers how familiar they are with the service and if they follow all safety measure to secure E-money. Lastly identified the level at which money operating systems from telecommunication companies are secured and why has been classified as measures to increase security of mobile money transfer in telecommunication industry in Tanzania.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Area of the study

The study were conducted at Dar es Salaam city which is located at 6° 48` South and 39° 17` East. It's is a commercial city where by virtue of its big population and commercial potentials, it is also a region in the Tanzania with many Mobile subscribers especially in Mobile Money transfer. All Mobile Money telecommunications companies that were selected are operating in Tanzania and their headquarters being in Dar es Salaam that is Vodacom, Tigo, Airtel and Zantel as explained in the research design.

3.1 Research Design

A research design is a master plan of the research study to be undertaken, giving a general statement of the methods to be used. The function of a research design is to ensure that requisite data in accordance with the problem at hand is collected accurately and economically. Simply stated, it is the framework, a blueprint for the research study which guides the collection and analysis of data. The research design, its function is to provide the collection of the relevance evidence with minimum expenditure of efforts, time and money (Kothari, 1999:17). Research design is also an overall plan or programme for doing research (Chamwali, 2006). Frank and Nachimias (1996) define research design as arrangement of conditions for data collection and data analysis in a manner that aim to combine relevance to the research purpose as well with economy in procedure.

The research design used was survey design in Telecommunications Industry dealing with Mobile Money transfer in Tanzania. The aim of selecting this design was due to the fact that;

- (i.) It is flexible in data collection
- (ii.) It generalizes the uses of mobile money transfer
- (iii.) It can be achieved with minimal resources that is time and money

- (iv.) It facilitates the deep investigation on the finding
- (v.) I am also the employee of the VTL that deal with Mobile Money known as M-Pesa.

3.2 Population of the Study

It is the population where data was obtained. Sarantakos (1991) describes population as units in which the investigation is required. It is for the benefit of the population or subscribers that researches are done. However, due to the large sizes of populations, researchers often cannot test every individual in the population because it is too expensive and time-consuming, this is the reason why researcher was relied on sampling techniques. For this research, units of the study focused on:

- (i.) Mobile phones subscribers
- (ii.) Mobile Money customers.
- (iii.) Mobile Money Agents
- (iv.) Banks offering Mobile Money services
- (v.) Companies that use Mobile Money as biller points.
- (vi.) Staffs of the Telecommunications companies

3.3 Sample size and sampling technique

The sample was randomly selected from the groups mentioned in sub section 3.2 above. Judgmental, Convenient and Cluster sampling techniques with reasonable sample out of the population were used.

The sample size of this study was 50 respondents per each Mobile Money operator as calculated here under. The Sample size determination formula;

$$n = \frac{N}{1 + N(e)^2}$$

Where;

n= Sample size,

N= Population of the study,

e= Standard error (5-10%)

In regards to this research, “n” will be obtained by, N=400, e= 10%

$$n = \frac{400}{(1 + 400(0.10)^2)}$$

$$= \frac{400}{(1 + 400(0.01))}$$

$$= 400/8.02$$

$$= 49.87531$$

$$\approx 50$$

Therefore Sample size is approximated to 50 per each Telecommunications companies total being 200 respondents.

The randomly selected sample was used for quantitative analysis in which case, questionnaires were administered to them, while purposive sample means qualitative analysis in which the structured interviewed was carried to as shown in Table 3.1 below for the distribution of respondents.

Table 3.1: Distributions of Respondents per each Telecommunications companies

Level	Number	Percentage (%)
Mobile phones subscribers	10	20
Mobile Money customers	15	30
Mobile Money Agents	5	10
Banks offering Mobile Money services	5	10
Companies that use Mobile Money as biller points	5	10
Staffs of the Telecommunications companies	10	20
TOTAL	50	100

Source: Researcher 2013

3.3.1 Convenient Sampling

It is sampling technique where subjects are selected because of their convenient accessibility and proximity to the researcher. In the case study, the area proved to be effective as most of the intended accessible population had similar characteristics and close proximity with the researcher working area. This type of sampling techniques was used in order to get quick answer from respondents; the researcher will pick respondents who will be available to respond. 10 Mobile phones subscribers , 15 Mobile Money customers, 5 Mobile Money Agents mobile phones users, 5 Companies that use Mobile Money as biller points and 10 Staffs of the Telecommunications companies from 4 different Telecommunications companies operating Mobile Money Transfer will be interviewed.

3.3.3 Cluster Sampling

Cluster sampling procedure was used because it cuts research costs and time. Interviewing small geographical area like Mlimani city Dar es Salaam where three Telecommunications companies operating Mobile Money Transfer have their shops is more convenient and less costly; also it is economically more efficient in terms of time.

3.4 Data Collection Methods and Instruments

Various methods were used in the data collection depending on the levels, aim of the research and availability of type of data, the methods such as interviews, questionnaires, and observation can be used. This study employed two different sources for data collection such as secondary and primary sources. Secondary data was obtained through various ways including library as scholarly papers, publications, the relevant documents and Internet documents while primary data was collected from the field through questionnaires and interviews. These sources are employed because of the fact that they are complimentary to each other (Kothari, 1999).

3.4.1 Data Collection Methods

Data were collected by undertaking survey from sample obtained as per 3.4 above by using primary and secondary data collection method. These instruments enabled to obtain data from various units of enquiry.

3.4.2 Primary Data

Primary data are those forms of data which the researcher directly will collect data have not been previously collected or does not exist. In the study it was collected by the use of the interviews, questionnaires and observation.

(i.) Interviews: These aimed at gathering deep knowledge on the respondents' view on the studied phenomena. An – open ended question method will be used as it provided the opportunity for the research to uncover new clues, to open – up new dimensions of a problem and to secure vivid description and memories as well as eliciting accurate and inclusive accounts based on the informants personal

experiences, other advantage of interview method are very good technique for getting the information about the complex, emotionally laden subject can be easily adapted to the ability of the person being interviewed, it yields a good percentage of returns, also data collected by this method is likely to be more correct compared to the other methods that are used for the data collection. Interviewing is the only suitable method for gathering information illiterate or less educated respondents. Through direct personal and telephone interviews helped a researcher depth and detailed information that is secured. These will mostly focusing with open ended questions, inquiring about the facts but allowing respondents an opportunity to give out their opinions and insights about issues. The questions will be the same from one interviewee to another, though the questions in the study design which I will use to provide focus to the question to be asked.

(ii.) Questionnaires: The questionnaire will made up of open – ended and closed questions. The study developed questionnaire that reflected study objectives. White (2002) defines questionnaire as a series of questions, each one providing a number of alternative answers from which respondent delivered. The method is said to be not expensive, free from the bias of the interviewer, and respondents had adequate time to provide their answers (Kothari 1990:100). Questionnaire was used and distributed to mobile phones subscribers, mobile money customers, mobile money Agents, banks that offering Mobile Money services, companies that use Mobile Money as biller points and staffs of the telecommunications companies from 4 different Telecommunications companies operating Mobile Money transfer as shown in Table 3.1. Questionnaires were only given to those who have no ample time for interview. The research questions were enabled I to select the relevant strategy to conduct the research.

(iii.) Observation: The observation method involves human or mechanical observation of what people/ respondents actually do or what events take place. This observation Method has the following advantage;

- a) If the researcher observes and record events, it is not necessary to rely on the willingness and ability of respondents to report accurately.

- b) The biasing effect of interviewers is either eliminated or reduced. Data collected by observation are, thus, more objective and generally more accurate (Kothari 1990). This method was used by observe how Mobile money agents give cash to customers once they came to withdraw at their Agent Till, few Agents were not record transactions from customers as it is supposed to be.

3.5.3 Secondary Data

Secondary data means the data that are already available, the data which have already been collected and analyzed by someone else (Kothari, 2004). They are not original because they have already been processed by others. These may either be published or unpublished materials. One of the major sources of secondary data is documentary review; this method entails the use of various relevant documents. In this study documents like various reports patterning to this study were consulted. Apart from relevant reports, other documents like files, publications, journals, magazines and other office records were reviewed. Documents like policy and strategy were also be used as a secondary data. More details about system originality and its functionality was reviewed so as to know the current status of the system implementation

Documentary Review: In order to support the interview data and enhance the reliability of the conclusion, the documentation method was used to enable me to come up with appropriate information. I spent some times revising and review relevant documents concerning the study through Library study, review of various publications like BOT regulations, IT systems, policies and reports.

3.6 Data analysis

In this research the quantitative data that was collected was analyzed by using readily technology available to research, MS- Excel, where necessary, specialized software, Statistical Package for Social Scientists (SPSS). For categorical variables, simple frequency analysis and cross tabulations will be deployed. On the other hand, for continuous variables descriptive analysis involving computation of mean, medium

and mode will be used. The presentation of findings were in form of tables, figures, text descriptions, diagrams, Bar chart, Histograms and Pie charts for easier interpretation and understanding after using regression analysis and chi squares as Statistical analytical model.

Collected data summarized, classified, presented and analyzed using readily technology available to research, MS- Excel, where necessary, specialized software, Statistical Package for Social Scientists (SPSS) were used. The rationale behind using this package rests in its extensive analytical capacity and easiest in administering data. This requires both quantitative and qualitative data. In explaining some research findings, descriptive statistics was employed as explained early. The results obtained from data analysis were presented in tables and figure.

In the data that was collected, the first stage was data editing. This procedure is done purposely to detect errors so as to omit and correct those errors. The completed questionnaire was carefully scrutinized so as to be assured with the accurate, consistent, uniformly and completed so as to be ready for arranged coding and tabulation.

After editing process be completed the following process was coding. According to Kothari (2008), Coding refers to a process of assigning numerals or other symbols to answers so as responses can be put into a limited numbers of categories or classes. Coding allows efficient analysis and through it several replies may be reduced to small numbers which contain the critical information required for analysis

Classification of data was follow after data being coded, this is because data collected are the raw one so they have to be reduced into homogeneous groups so as to bring meaning relationships. Data of the same or common characteristics was arranged into groups or classes. Classification of data was focus on the same attribute or class interval.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

4.0 Introduction

Following are due to presentation and discussion of the research methodology and literature review in the previous chapters hereunder is the presentation of research findings and discussion. Security of mobile money transfer is crucial for both users and non-users of the services including mobile operators and government. These effects are direct or indirect; positive or negative impact on a party not involved in a specified economic/social transaction i.e. the effects that accrue to non-users of mobile money services due to others' use of the service.

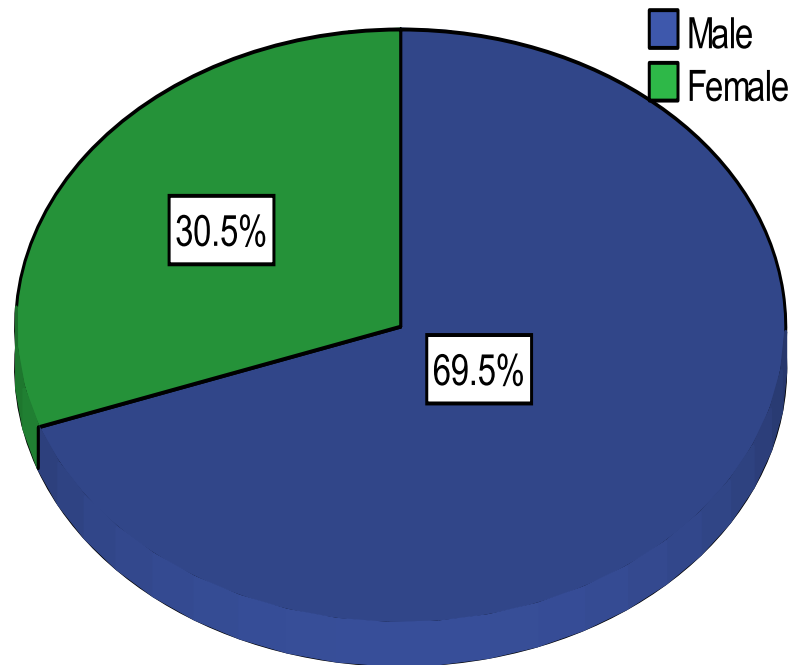
4.1 Characteristics of Respondents

This study concentrated on mobile phones subscribers, mobile money customers, mobile money Agents, Banks offering mobile money services, companies that use Mobile Money as biller points and Staffs of the Telecommunications companies. Respondents were characterized by gender, age, residential districts and education level. All these have great implication in the security of mobile money transfer.

4.1.1 Respondents by Sex

Gender of respondents was considered as social phenomena could be perceived differently by people in different sex groups. The anticipation was that in each sex group, mobile phones users had common interests with either major or minor differences with another sex group or they were having similar interests. Furthermore respondents' sex determines type of data given as sex influence perceptions, feelings and preferences. With regards to sex there were 139(69.5%) male and 61(30.5%) female as tabulated in the Figure 4.1 below depicts respondent's sex.

Figure 4.1: Depicts Respondent's Sex.



Source: Researcher 2013

4.1.2 Respondents by Age

The age of respondents was also considered as social phenomena could be alleged differently by people in different age groups. Respondents' age determined the group which are users and those who are non users of the electronic money transfers. The expectation was that in each age group, mobile phones users had common interests with either major or minor differences with another age group or they were having similar interests. Table 4.1 below depict respondents' age group as was tabulated; age below 30 years had 66(33%), age ranging from 31-40 years had 106(53%), age ranging from 41-50 years had 24(12%) and age ranging from 51-60 had 4(2%).

Table 4.1: Respondents by Age

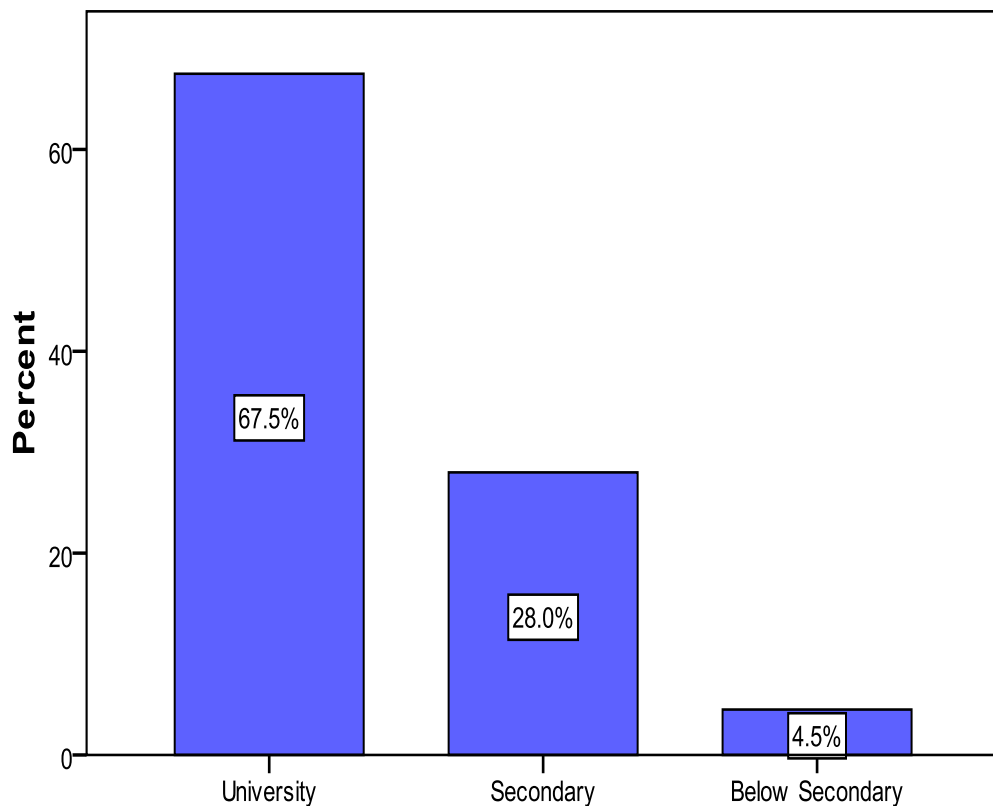
	Frequency	Percent	Valid Percent	Cumulative Percent
< 30 Years	66	33.0	33.0	33.0
31 - 40 Years	106	53.0	53.0	86.0
41 - 50 Years	24	12.0	12.0	98.0
51 - 60 Years	4	2.0	2.0	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.1.3 Respondents by Education Level

Education level of respondents was also considered as social phenomena could differentiate perceptions of issues by people in different education level, this means the education level of mobile money stakeholders could bring the great influence on the security of mobile money transfer. Respondents' level of education was taken into consideration due to the following arguments. First respondents' level of education could determine his or her clear or unclear understanding of studied phenomena. Second respondents' level of education could determine their ability to link studied phenomena with ever changing world perspectives on the social phenomena and third respondents' level of education determined ability to analyze question posed to them as working position goes together with level of education. Respondents' working position was as shown in Figure 4.2 below.

Figure 4.2: Respondents Education Level



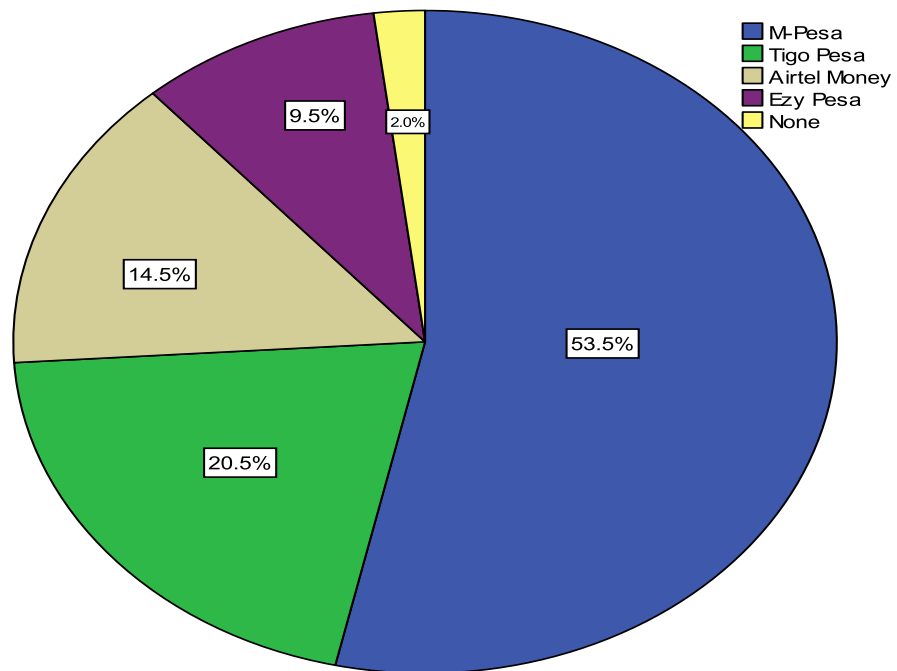
Source: Researcher 2013

With regards to the level of education, the result showed that about 135(67.5%) were at university education level, 56(28%) were at secondary education level and 9(4.5%) were below secondary education level.

4.1.4 Respondent's Registration to different Mobile money services

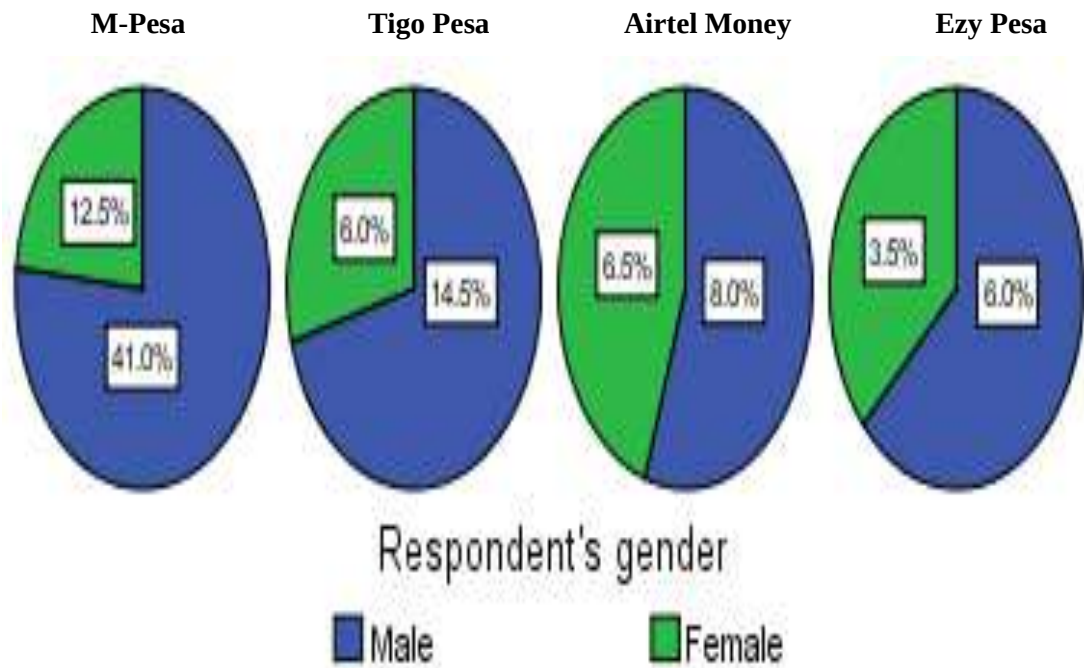
With regarding to the number of registered customers to the different mobile money operators, 107(53.5%) registered with M-pesa, 41(20.5) registered with Tigo pesa, 29(14.5%) registered with Airtel money, 19(9.5%) registered with Ezy pesa and 4(2%) were not registered by any Mobile money service as stipulated in the Figure 4.3. and 4.4. below

Figure 4.3: General Service Preference (for all respondents)



Source: Researcher 2013

Figure 4.4: General Service Preference by Gender



Source: Researcher 2013

4.1.5 Understanding of Mobile Money Services

Many mobile money services understand what mobile money, this is good new since it can eliminate the number of fraud among users, as stipulated below, 196(98%) understand the meaning of mobile money and rest 4(2%) have heard about it. The higher awareness the lower attempt of fraud and vice versa.

Table 4.2: Understanding of Mobile Money Services

	Frequency	Percent
Yes, Very well	196	98.0
Have heard about it	4	2.0
No, not at all	0	0
Total	200	100.0

Source: Researcher 2013

4.2 Uses of Mobile Money in transferring E-money

It has been known that in Tanzania, almost all of the mobile money customers are using it in transferring money and not as bank, the Table 4.2 below indicate that 192(96%) are using in only transferring money from one destination to another and the rest 8(4%) has been registered but are not using at all.

Table 4.2: Use of Mobile Money in Transferring E-money

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	192	96.0	96.0	96.0
No	8	4.0	4.0	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.2.1 Familiarity of the Method Used in Transferring E-Money

There are various methods used to transfer money in Tanzania, Security of mobile money transfer also depend on the familiarity of the customers to the methods that are used in transferring E- money. The Table 4.3 below show that 159(79.5%) are aware of the methods and 42(20.5%) of the customers are not aware of the methods

they are using although they transfer money in their day to day life. This implies that customers can lose their money or stolen their money due to not being sure of what they want to do in the mobile money.

Table 4.3: Familiarity of the Method Used in Transferring E-Money

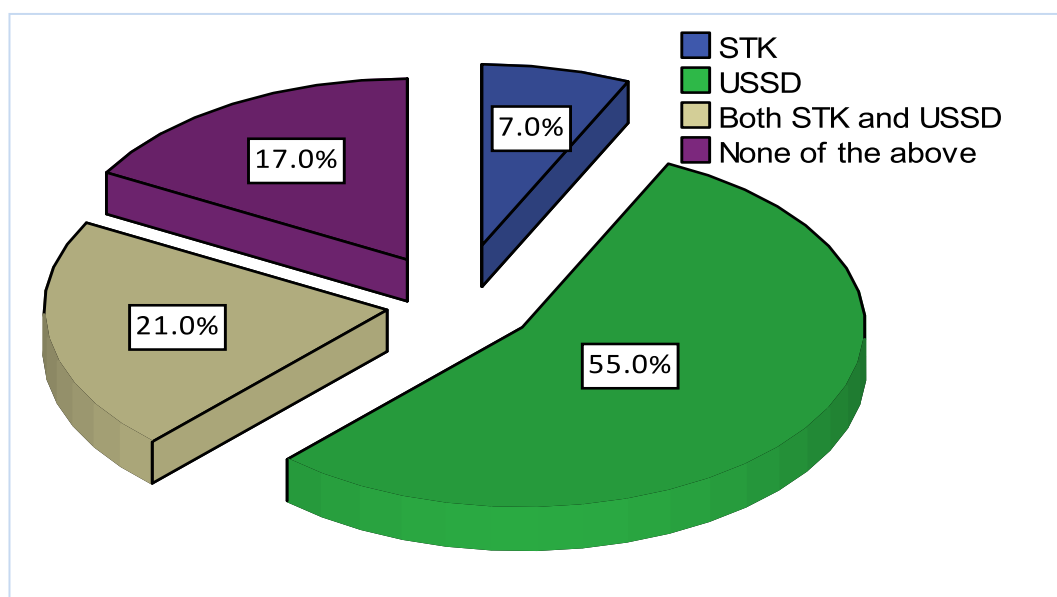
Familiarity	Frequency	Percent
Yes	159	79.5
No	41	20.5
Total	200	100.0

Source: Researcher 2013

4.2.2 Various Method Used in Transferring E-Money

Various methods are used in transferring money from one person to another, these methods are STK, USSD, and Both STK & USSD, with regarding to the number of registered customers to the different mobile money operators a different methods were used as stipulated below in Figure 4.5 namely 14(7%) are using STK, 110(55%) are using USSD and 42(21%) are using both method STK and USSD. The rest 34(17%) are not aware of the any method that are using.

Figure 4.5: Various Methods Used in Transferring E-money



Source: Researcher 2013

4.2.3 Use of Mobile Money to Transfer Money to Relatives & Friends

In Tanzania, such as in Dar es Salaam city still mobile money services are almost used in transferring money from one person to another especially from urban areas to rural areas rather than used as bank . As stipulated in the Table 4.5 below among two hundreds mobile money customers 193(96.5%) are using MMS to send or receive money from relative and friends and 7(3.5%) are using for other purposes such as paying utility bill i.e LUKU, DSTV and DAWASCO.

Table 4.5: Use of Mobile Money to Transfer Money to Relatives & Friends

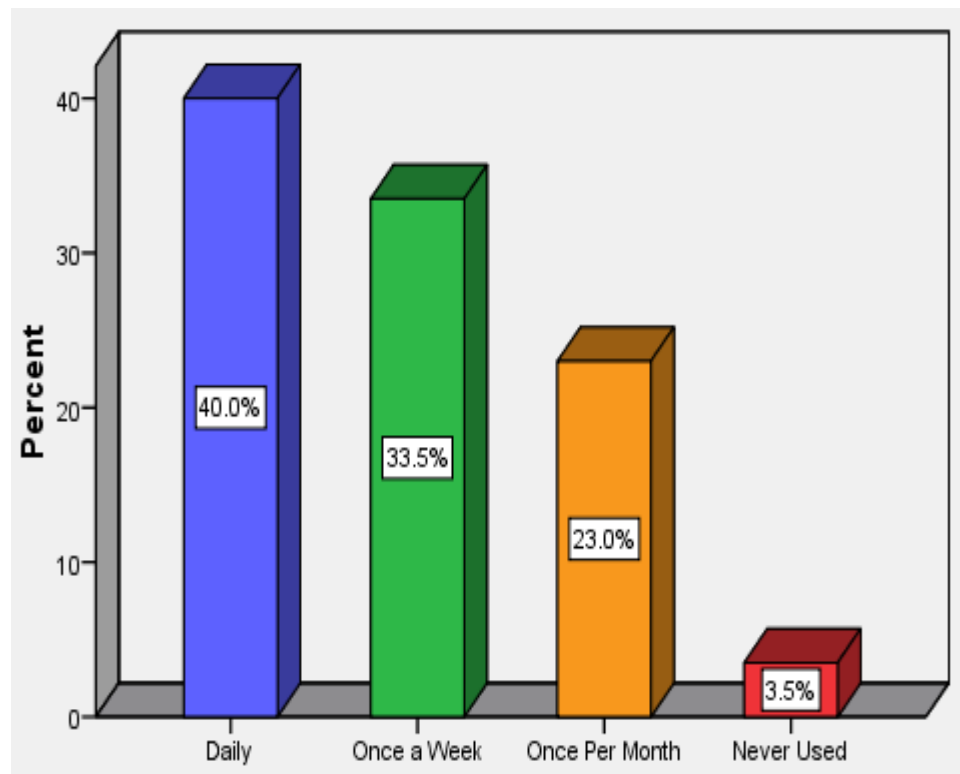
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	193	96.5	96.5	96.5
No	7	3.5	3.5	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.2.4 Frequency of Use of Mobile Money Service

Since mobile money service are almost used to transfer money from one person to another, most users are frequently in receiving or sending E-money, it has been observed that 80(40%) are almost using MMS more than once in a week, 67(33.5%) using once a week, 46(23%) are using mobile money once per month and 7(3.5%) never using in either receiving or sending money as stipulated in the Figure 4.6 below;

Figure 4.6: Frequency of Use of Mobile Money Service



Source: Researcher 2013

4.3 Whether or Not Mobile Money Transfer is Safe Means of Transferring Money

Security play important roles in mobile money transfer, customers are always ready to use services that are available at all times when need and this made them to fill as they are safe customers, stakeholders engaged in electronic money transfer services confirm that 181(90%) of the E-money transfer means is safe, 9(4.5%) confirm the service is not safe and 10 (5%) are not sure about the security of Mobile money as stipulated in the Table 4.6 below;

Table 4.6: Whether or Not Mobile Money Transfer is Safe in Transferring E-Money

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	181	90.5	90.5	90.5
No	9	4.5	4.5	95.0
Don't know	10	5.0	5.0	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.4 Experienced Mobile Money Security Problem in Transferring E-Money

Although 90.5 % believe mobile money transfer is safe but still other user's experience insecurity in transferring E-money. It show that about 41(20.5%) already encounter security problem, these is due to operating system problem whereby sometimes E-money are not delivered on time due to remain in authorized status or less amount is delivered to intended recipients, and last is due to transferring money to incorrect recipients which is caused by time limit in reading the confirmation SMS in attempting to transfer money or pay bill and 156(78%) did not face any security challenge in Mobile money, and 3(1.5%) are not sure if they face challenge in security either direct or indirect as stipulated in the Table 4.7 below, the insecure can be interim of E-money lost, password or individual E-money information hacked which can cause the theft of money. Furthermore experienced mobile money security problem will be explained I the next later in terms gender, age and education level.

Table 4.7: Experienced Mobile Money Security Problem in Transferring E-Money

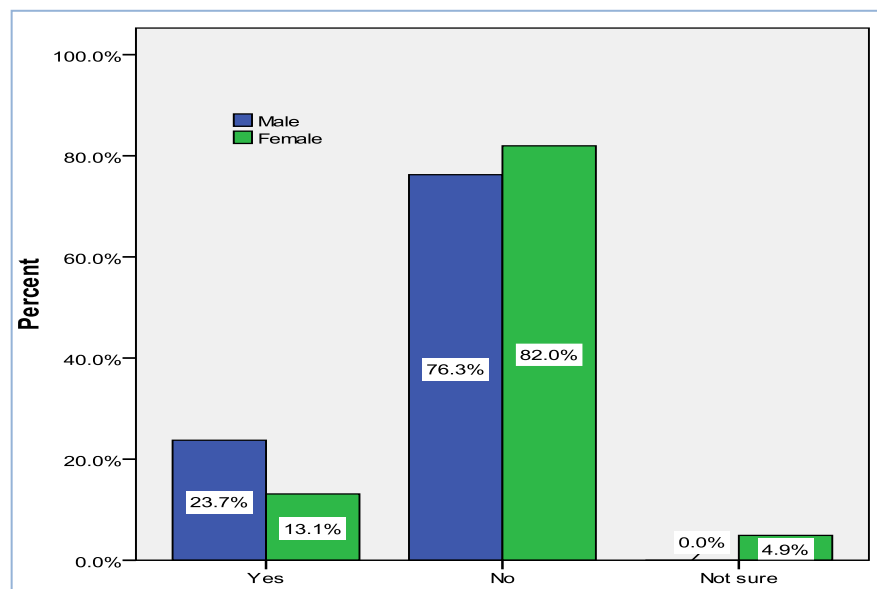
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	41	20.5	20.5	20.5
No	156	78.0	78.0	98.5
Not sure	3	1.5	1.5	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.4.1 Experienced Security Problems by Gender

Regarding security of mobile money transfer by gender, the number of male users affected in terms of lost their money is big compared to female subscribers, this is due to the fact that majority of mobile money users are male, about 23.7% of male were affected, and only 13.5% of male affected for the same issue and 4.9 % of female are not sure if they got any security problem in one way or another as stipulated in the Figure 4.7 below, this means there is bigger number of male users compared to female users, also male are the once who frequently transfer money to female.

Figure 4.7: Experienced Security Problems by Gender

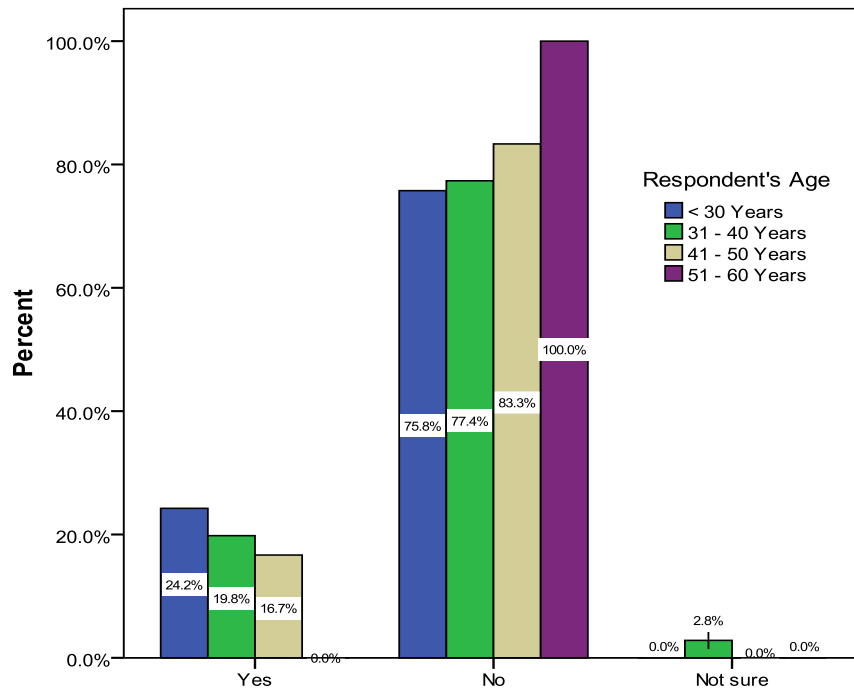


Source: Researcher 2013

4.4.2 Experienced Security Problems by Age Group

Regarding security of mobile money transfer by age group who experienced security issues for both male and female, about 24.2% were below 30 years of age, 19.6% were 19.6% were between 31 to 40 years of age, 16.7% were 41 to 50 years of age, and no one was affected with the age of 50 to 60 as stipulated in the Figure 4.8 below. This means those with age below 30 years were affected more, this can be due to negligence in using mobile money service.

Figure 4.8: Experienced Security Problems by Age Group

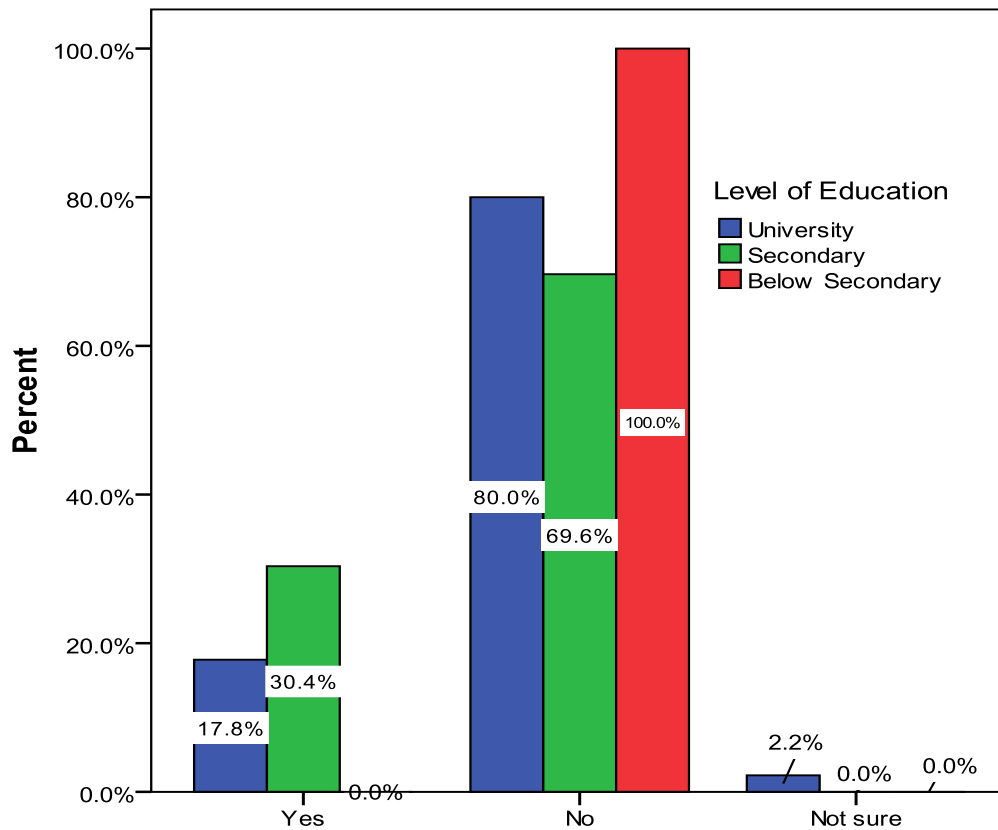


Source: Researcher 2013

4.4.3 Experienced Security Problems by Level of Education

Level of understanding or education level help in identifying the security level associated with any service, it has been observed that 17.8% of the mobile money users which has university knowledge were affected, this is almost half of the affected customers of mobile money services which has secondary education and were affected by 30.4% as stipulated in the Figure 4.9 below. This means the higher level of education, the lower the number of in security risk in mobile money transfer service.

Figure 4.9: Experienced Security Problems by Level of Education



Source: Researcher 2013

4.5 Mobile Money PIN Sharing

E-money in mobile money services can be transferred from one customer account to another by confirming the correct mobile PIN in handset, once mobile money password/PIN is used by more than one person it can allow other person who is not the owner of the account to transfer or withdraw money without awareness or willingness of the owner, the result show that 26(13%) share or expose their password with other person who are not owner of the account, 174(87%) as stipulated in the Table 4.8 below are not sharing their PIN with other person which is safe in transferring mobile money. Mobile money PIN sharing create insecurity by bringing fraud

Table 4.8: PIN Sharing In Mobile Money

	Frequency	Percent	Valid Percent	Cumulative Percent
Share or expose pin/password	26	13.0	13.0	13.0
Do not share/expose pin/password	174	87.0	87.0	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.5.1 With Whom Mobile Money Password/PIN Is Shared

As stipulated in the Figure 4.9 above, 13% of mobile money users are sharing or expose their MM PIN or password, it has been noticed that 19(9.5%) share password with their spouses namely wife or husband and 8(4%) share mobile money PIN with their close friend while 173(86.5%) do not share password with anybody as stipulated in the Table 4.9 below. This implies that the total percent that sharing password is small compared of those who are not sharing password but has great impact in the security of E-money in which their money can be stolen smooth by their spouses of friend without their awareness.

Table 4.9: Relationship in Sharing Mobile Money PIN

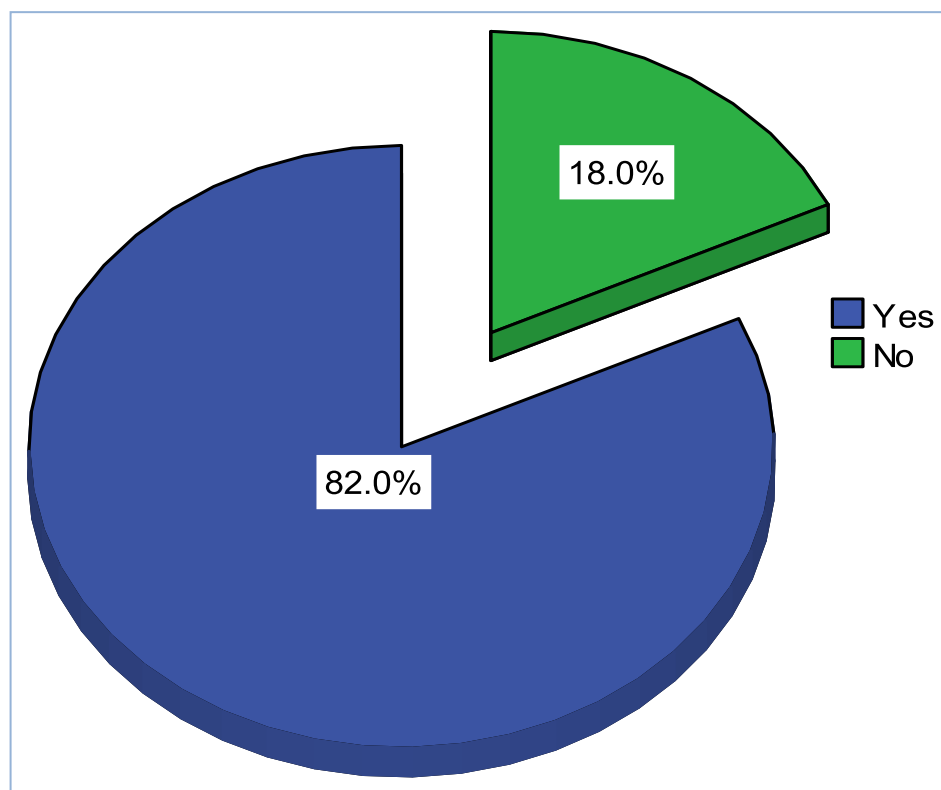
	Frequency	Percent	Valid Percent	Cumulative Percent
Wife/ Husband	19	9.5	9.5	9.5
Close Friend	8	4.0	4.0	13.5
None of the above	173	86.5	86.5	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.5.2 PIN Sharing is Hindering Security of Mobile Money

Many mobile money customers know that PIN sharing is restricted by mobile money operators in order to reduce if not to eliminate complains from their esteemed customers that their E-money has been stolen or theft due to PIN sharing, lucky 82% understand the PIN sharing is not safe to secure E-money and 18% they don't accept that can lost money due to exposing password as stipulate in the figure 4.10 below;

Figure 4.10: How PIN Sharing Hindering Security of Mobile Money

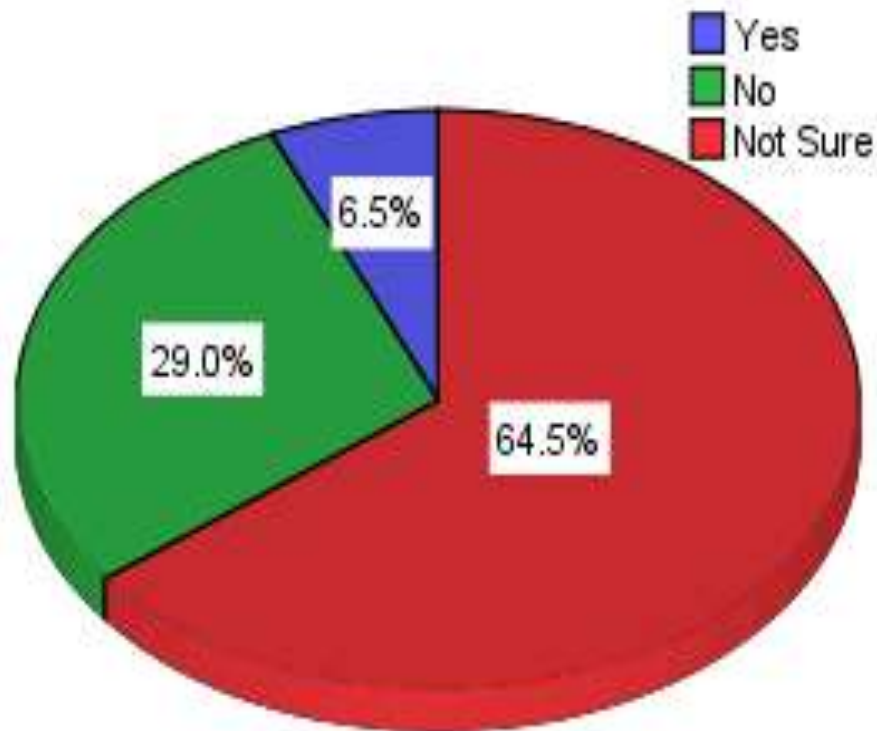


Source: Researcher 2013

4.5.3 Security risks in sharing or exposing MM PIN/Password with other person

Mobile money risk or fraud also associated with sharing mobile PIN, result show that 13(6.5%) still believe that there is no any risk in password sharing, 58(29%) believe there is risks in sharing password and 129(64.5%) are not sure if there is risk in sharing password as stipulated in the figure 4.11 below.

Figure 4.11: Security Risk in Mobile Money PIN Sharing

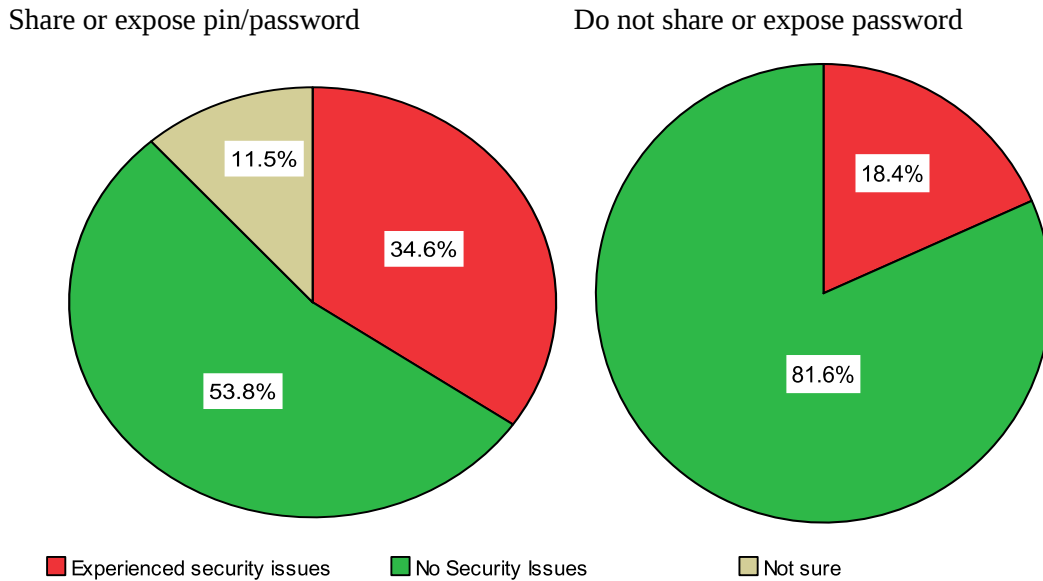


Source: Researcher 2013

4.5.4 Relationship between PIN sharing and experiencing loss security problems

Many subscribers who share their password with other person also experience loss or theft of their E-money, about 34.6 % who share passwords were affected, about 11.5% are not sure if there were affected or not and about 53. 8% who share password were not affected, in other hand for those who didn't share password about 81.6% were not affected and only 18.4% were affected, this means the those who sharing password affected by 34.6% compared by those who were not sharing password who was only affected by 18.4% only as stipulated in the Figure 4.12 below, this means that password sharing is hindering the security of mobile money transfer.

Figure 4.12: Relationship between PIN Sharing and Security Problems



Source: Researcher 2013

4.5.5 E-money stolen/lost in unknown way since started to use Mobile Money transfer service

Since starting of Mobile money, some customers have complaint their E-money being stolen but they don't know how they stolen, this create a challenge to all mobile moneys stakeholders such as MM subscribers, MM operators, TCRA, BOT and government in which 6(3%) already affected, 174(87%) were not affected and 20(10%) are not sure if the E-money balance was decreased in their account or not as stipulated in the Table 4.10 below due to not remembering the actual balance they had before next transactions.

Table 4.10: E-money stolen in unknown way since started to use MMS

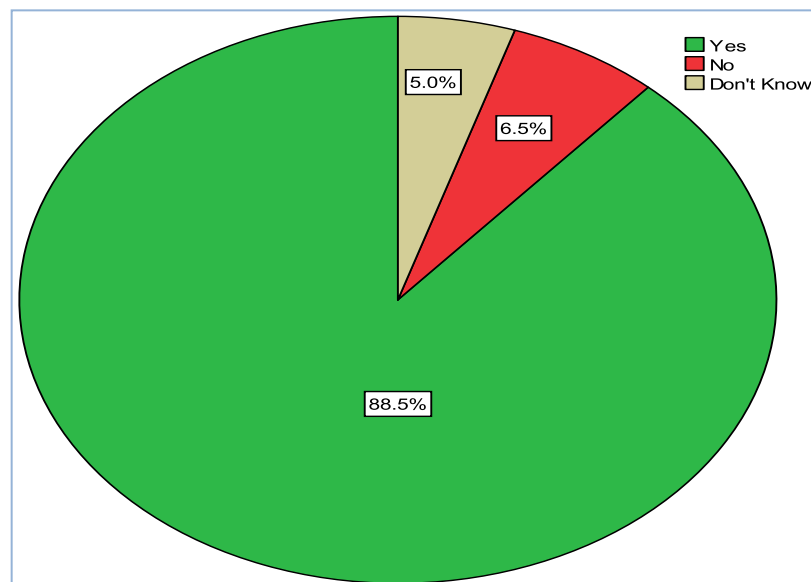
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	6	3.0	3.0	3.0
No	174	87.0	87.0	90.0
Not Sure	20	10.0	10.0	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.6 Understanding of Money Laundering in Mobile Money

Money laundering is also available in mobile money transfer service, the result show that 177(88.5%) know what money laundering is, 13(6.5%) do not know what this is all about and 10(5%) they don't know if they know what money laundering is not as stipulated in the Figure 4.13 below; This means customers can avoid circulation of fake and illegal money in mobile money service and increase and fostering the security in E-money in general.

Figure 4.13: Understanding of Money Laundering in Mobile Money

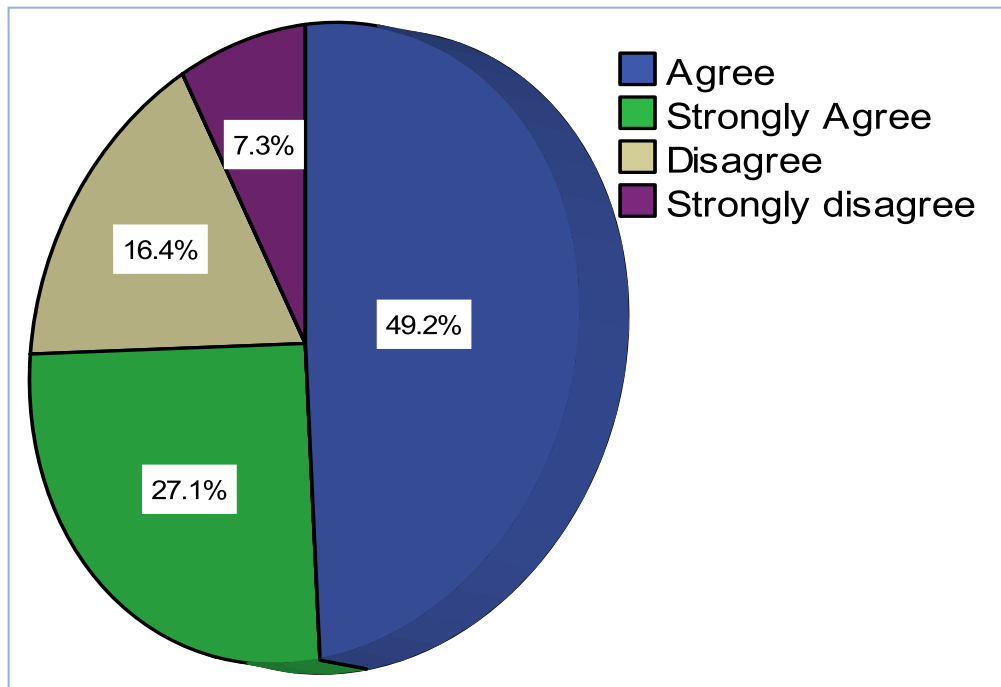


Source: Researcher 2013

4.7 Money Laundering Affect Mobile Money Service Security Wise

As discussed in 4.9.6 above, among 177(88.5%) who understand what money laundering is have confirm that money laundering affect mobile money in terms of security in which 49.2% have agree this sector is affected by mobile money and 27.1% have strongly agree that it is affected much in terms of security, also 16.4% who understand what money laundering is disagree that there is no any effect of money laundering to mobile money and the rest strongly agree that money laundering has nothing to do with security of mobile money transfer. This implies that security of mobile money is affected by money laundering as stipulated in the Figure 4.14 below;

Figure 4.14: Money Laundering Affect Mobile Money Service Security Wise

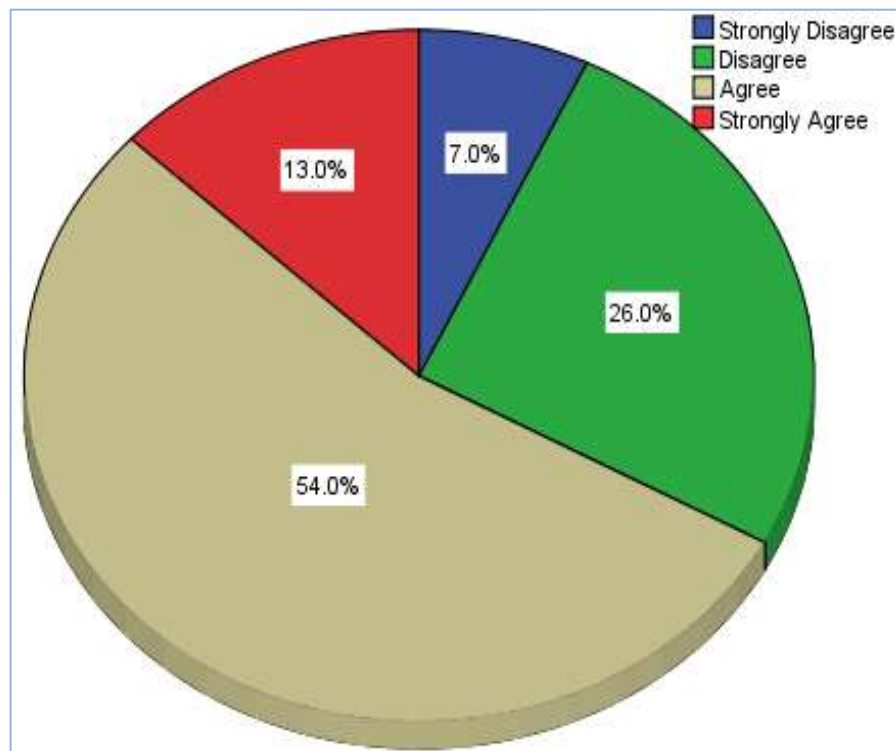


Source: Researcher 2013

4.8 Mobile Money Operating System

Mobile money operating system should be secured in order to allow customers' transactions to pass successful without stuck or remain in authorized status. In order customers to be satisfied that their E-money can reach the intended recipients on time and as expected without any error or delay and can create faithful to customers as stipulated in the Figure 4.9.7 below that 14(7%) strongly disagree that they don't know the mobile money operating system, 52(26%) also agree that they don't know MM operating system, 108(54%) agree they little know operating system on how their passing thru from one points to intended parts and 26(13%) they are happy that they know one to one steps of how E-money is transferred by operators once they initiate transaction, this include the time slot used to access MM menu and time E-money hit to another account.

Figure 4.15: Money Operating System

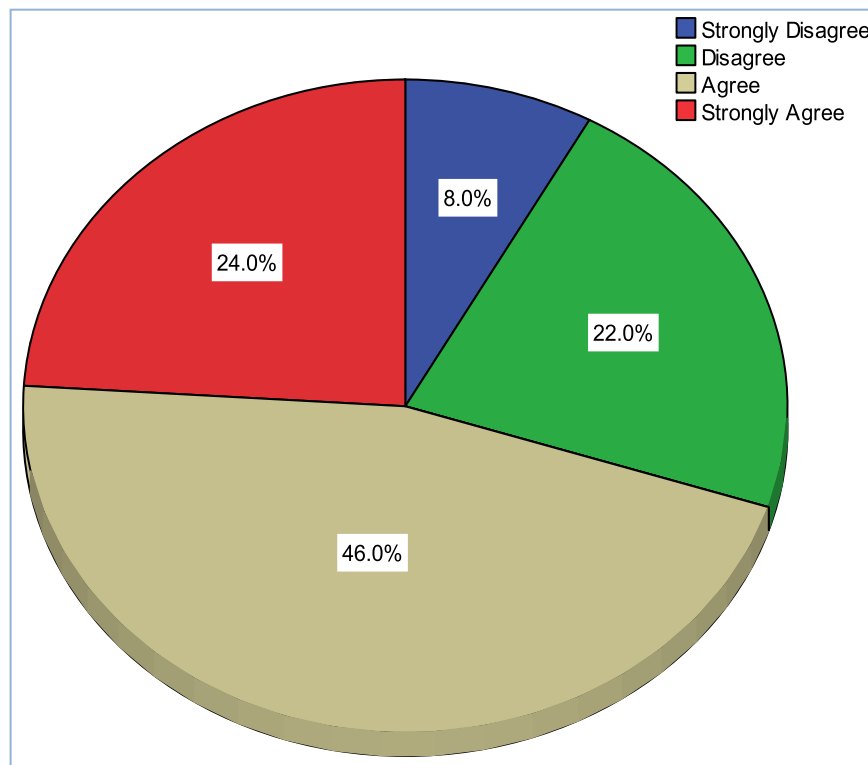


Source: Researcher 2013

4.8 Identification of Mobile Money Transfer Methods

There are two mainly methods of transferring E-money in Tanzania, these are USSD and STK, the famous method being USSD, to enhance security of mobile money customers should be aware of the methods that are used to transfer money, it has been observed that 16(8%) of the mobile money user strongly disagree to know the methods that are used to use the service although they use mobile money in transferring electronics money to their relatives of friends or pay bills such water, LUKU and various decoders in their day to day life also 44(22%) are not aware of the method although they use in every day to transfer money, while 92(46%) they also know the methods that are using, and 48(24%) they are very sure of the methods that are used. This means 70% they know what they are doing and 30% are not aware of these methods as stipulate in the Figure 4.16 below;

Figure 4.16: Identification of Mobile Money Transfer Methods



Source: Researcher 2013

4.9 Safety in Mobile Money Procedures

To transfer E-money from one person account to another, subscriber should follow proper procedure of the mobile money, these are to use the handset that that support this technology, to use mobile money Menu, and to allow transaction time at least two one minutes per transaction of the same amount, other procedure is to enter correct business code or recipient number and the amount you need to transfer of pay as bill. In order to transfer money without doubt or fear of losing money the procedure should be friendly to customer and which does not allow hacked the mobile PIN number, subscribers 153(76.5) agree the mobile money transfer procedure are safe, 46(23) confirm the procedure are very safe, meanwhile 1(0.5%) disagree procedure are not safe. This means almost all of the customers accept the procedures are safe to use as stipulated in the Table 4.11 below;

Table 4.11: Safety in Mobile Money Procedures

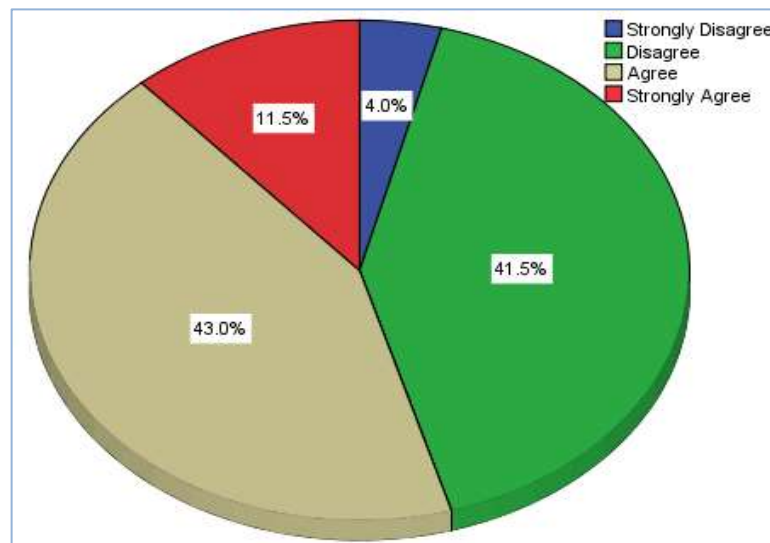
	Frequency	Percent	Valid Percent	Cumulative Percent
Agree	153	76.5	76.5	76.5
Strongly Agree	46	23.0	23.0	99.5
Disagree	1	.5	.5	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.9 Customer Awareness on Mobile Money Security Provided by MMO

Mobile Money operators has responsibility of providing customers awareness especially on the security, customers should be emphasized on the important of hiding the PIN and to transfer E-money careful to intended recipient in order to avoid fraud, as analyzed in the Figure 4.10 below 8(4%) strongly disagree and 83(41.5%) disagree that mobile money operators are not provide sufficient awareness regarding the security of mobile money or how customers should use their account in order to be is the safe side, in other hand 86(43%) strongly agreed and 23(11.5%) confirmed mobile money operators are doing their parts in educating customers on the issue of security as such as importance of hiding mobile PIN as stipulated in the Figure 4.17 below.

Figure 4.17: Customer Awareness on Mobile Money Security Provided by MMO



Source: Researcher 2013

4.9.1 Deposit Fake money to Mobile Agent

Fake money affect both Mobile money operator, mobile money subscribers, and mobile money agent, Agent s who have no money counter machine are experiencing this problem from customers once they came and request to deposit in order to get float in the mobile account. Table 4.12 below stipulated that 1(0.5%) deposited fake money to mobile money Agent intentionally, 195(97.5%) did not try to attempt to deposit any fake money to Agent and 4(2%) are not sure if they were deposited fake money or not. This implies that those who are not sure and those who are sure that did deposit fake money are about 99.5% and show that customers are not deposit fake money to Agent and complies there is security of mobile money in terms of fake money from customers to Mobile Agents.

Table 4.12: Deposit Fake Money to Mobile Agent

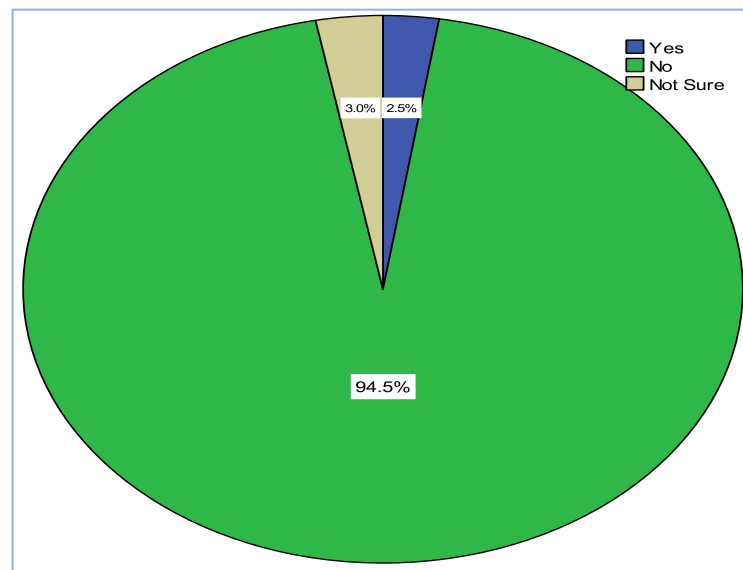
	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	1	.5	.5	.5
No	195	97.5	97.5	98.0
Not Sure	4	2.0	2.0	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.9.2 Withdrawn Fake Money from Mobile Agent

The same to Mobile money agents as explained in 4.12 above, many customers confirmed that they did not get any fake money problem, as stipulated in the Figure 4.18 below elaborate 5(2.5%) got fake from Mobile Agent, 189(94.5%) did not get experience such scenario from Agents and 6(3%) were not sure if they had fake money or not from Mobile money Agent, this implies that almost 98% believe the service is safe in terms of receiving fake money from Mobile money agent.

Figure 4.18: Withdrawn Fake Money from Mobile Agent



Source: Researcher 2013

4.9.3 Cause of Fraud in Mobile Money Transfer - company side

There are different scenarios that can cause fraud in Mobile Money transfer, among of these are Mobile Money Agents, transfer methods and Mobile Money operating system, as stipulated in the Figure 4.12.1 which indicate that 96(48%) mobile money stakeholders confirm mobile money Agents are the one who are involved in the fraud such as money laundering and Fake money as well as requesting the resetting of Mobile money PIN of the customers once they came to Agent to request the assistance.

Mobile money transfer methods such as STK and USSID are sometimes time-out during the transaction period and doesn't show if E-money was moved from account or not, this is especially for USSID method in which 39(19.5%) of the customers believe this is the cause of the fraud. Mobile money operating system such as MM Menu facilitate the fraud by 14(7%) and other 51(25.5%) of the frauds are caused by other scenarios such customers themselves as explained in the Table 4.13.

Table 4.13: Fraud Cause in Mobile Money Transfer - company side

	Frequency	Percent	Valid Percent	Cumulative Percent
Mobile Money Agents	96	48.0	48.0	48.0
Mobile Money transfer methods	39	19.5	19.5	67.5
Mobile Money operating system	14	7.0	7.0	74.5
None of the above	51	25.5	25.5	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.9.4 Causes of fraud in Mobile Money Transfer – customers side

Fraud are also caused by the following things such as Password/PIN sharing, Customer awareness, and Mobile Money customers, the result show that many subscribers believe that 48.5% of the fraud are caused by sharing of mobile account PIN, this means that mobile money account PIN is exposed to relative, friends or spouses in which any one can take the mobile money handset with enough mobile money and transfer to his/her account and then delete the notification SMS as if there is no any electronic money has been transferred without owner willingness , 45% are caused by lack of awareness on how to use mobile money in proper and effective way, 4.5% this is caused intentionally by customers so that to earn more as stipulated in the Table 4.14 below.

Table 4.14: Fraud causes in Mobile Money Transfer – customers side

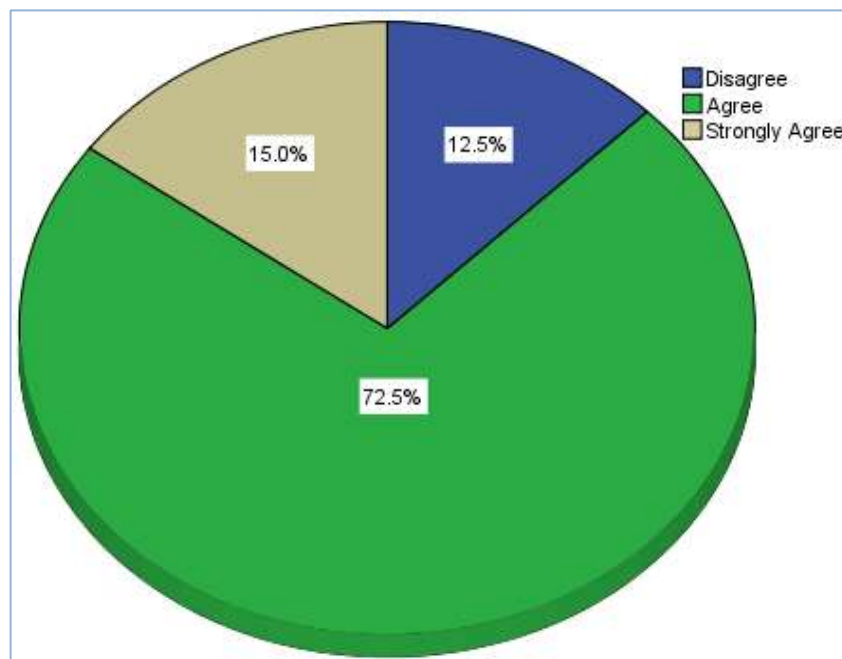
	Frequency	Percent	Valid Percent	Cumulative Percent
Password/PIN sharing	97	48.5	48.5	48.5
Customer awareness	90	45.0	45.0	93.5
Mobile Money customers	9	4.5	4.5	98.0
None of the above	4	2.0	2.0	100.0
Total	200	100.0	100.0	

Source: Researcher 2013

4.10 Security of Mobile Money is nowadays increased compared to previous years

Due to present fraud in Mobile money transfer, 25(12.5%) of the mobile money stakeholder see that the security of mobile money decrease compared to the previous years, this is due to these stakeholder being affected in one way or another, either by hacked their mobile PIN account or conflict with Mobile money Agent or their money stolen anonymous, also 145(72.5%) strongly agree mobile money transfer are now secured and the rest 30(15%) strongly agree MMT are nowadays more secured compared to previous years as stipulated in the Figure 4.19 below; this is due to effort taken by the network provider on increasing customers awareness and registration that has been emphasized by TCRA.

Figure 4.19: Security of Mobile Money is Nowadays Increased Compared to Previous Years



Source: Researcher 2013

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.0 Introduction

The findings were based on survey conducted in telecommunication industry in Tanzania. Objectives of the study were to investigate level of security of mobile money transfer. The main concern of this study was done to examine the transfer method used by telecommunications companies in transferring money in Tanzania in order to know if they were sufficient or not to secure E- money in mobile money transfer, also examined customers awareness in Mobile money transfer, this helped to understand mobile money customers how familiar they were with the service and if they followed all safety measures to secure E-money. Lastly identified the level at which money operating systems from telecommunication companies were secured as measures to increase security of mobile money transfer in telecommunication industry in Tanzania.

Findings were collected through interview and questionnaire. The recommendation and conclusion given below were based on the statement of the problem under chapter one, Literature review under chapter two and the practical aspects as described under chapter four.

5.1 Summary of the Discussion

This research worked out to investigate level of security of mobile money transfer in Tanzania by examined customers awareness in Mobile money transfer, examined the transfer method used and identified the level at which money operating systems from telecommunication companies were secured. It was well established and obvious that there are impacts of the electronic money transfer in security aspect in Tanzania.

Overall, Mobile money security is safe although it face small challenges such as mobile PIN sharing. The result show that 26(13%) share or expose their password with other person who are not owner of the account. Many subscribers who shared their password with other person also experienced loss or theft of their E-money, about 34.6 % who share passwords were affected, about 11.5% are not sure if there were affected or not, in other hand for those who didn't share password about 81.6% were not affected and only 18.4% were affected, this means the those who sharing password were affected by 34.6% compared by those who were not sharing password who was only affected by 18.4%, this means that password sharing is hindering the security of mobile money transfer.

Mobile money operating system should be secured in order to allow customers' transactions to pass successful without stuck or remain in authorized status. In order customers to be satisfied that their E- money can reach the intended recipients on time as expected without any error or delay and can create faithful to customers .The result show that 33% also agree that they don't know MM operating system, 67% they are happy that they know one to one steps of how E-money is transferred by operators once they initiate transaction, this include the time slot used to access MM menu and time E-money hit to another account.

There are two mainly methods of transferring E-money in Tanzania, these are USSD and STK, the famous method being USSD, to enhance security of mobile money customers should be aware of the methods that are used to transfer money, it has been observed that 30% are not aware of the method although they use in every day to transfer money. This means 70% they know what they are doing and 30% are not aware of these methods

Customers awareness especially on the security, result show that 45 disagree that mobile money operators are not provide sufficient awareness regarding the security of mobile money on how customers should use their account in order to be is the safe side, in other hand 55% confirmed mobile money operators are doing their parts in educating customers on security manner.

5.2 Conclusion

This study concludes that, despite of little awareness of electronics money transfer and methods used in transferring electronics money from one customer account to another, still mobile money transfer is safe to both customers and telecommunication companies that are providing mobile money transfer services.

Many mobile money customers are using USSD methods instead of STK being in mind that STK is the latest methods which is more secured than old method of USSD which is not very secured in transferring electronics money. This implies that transferring methods is hindering the security of mobile money to many customers although many customers are not affected.

5.3 Recommendations/ Policy Implication of the Research

This study reveals that the mobile money services is secured and plays great role which enhance the security from customer level to the mobile money operator level.

5.3.1 Mobile Money PIN Sharing

It has been found that still customers are sharing Mobile money PIN with other customers, this sharing create insecurity by bringing fraud in the customer's account whom their password are shared to by transferring E-money from one customer account to another customer account or withdraw the money in the ATM machines. Although the number of customers who are sharing their password is small but hindering a lot the security of mobile money, most customers who are sharing password is female and they share with their husband/spouse.

To sort the issues of mobile money PIN sharing, customers should be insisted by mobile money operators though fliers, radio and television advertising, street promotion and sent SMS to customers to insist on the importance of fostering security of their E-money account via hiding and not sharing mobile PIN especially to female customers.

5.3.2 Security of Mobile Money Agents

Mobile money services are almost used in transferring money from one customer to another especially from urban to rural areas, during each transaction that customer make there is an transaction fees that customer should pay, to avoid these fees customers are doing direct deposit to customers, this means the one who give cash money to Mobile agent is not the who intended to receive money rather that sending direct to his/her friend from Agent to customer account, this hindering the security of mobile money in which agent can deposit to incorrect account without know in time and electronic money can be withdrawn and give loss to Mobile Agent.

To avoid this kind of fraud, Mobile money agent should not allowed to deposit electronic money direct to customers who are not at present to mobile agent during transaction time, various initiative like suspending agent accounts should be done by mobile operators and sometimes go further by removing agents permanently from performing mobile money services like Vodacom and Tigo Tanzania do.

5.3.3 Security procedure during E-money withdraw

Many customers are neither sign in the mobile money log book nor show their identity when withdraw electronics money from mobile agents, this enhance fraud done by customers in which customers are reported to their service provider or operators that they have done withdrawing transaction and request for reversal and as it create fraud and insecurity in the mobile money transfer services.

Based on the BOT policy on the driving mobile money services, customer should not given cash money once withdrawn electronic money from mobile agent until he show identify card with his/her photo and should be willing to sign in the log book but still Mobile money agent allow such kind of fraud in order to get more transaction s and more commission/profit per months.

To avoid such kind of frauds form customer to mobile money agents, Agents should not give cash if customer is not willing to sign and show his ID otherwise mobile money agent should report immediately to its mobile money network operator regarding misunderstand between him/her and customer.

5.3.4 Confirmation during transferring E-money

Mobile money phone menu are allowing customers to confirm mobile money transaction in transferring E-money from one customer account to another, this including confirmation of customer name, number and amount that is intended to be transferred. Customer has an option either to confirm transaction or cancel after satisfying what is seen in the display menu of mobile menu but some customers are not ready to check the confirmation notification message and they transfer E-money ending in sending to wrong recipients and finally lost their money due to negligence.

It is true that mobile money menu take few minutes to time out but this should not be the reason of not reading the confirmation notification message and create insecurity in mobile money transfer services. To tackle this insecurity both customers and mobile operator should take ownership on fostering security of this sector by taking time of viewing displaying confirmation notification message before attempting to confirm and mobile money operators should increase mobile money menu on time to timeout or expiring in order to allow customer to have sufficient time to read and understand the notification message.

5.3.5 Anti-Money laundering

It has been found out that few customers still are not aware of what anti-money laundering is and how is related with mobile money transfer security, this enable money laundering to circulate easy and affecting the transfer money service and affect both customers and mobile operators and national in general.

To sort out money laundering, well-trained agents are proven to be effective in creating and driving customer's awareness. Training is an ongoing process that it should be updated regularly to reflect developments to the platform and changes to AML laws and regulations, as well as money terrorist financing trends and developments.

The AML training outlines how to comply with mobile money Anti-Money Laundering Procedures and to makes both customers and agents aware of the criminal and civil liability that they may face in the case of failure to report suspicious activity. The agents are also required to ensure that any staffs they hire or assign to process electronic money transfer transactions have received the appropriate training. An AML test is administered by the agency to ensure that agents have clearly understood the training.

5.3.6 Mobile Money operating system

Mobile money operating system has greater roles in fostering mobile security. The current operating system are sometimes cause customers transactions not to pass successful by stuck or remain in authorized or pending status, this pending status confuse customers not to be sure if what they have transact reach the intended recipient or not and reduce reliability of the system to customers.

To sort out or minimize fraud risk due to mobile money operating system, the mobile operator should come up with new system that are accommodate new technology and does not allow any mobile money transaction that are stacking, this is possible to be implemented although it is cost, this means all mobile money customers will be allowed to use STL SIM card instead of normal SIM cards that are taking many minutes to get notification SMS and also out time out quickly.

5.4 Further Study

Finally, the finding of this study is not final and conclusive of security of Mobile money transfer, because it has been founded that there are customers who sharing mobile money PIN with others persons like friends, relative or spouses which is dangerous in the E-money security, but due to time limit and financial problem the researcher did not look on the reasons of exposing mobile money PIN.

Therefore the study should be stimulant for further studies and could add further insight on security of mobile money especially regarding why customers are sharing mobile money security PIN so that we can have final say of Mobile Money security.

REFERENCES

- Bångens, Dr. L. and B. Söderberg (2008) “Mobile Banking –Financial Services for the Unbanked?” The Swedish Program for ICT in Developing Regions, SPIDER.
- Boer, Remco, and Tonnis de Boer. (2009). *Mobile Payments 2010: Market Analysis and Overview, version 1.01. Innopay. Available from* https://www.ebaportal.eu/_Download/Research%20and%20Analysis/2010/Mobile_payments_2010_Innopay.pdf; accessed on 22 June 2012
- Camner, Gunnar and Leishman, Paul and Pulver, Caroline and Sjöblom, Emil, 2009. “What Makes a Successful Mobile Money Implementation”. GSMA
- Camner G., Pulver C. & Sjöblom E. (2009): *M-PESA in Kenya and Tanzania*, FSD Kenya.
- C.R.Kothari – Research Methodology, methods and Techniques – Willy Eastern Ltd., 1999.
- Davidson N. & Leishman P. (2010): *Incentivizing a Network of Mobile Money Agents*, GSM Association.
- GSM Association (GSMA). 2007. Regulatory Framework for Mobile Money Transfers. Available from <http://www.mobilemoneyexchange.org/Files/8e31752b>; accessed 23 March 2012
- Jenkins, Beth. 2008. “Developing Mobile Money Ecosystems.” Washington, D.C.: IFC and the Harvard Kennedy School. Available from http://www.hks.harvard.edu/mrcbg/CSRI/publications/report_30_MOBILEMONEY.pdf. Accessed June. 9, 2012,

- Leishman P. (2009): Quarterly Update, *GSMA Mobile Money for the Unbanked*, GSMA Association.
- Mas I. (2009): "The Economics of Branchless Banking", *Innovations*, Vol. 4, pp. 57-75.
- Mas I. & Ng'weno A. (2009): *Three Keys to M-PESA's Success*, Bill & Melinda Gates Foundation, pp. 13-15.
- Mas I. & Radcliffe D. (2010): *Mobile Payments go Viral: M-PESA in Kenya*, Bill & Melinda Gates Foundation.
- Mas and Morawczynski (2009): "Designing Mobile Money Services: Lessons from M-PESA," *Innovations*, 4(2), 77-92, MIT Press.
- Mas, Ignacio and Kabir Kumar (2008): "Banking on Mobiles: Why, How, for Whom?," Consultative Group to Assist the Poor, Focus Note No. 48, Washington DC. Available from <http://www.mit.edu/~tavneet/M-PESA.pdf> . Accessed July. 20, 2012
- Pickens, Mark, and Brian Richardson. 2007. "Mobile Wallets and Virtual Currencies," in "Financial Services," *ICT Update* (36). Available from <http://ictupdate.cta.int/en/Feature-Articles/Mobilewallets-and-virtual-currencies>. June. 27, 2012
- Pickens, Mark. 2009. "Window on the Unbanked: Mobile Money in the Philippines." *CGAP Brief* (December). Available from http://www.cgap.org/gm/document-1.9.41163/BR_Mobile_Money_Philippines.pdf. Accessed June. 20, 2012

OMorawczynski, Olga and M, Mark Poor People Using Mobile Financial Services:
Observations on Customer Usage and Impact from M-PESA, CGAP
(http://www.cgap.org/gm/document-1.9.36723/MPESA_Brief.pdf)

Saunders, M., Lewis, P. and Thornhill, A. 2007. *Research methods for business students*. 4th ed. London: Prentice Hall.

Sarantakos, S. (1991), *Social Research*, London: Sage. UNCTAD Annual Report 2009

White, H. (2002) 'Combining quantitative and qualitative approaches in poverty analysis', in *World Development* 30(3)

APPENDICES

Appendix 1: Time Schedule and Budget

The study was conducted between the period of January, 2013 to July, 2013 in Dar es Salaam, Tanzania as per below descriptions;

Activity	Description
Activity 1	Introducing and briefing my intention to the selected entities and arrange for my visits and data collection.
Activity 2	Collected some supporting relevant information on mobile money transfer.
Activity 3	Visiting and collecting data from other stakeholders by sending questionnaires and arranging interviews with intended respondents
Activity 4	Data compilation
Activity 5	Data analysis and presentation
Activity 6	To compile report and prepare 1 st Draft
Activity 7	Present reports to supervisor
Activity 8	Report writing, Editing, Binding and submission

Activity	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13
Activity 1							
Activity 2							
Activity 3							
Activity 4							
Activity 5							
Activity 6							
Activity 7							
Activity 8							

Appendix 2: Questionnaire for determining security level of Mobile Money transfer in Telecommunication Industry in Tanzania.

1. What is your gender
☐ Male
☐ Female
2. What is your age?
☐ Below 30 years
☐ 31-40 years
☐ 41-50 years
☐ 51-60 years
☐ 60 +
3. What is your level of Education
☐ University Level
☐ Secondary school Level
☐ below Secondary school level
4. Do you understand what mobile money services are?
☐ yes, very well
☐ No, not at all
☐ I have heard about it
5. Are you registered customer for any mobile money service?
☐ Yes
☐ No
6. If yes, which mobile money service are you registered with
☐ M-PESA
☐ Tigo PESA
☐ Airtel Money
☐ EzyPesa

7. Do you use Mobile Money in transferring E-money?
[] Yes
[] No
8. If answer to question seven is YES, Are you familiar of the method that you are using in transferring E-money?
[] Yes
[] No
9. If answer to question eight is NO, skip this question. If answer is YES, which methods are you using in transferring E-money?
[] STK
[] USSD
[] Both STK and USSD
[] None of the above
10. Do you use mobile money services to transfer money to your relative or friends?
[] yes
[] No
11. How often do you use mobile money services?
[] Daily
[] at once week
[] at once per moth
[] never used.
12. Do you think Mobile Money transfer is safe means of transferring money?
[] Yes
[] No
[] I don't know

13. Have you experienced any security problem in transferring E-money?
- ☐ Yes
- ☐ No
14. Do you share or expose your mobile money PIN/Password with any other person?
- ☐ Yes
- ☐ No
15. If answer to question 14 is YES, do you think share or expose your mobile money PIN/Password with other person is safe?
- ☐ Yes
- ☐ No
- ☐ I'm not sure
16. If answer to question 14 is YES, Do you share your mobile money password/PIN with whom one?
- ☐ Wife/ Husband
- ☐ Close Friend
- ☐ Children's
- ☐ All of the above
- ☐ None of the above
17. Do you think password/PIN sharing is hindering security of Mobile Money?
- ☐ Yes
- ☐ No
18. Have you loss/theft any amount of E-money in unknown way since you started to use Mobile Money transfer service?
- ☐ Yes
- ☐ No
- ☐ I'm not sure

19. Do you think mobile money services will be safe in the years to come?
- ☐ Yes
- ☐ No
- ☐ I don't know
20. I there any day that you deposited fake money to Mobile Agent/ Bank?
- ☐ Yes
- ☐ No
- ☐ I'm not sure
21. I there any day that you withdraw money from Mobile Agent/ and given fake money?
- ☐ Yes
- ☐ No
- ☐ I'm not sure
22. Do you understand money laundering in mobile money?
- ☐ Yes
- ☐ No
- ☐ I don't know
23. If answer to question 22 is YES, Do you think money laundering affect mobile money service security wise?
- ☐ Agree
- ☐ Strongly agree
- ☐ Disagree
- ☐ Strongly disagree

24. Is the Mobile Money procedures are safe to use?
- ☐ Agree
- ☐ Strongly agree
- ☐ Disagree
- ☐ Strongly disagree
25. From company side, what might be the cause of fraud in Mobile Money services?
- ☐ Mobile Money Agents
- ☐ Mobile Money transfer methods
- ☐ Mobile Money operating system
- ☐ None of the above
26. From uses side, what might be the cause of fraud in Mobile Money services?
- ☐ Password/PIN sharing
- ☐ Customer awareness
- ☐ Mobile Money customers
- ☐ None of the above

	ARGUMENTS	Strongly Disagree	Disagree	Agree	Strongly Agree
27.	Mobile money transfer Methods are well identified				
28.	Customer awareness on Mobile Money security is highly provided by Mobile network operators				
29.	Security of Mobile Money is nowadays increased compared to previous years				
30.	Mobile Money operating system is well known				