THE EFFECTIVENESS OF MOBILE BANKING PHONE COMPANIES STRATEGIES ON PROMOTING SAFETYNESS OF CUSTOMERS MONEY IN TANZANIA: CASE STUDY OF VODACOM M-PESA, TIGO PESA, AIRTEL MONEY OPERATIONS IN MBEYA REGION: 2008-2012

CRISPIN KAIJAGE

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE MASTER OF LAW DEGREE IN INFORMATION TECHNOLOGY AND TELECOMMUNICATION (LL. M IT & T) OF THE OPEN UNIVERSITY OF TANZANIA

2013

CERTIFICATION

The undersigned certify that he have read and hereby recommend for examination a Dissertation entitled, **"Effectiveness of Mobile Banking Phone Companies Strategies on Promoting Safetyness of Customers Money in Tanzania: Case Study of Vodacom M-Pesa, Tigo Pesa and Airtel Money Operations in Mbeya Region, 2008-2012",** in partial fulfillment for the award of Master of Law Degree of The Open University of Tanzania.

…….

Prof. Ian. J. Lloyd.

(Supervisor)

……

Date

COPYRIGHT

DECLARATION

I, Chrispin Kaijage, 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 a similar or any other degree award.

……..……..

Signature

……..

Date

DEDICATION

This work is dedicated to my Mother, Yohanamaria Kaijage.

ACKNOWLEDGEMENT

Completion of this work would have been impossible without valuable contributions from many individuals, to all of whom I give many thanks. It would have been fair and just to mention everyone in this regard, but unfortunately time and space do not allow. However, it is deemed appropriate to mention at least few.

My supervisor, Prof. Ian Lloyd have supported and guided me throughout the progress of this work. His valuable inputs, criticisms and encouragement have significantly contributed in the shaping of this Dissertation and making it reach this standard. I am sincerely grateful to him.

I am also grateful to Dr. Suzane Kolimba and Gervase Emmanuel, both of the Open University of Tanzania (O.U.T) faculty of law, for their helpful suggestions on the initial proposal and Dissertation approval form of this Dissertation. And also Mr. Selestine Ramadhani from Bank of Tanzania- Mbeya zone for his valuable comments on its proposal and outline and for allowing me to have access to his mini-library.

I am also grateful to a number of respondents whose comments have enriched this work. I thank all of them for the time they took in responding to a number of questions in relation to this Dissertation during field research. In this respect, I wish to especially thank Mr. Nuru Abdallahmed and Timoth Mulisa from the office of the Attorney General- Dar-es-salaam head quarter and Mbeya zone.

Lastly, but not least, I would like to thank my wife Marina Kaijage for her love, care and prayers. Indeed she was always behind me during the whole period of my studies just to make sure that I had all that I needed. Again my father, Cyprian Majaliwa and our child, Innocent has always been a blessing and an inspiration to me.

ABSTRACT

This work investigate the effectiveness of strategies used by mobile phone banking companies in Tanzania to ensure that there is maximum possible safety of customers money, through preventing loss of customers money through frauds by mobile phone banking employees, and incorrect entry by customers who use a network of mobile phone banking system. The study was motivated to be undertaken to increase number of customers who lose their money through a network of mobile phone banking system, and also through increasing amount of money of customers that is lost through increasing amount of money of customers that is lost through the network of mobile phone banking system in Tanzania. The study area was Mbeya region, and used a sample of three mobile phone companies which offer the services of mobile phone banking, namely Vodacom, Tigo and Airtel. The study used a field sampling survey method, and a combination of primary and secondary data. Primary data was collected through a combination of questionnaires, interviews and observations methods from customers duties of sending money, and at normal interviews when customers explains what they have encountered. Also an interview was done with the management of the Bank of Tanzania (B.O.T) and the Tanzania Communications Regulatory Authority (T.C.R.A) as the main regulators. Again interviews were done with selected commercial Banks in Mbeya city which use partnership mobile banking services with mobile phone companies, these were CRDB, NMB, Stambic and Barclays. The study found that since the year 2008, more customers in Mbeya region and other parts in Tanzania have been losing huge amount of money through frauds done by employees of mobile phone companies and incorrect entry by both customers and employees of the companies, hence causing customers to incur huge financial loss.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF LEGISLATION

PRINCIPAL LEGISLATIO

Tanzania

The Tanzania Communications Regulatory Authority Act, N0. 12 of 2003

The Electronic and Postal Communications Act, N0. 3 of 2010

Other Countries

United States of America

The Electronic Funds Transfer, Act of 1978.

Malaysia

The Malaysia Electronic Funds Act.

India

India Information Technology Act, 2000

LIST OF CASES

Joachimson V. Swiss Bank Corporation, 1921 ALLER 92 at 3KB 110.

Chettinad Ltd of Colombo V. Income Tax Commissioner, 1948 A.C. 378.

Union Dominion Trust V. Kirkwood (1966) 1 ALLER Page 968

LIST OF ABREVIATION

ATM	Automated Teller Machine.
ALLER	All English Report.
BOT	Bank of Tanzania.
CLF	Converged Licensing Framework.
EFT	Electronic Funds Transfer.
ID	Identity.
ICT	Information and Communication Technology.
IT	Information Technology.
M	Mobile
MOU	Memorandum of Understanding.
NBC	National Bank of Commerce limited.
NMB	National Microfinance Bank.
O.U.T	Open University of Tanzania.
PIN	Personal Identification Number.
PU	Perceived Usefulness.
TAM	Technology Acceptance Model
TCRA	Tanzania Communications Regulatory Authority.
TTCL	Tanzania Telecommunications Company Limited.
UK	United Kingdom.
USA	United States of America.

CHAPTER ONE

1.0 INTRODUCTION

1.1 Introduction

Banking services are of more importance for the general promotion of country economic development. This is because banks perform different important roles in the economy such as important areas where government implements its monetary policy. Banks also offers payments mechanism in the economy. Also through banks transfer of money from one part of the country to another or from one person to another can be facilitated and hence sped smith transactions.

Due to the development of technology, now Tanzania like in Kenya and Uganda and in other parts of the world experience the growth of mobile phone banking where by customers registered with mobile phone banking industry conduct some of their banking transactions through a network of mobile phone. However as is the case where money /financial transactions are conducted, safetyness of customer's money is of great concerned to both customers of mobile banking services, Mobile Phone Company and the government through the Tanzania Communication Regulatory Authority (TCRA) as the Regulatory.

That's why the Communication, Science and Technology deputy minister January Makamba in Tanzania said once that, mobile phone users who make money transactions through cellular networks must be protected, he said TCRA and the Bank of Tanzania (B.O.T) should discuss how to protect such people due to millions of shillings deposited in their SIM cards**,** (The Guardian, May 24, 2012). It is this

views that has motivated to undertake this study in order to investigate effectiveness of mobile phone companies strategies on promoting safetyness of customers money banked through mobile phone banking in Tanzania.

1.2 Background to the Problem

In order to make banking services be available to more people in the country, in both rural and urban areas, the Government of Tanzania allowed mobile phone banking firms to offer the services of banking to the public. These ware like accepting customers money deposits, allowing customers to withdrawal money from their accounts, and facilitating customers to make various payments such s school fees, electricity bills, water bills etc using the network of mobile banking system. The move to this action was taken since the traditional banking services were limited mainly in few urban areas, leaving majority of people to travel a long distance to get the banking services, while also weakening the national payments system in the country. The overall effects of these were to contribute to slow down the economic development of the country.

Banks are important to the development of the country since they help to mobilize financial savings from different savers in the economy, such as individual households, Business firms and Government. These savings in turn are used to give loans to different borrowers in the economy for personal and investment purposes. Due to the development of technology, currently there have been tow major groups of banks in the economy, namely traditional banks with fixed building premises and branches in other parts of the country offering banking services to its segmented

customers, and mobile phone banking services where by mobile phone companies such as Airtel, Vodacom, Zantel etc are offering mobile banking services to its customers. In that case, these mobile phone banking services become substitutes to traditional banking companies and have the advantages that there services are available to most people in more areas than the case is with traditional banking companies in the economy.

But in other cases, these mobile phone banking series from mobile phone banking companies are complements to traditional banking services since in other cases, there are cooperation's between traditional banking firms such as Barclays Standard Bank etc with mobile phone companies offering mobile phone banking services, whereby customers can transfer money (such as making deposits and withdrawals) from his account in the traditional bank to his mobile bank account managed by the mobile banking firm and vice versa. This implies that the services of mobile phone banking companies are both substitutes and complements to the services offered by the traditional banking business firms.

Most experts in the field of banking law such as Summer and White (2008); Carnell (2011), Carnell et all (2008) have strongly stressed on the need of management of financial institutions to formulate and implement proper financial security policies which promote maximum security of their customers money kept at their money which in the end may in crease poverty in the economy. This is because most customers deposit millions of shillings in their SIM cards (*The Guardian may 24, 2012).*

Up to the year 2004, all banking services in Tanzania to both public government institutions and private institutions was done through the traditional banking .These banking services were like;

i) Keeping customers deposits

ii) Customers withdrawals of money

iii) Money transfers

iv) Payments of schools fees

v) Payment of medical fees

vi) Paying interest by agreement on deposits

vii) Collecting notes and drafts deposited

viii) Issuing letters of credit

ix) Selling its drafts or cheques on other banks and banking correspondents

x) Receiving money on deposits from its customers.

By the year 2004, banks offered banking services to people inside and outside Tanzania were like National Bank of Commerce (NBC), CRDB Bank, Postal Bank, Stanbic Bank, National Microfinance Bank (NMB), Diamond Trust Bank and Barclays Bank. However despite their significance, most of these banks had also sole problems with respect to their offered services such as;

i) Most of them are located in few major urban areas,

ii) Sometimes it takes a lot of customers to complete certain specific banking transaction.

As a response to the demand and supply need, accompanied with a change in technological development, in the year 2008 mobile phone companies in Tanzania started to offer banking services to the public. These banking services offered by mobile phone services are like;

i) Depositing money in the SIM cards,

ii) Withdrawing money from the SIM cards,

iii) Transfer of money to another account

Currently in Tanzania mobile phone banking services is offered by the following mobile phones companies as follows;

i) Vodacom Tanzania Ltd……M-Pesa,

ii) MIC (T) Limited……...Tigo pesa,

iii) Airtel (T) Limited…….Airtel Money,

iv) Zantel……Ezy pesa,

1.3 Statement of the Problem

Safetyness of customer's money is of more importance for the any banking institution, including mobile banking phone company services. In Tanzania, Mobile banking services is offered by Mobile banking Phone Companies like Vodacom, Tigo, Zantel and Airtel. However, While most people are increasingly joining the services, more people are also complaining about losing their money due to theft conducted by criminals collaborating with employees of mobile phone companies or incorrect entry made by the customer himself or both (Central Bank of Tanzania Annual Report. 2011)

Recently it has been revealed that a lot of money expected to be Tsh. 2.6 billion from Vodacom M-Pesa accounts were stolen by the employees (Central Bank of Tanzania fraud prevention unit Report 2012). This has made more people to complain that mobile phone company's security strategies are increasingly more ineffective, leading to increasingly loss of customers money. Todate little researches have been done to investigate this issue and this has motivated the researcher to undertake this study.

1.4 Literature Review

This chapter presents Literature review of the research. Section 2.2 presents theoretical Literature on traditional banking and mobile phone banking system. Section 2.3 Presents Empirical Literature on frauds in traditional and mobile phone banking system. And section 2.4 Presents gaps that have been covered by this study after reviewing both theoretical and empirical literature.

1.4.1 Theoretical Literature

Frauds of customer's money stored in the network of both formal and traditional banking system have been a major problem facing the banking sector all over the world. These frauds have been noted to be the results of joint actions by employees of the banks, outsiders, combination o f employees of the bank and poor information handlings of the customers of the bank whose accounts are frequently frauded by criminals. Poor measures undertaken by the management of the bank to prevent these financial frauds have also increased the severity of the problem. For the case of frauds in the mobile phone banking system, proper lack of proper information on how to protect their information from being acquired by unwanted personnel's, have

made criminals be in a good position to acquire sensitive information of customers accounts and be in a good position to steal the customers money. That problem have been accerelated by poor measures undertaken by mobile phone banking companies to educate their clients and general public on how to protect their accounts information from being accessed by unwanted personell, which could have been resulted into facilitating stealing their money stored in the network of mobile phone banking system.

The security of customer's money within the banking system has been receiving wide attention among various scholars. Various measures have been proposed to protect customer's money stored within the accounts of the customers managed by the banking firms. These measures are in general divided into two parts namely those measures that should have been executed by the customer himself whose accounts is managed by the banking firm, and those measures that should be executed by the banks through its employees, who are in constant contact with all details regarding customers money stored in the accounts of the banking system. The supplementary measures are those that are concerned taking security measures against the third part outsiders who may inflict customer's accounts and stole customers money, either individually, or in collaboration with unfaithfully employees of the bank.

With The development of technology, nowadays mobile phone banking system have come to spread in larger parts of each country and be used by many more people in both rural and urban areas, due to its convenience in that mobile phone banking

system can be available in various areas even in remote areas and at any time, compared to the traditional fixed premises banking system. But the development of mobile banking system has also go hand in hand with development of sophiscated frauds measures that have been used by criminals to steal customers money from the network of mobile banking system.

In other cases, that theft is done within the accounts of customers managed only in the mobile phone banking accounts, and also in some times in the accounts of customers managed in the traditional fixed premises banking system, where by there are interconnection between mobile phone banking system and traditional banking firms accounts when a customer can deposit his money into the accounts of traditional banking firm from his accounts in the mobile phone banking system, and vive versa.

Since the year 2000, it has been reported that cyber-attacks have mostly targeted the banking sector, both traditional banking system and mobile phone banking system all over the world. These includes the ATM and Internet banking applications, Mobile phone banking and the combination of either mobile phone banking and internet banking, internet banking and formal banking system or the mobile phone banking system and the interment banking, or the combination of two or all of the mentioned groups of banking system**.** Fraud cyber crime in banking sector has been growing all over the world. Bank Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone bank account for the purpose of stealing some one money stored in the accounts of the bank. For

instance, making a false bank webpage to retrieve information of account of someone. The concept is simple, someone gains access to your personal information and uses it for his own benefit. This could range from a black - hat hacker stealing online banking account login and password to getting access to ATM, mobile phone banking system and using such people can make themselves a lot of money with personal information.

The modern contemporary era has replaced these traditional monetary instruments from a paper and metal based currency to “plastic money” in the form of credit cards, debit cards, etc. This has resulted in the increasing use of ATM all over the world. Another form of money that have been developed due to development of technology is electronic money usually executed in the mobile phone banking system and internet banking system of the banking sector.

Due to changing in technology the banking industry is also changing rapidly. Development of international economics and competitive markets also has affected the banks. Technology is a major force in this environment that led to breaking the geographical legal and industrial barriers and has created new products and services. In recent years with growth and development of information technology all aspects of human life have been radically transformed. Meanwhile financial institutions like banks are not the exception, and have undergone major changes in the management methods and processes and system oriented and information-based business. In recent years mobile banking services along with internet banking services have fundamentally changed the ways and method of doing daily activities by bank

customers, and banks have also used it not only as a new way to increase profitably.

Meanwhile mobile banking is one of the main branches of the mobile commerce that has critical and influential role on other areas of the business. Mobile banking is a payment method that applying it in an appropriate manner can greatly reduce the banking costs. To survival in the competitive world of modern banking, banks need to pay attention to optimized management of necessary costs in using various technologies, and use the best methods to create minimum cost for banks.

Use of mobile banking greatly reduces the banking costs, on the other hand it increasingly provides customers satisfaction through easy access to financial transactions at any time and place with the lowest possible too (just a mobile phone) instead of waiting hours in line at the box office bank . The term “mobile banking “refers to the use of mobile as a channel of offering and delivering banking services which includes traditional services such as funds transfer as well as new services such as on line and electronic payments. In fact mobile banking is defined as doing bank transactions via mobile phone.

Mobile banking services will continue to grow in Tanzania and other developing and developed countries. Meanwhile, one of IT management concerns, Particularly in the field of mobile banking is the attitude of customers to this technology and its adoption among customers studying the determinants of mobile banking adoption will lead to a better understanding of beliefs and ideas that propel the potential users to use the new technologies, and considering how and types of users, attitudes,

creates the conditions that accelerates the adoption of mobile banking by customers.

Victoria Yemi-Peters (2011) points out that the security in mobile phone banking system is of very importance both to the mobile phone firm and the customers who use the services of mobile phone banking system. She points that in an attempt to increase their customer base and reduce costs, financial institutions constantly look for new and better delivery channels for their services. As customers demand faster, more security and convenient services, financial institutions turn to new technologies to expand their customer relationships to compete with other financial service providers.

This project work provides a convenient mobile phone service for bank customers to transact business with their financial institution with the use of their mobile phones, taking into cognizance the vital issue of security. She noted that one of such security devices that have been used by mobile phone banking firms are JAXWS (Java API for XML web server) which was used to develop the application as the front-end engine, while Microsoft server 2008 and MySQL were used as the back-end engine using the WEP protocol concept and Julius ceaser cipher text. Java 2ME (J2ME or Midlet) is used to develop the application that controls a small computing device. She concludes that iIn this project work, a simulated cell phone is used as interface between the customer and the server.

Pavan_duggal (2013) points out that the use, adoption and continues reliance on mobile phones and communication devices has given rise to a new kind of economy, which has made the use of mobile phone to further propelled growth of new lining

sytiles. He further points that nowardays, more and more people are today relying upon mobile phones for the purposes of not only for communication, or accessing the Internet but also making purchases and also dealing with their moneys through the network of mobile phone banking system. All these implies that the mobile phone firms involved with the banking issues should increasingly take into accounts the issues of security of customers moneys.

Mobile Phone baking system operated through a network of computer system . Hence a fraud in the mobile phone banking system directly linked with computer cyber crime. According to Taylor, 1999, computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of computer system by putting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud .

Pednault, S (2009) points out that fraud within the banking sector, continues to be the fastest growing and most costly crimes in the United States and around the world. He further notes that if an organization can learn well about fraud in general and the potential fraud risks that threaten the financial stability of the organization's cash flow, it will be in a good condition to be equipped to design and implement

measures that prevents frauds in the banking system of the country.

Akindele R.I (2011) in examining frauds in banking and other financial institutions, points out that Frauds in financial institutions vary widely in nature, character and method of perpetrations. He classified frauds into the following groups: based on perpetrators and method used on the basis of perpetrators. These groups of frauds in the financial sector noted by Akindele R.I (2011) are: -internal, external and mixed perpetrations. Internal perpetrators are made up of the staff of the financial company, external perpetrators refer to outsiders not connected with the financial institution, mixed refers to collusion between the staff and external parties.

The major objective of mobile phone banking system, unlike the traditional fixed premises banking system, is to provide customers with access to their bank accounts through their cellular phones. In order to comply with acceptable industry standards for access into a bank account, and ensure that there is maximum safety and security of customers money stored in the mobile phone banking system, a combination of security measures should be observed by both the customer who has deposited his money in his accounts managed and operated by the mobile phone banking system, and also by the mobile phone company that operates the mobile phone banking system. Among these measures are these summarized there: the first item to consider is the successful authentication of the customer. Once authentication is done, the information that is transported between the bank and the customer's cellular phone needs to be encrypted to eliminate interception by non-authenticated parties.

Kruger (2011) points that in mobile phone banking system, the security approach in

a cellphone banking application is crucial, because the customer will use the cellphone to access his bank account remotely by utilising the network reach of his GSM mobile network operator. The cellphone banking application will allow the customer to view balances in accounts and to transfer money from his account to any other bank account, it is of the utmost importance that the cellphone banking application enforce that each transaction can only be executed by the owner of the bank account. Application security in a cellphone banking application must assure non-repudiation of transactions. This implies that there must always be proof that the originator of the transaction was uniquely authenticated before the transaction was processed on the bank account.

To assist with proper authentication it is recommended that the approved technology always use a Two-factor authentication mechanism of something you have "(your cellphone) and something you know" (your cell phone banking Personal Identication Number (PIN)). To comply with the first factor of authentication which is \something you have", it is recommended that the application is designed to ensure that the mobile handset or unique SIM card is always linked to the customer during the registration process in the cell phone banking platform. This approach will limit the customer to only access the cell phone banking application from his own handset and it will eliminate fraudulent by any person intends to steal others money stored in the mobile phone banking accounts operated by the mobile phone company. The second portion of the two factor authentication mechanism is a unique PIN that is selected by the customer during the registration process. PIN selection is important to assure that the customer's identity is not comprised. It is recommended

that customers select unique cellphone banking PIN codes, while the application must be designed to not allow weak PIN combinations.

In order for the PIN to be effective in protecting customer's money, the customer must be forced to change his cell phone banking PIN on a regular basis. This is embraced from a security perspective but experience has shown that people tend to have one PIN for multiple applications. For example customers select the same PIN for their bank card as well as for the cellphone banking PIN. Our experience in different countries proved that if you continuously force customers to select a new PIN after a certain period of time

has elapsed, customers will become resistant and negative about the product and could even stop using both the card and cellphone banking product. To assure security even further, it is recommended that all transactions with financial impact is notified to the customer through an alert service. The advantage of a cellphone banking application is the fact that the bank will always have the Mobile Station Integrated Services Digital Network or cellphone number (MSISDN) of the customer and it allows the sending of transaction notifications immediately to the customers at the time of the transaction through an SMS alert service.

To support the security of a cellphone banking solution, it is good practice to introduce. Associated daily limits for the transaction types that will be delivered by the solution. The introduction of daily limits combined with transaction notifications that will notify the customer of fraudulent activity will make cellphone banking less vulnerable for attacks and mitigate the potential fraud risk. It is in the discretion of

the bank to determine the value of these limits but the rule of thumb is that it needs to be small enough amounts that discourage fraudsters in attempting to bridge the security of the solution.

As part of the security of a cellphone banking solution, a bank will have to evaluate the ease of use of end to end encrypted channels compared to more easily accessible channels with less security in place. The author is of the opinion that the target market for the cellphone banking application will determine the security measures of the solution and further chapters will illustrate this opinion.

Samuel Maimbo, Tania saranga and Nicholas Strychacz (2010), proposes that the use of mobile banking is increasingly becoming important since it facilitate smooth economic growth by facilitating quick and smooth financial transactions in two ways namely: First , Mobile banking may enable faster and more efficient financial transfers increasing the volume of trade and subsequent payments of workers and their families. This dynamic is especially important for informal trade which is practiced primary by low-income unbanked international, regional and domestic migrants. Second mobile banking greatly increases access to finance for large segments of the unbanked populance in both developed and developing countries.

Adrian. D. kamotho Njengwa (2007), proposes that the terms mobile phone banking and mobile banking (M-banking) are used to donate the access to banking services and facilities offered by financial institutions such as account-based savings, payment transactions and other products by use of an electronic mobile device. Mobile banking has yielded a multiple effect on the number of solutions available to

clients. This is in addition to more efficient transactional environment and the high substitution of banking points.

Porteous (2006), distinguishes two aspects of mobile banking; Additive and transformational characteristics. Additive aspects are those in which the mobile phone is merely another channel to an existing bank account. Mobile banking is additive when it merely adds to the range of choices or enhances the convenience of existing customers of mainstream financial institutions. Transformational characteristics arise when the financial product linked to the use of the phone is targeted at persons who do not hold formal bank accounts with the conventional banking institutions.

Sacker and wells (2003), assent that the only single access requirements or barrier to the resultant mobile banking will be the mobile phone. However, worldwide market penetration of affordable cellular devices and growing network services device diffusion makes this intricacy almost fully resolved hence setting a firm pedestal for mobile banking escalation. The effects of usage associated with mobile phone banking in Kenya are yet to be consolidated or quantified in a well documented fashion .With the dramatic adoption of mobile banking services this study seeks to extend its scope of analysis to indicators that reflect the nature of usage. This ranges from overall patterns of use, access and provision strategies and consumption patterns. The study provides a baseline against which to assess the usage patterns and characteristics analyze the gains and challenges emanating from the ***Abdolreza*** Begonia et al (2011) formulated an extended theory of planed behaviour to study customer's attitude to mobile phone banking in Iran.

In most of the previous researches in the field of electronic banking have focused mainly on the technology adoption based on planned behaviour model they noted that Shih and Fang have done intensive studies on individuals beliefs attitudes perceived behavioral intentions .However, most studies conducted in the field of electronic banking adoption models, an important factor such as quality and properties of electronic banking services on which mobile banking is defined, is not considered. They further add the common five factors related to mobile banking services (information quality transaction speed ease of use the banks reputation and security of the mobile network) to get a model that explain traditional factors in theory of planned behaviour to obtain a better understanding of customers attitudes toward mobile banking.

1.4.2 Empirical Literature

Samuel Maimbo, Tania Saranga and Nicholas StryChacz (2010**),** conducted study to determine the role of mobile phone banking on facilitating cross border trade in southern Africa using a supply side approach. They found that mobile phone banking was becoming more popular in southern Africa and used to facilitate cross border trade by migrant labourers, there are several reasons why many migrants choose to use informal channels, rather than the formal financial sectors to remit payments such as;

i) Ease of use migrants prefers methods with less paperwork.

ii) Familiarity informal channels have been used or recommended by family and friends

iii) Costs-Higher costs in the formal financial sector drive away migrants.

Fees in informal net works tend to be lower than at banks or with money – transfer operators. Since in some cases the cost of formal transfers can be up to six times as great as those of informal transfers with fees exceeding 50 percent of the remittance value.

iv) Risk tolerance – there is a perception among migrants that banks are untrust worthy and may loose or steal migrants money.

v) Access- it can be difficult for the recipient to reach the point of delivery.

vi) Source of remittances- Many migrants are working in the informal labour sector in South

vii) Africa, so their remittances are, by definition the result of illegal employment. They recommended that, the government in Africa should, provide policy support for branchless mobile phone banking initiatives that target the unbanked population. Also African countries can learn from branchless mobile phone banking leaders around the world.

Grutam Ivatury and Mark Pickens (2006) conducted a field study to determine the role of mobile phone banking on promoting economics poverty reduction among low income people in South Africa, using sample of 215 low income WIZZIT mobile phone company users, and 300 mobile phone company low-income non users. They found that four main findings emerged from the surveys. First low income people use mobile phone WIZZIT`S M-banking services and give it high ratings for convenience, costs, and security, second, although the users surveyed are low-

income people, they are not among South African's poorest people. They tend to have higher income and assets than non users and also greater financial and technological sophistication.

Third, although users and non users say they are open to using new technology, they still value human interaction. Finally, beyond how awareness, some potential customers do not use WIZZIT because they also perceive themselves as ineligible for bank accounts and see M- banking as expensive and insecure. This study covers the gap since it examines strategies mobile phone banking companies in Tanzania on ensuring safetyness of their customers money transacted through mobile phone banking network system.

However, as the case with transactions in the money sector some insecurities in the conduct of mobile phone banking have started to be experienced by increasing number of customers using these mobile phone banking services, (Bank of Tanzania annual Report, 2011). These insecurities experienced by Mobile phone banking customers in Tanzania are like;

i) Customer's accounts (mobile phone numbers) are debited without the consent of the owners of that accounts,

ii) Customer's money is transferred without the permission of the owners account,

iii) It is easy to enter into customers account because most of their PIN numbers is like years of birth e.g. 1960, 1967, 1950 and 1955.

iv) Few employees who are expert in IT, they just collaborate with other

employees in those companies who are not faithfully,

v) The duty of Secrecy is not observed especially by the employees and agents,

In general mobile phone banking customers of Vodacom M-Pesa , Airtel Money and Tigo Pesa Country wide are summarized below.

1.5. Research Objectives

1.5.1 General Objective

General objective of this study was to investigate effectiveness of mobile banking phone companies strategies on promoting safeties of customers money in Tanzania with reference to Mbeya region for the year 2008- 2012 period.

1.5.2 Specific Objectives

Specific objectives of this study were:

i. To investigate the effectiveness of mobile phone banking companies security strategies on preventing frauds of customer's deposits within their companies in Tanzania with reference to Mbeya region for the year 2008-2012 period.

ii. To investigate the effectiveness of mobile phone banking companies security strategies on preventing loss of customer's money through conduct of incorrect entries by customers.

iii. To suggest solutions that will make mobile phone companies to formulate and implement effective security strategies that will ensure maximum safety of customers money deposited /transacted through their financial network.

1.6. Significance of the Study

This study will be more significant to research in the field of banking, mobile phone banking and market competition. Moreover it will provide materials for further research. The study will also enable the researcher meet requirements for the awards of masters degree.

1.7. Research Hypothesis

i. What are the effectiveness of mobile phone banking companies security strategies on preventing frauds of customers deposits within their companies in Tanzania?

ii. What are the effectiveness of mobile phone banking companies security strategies on preventing loss of customers money through conduct of incorrect entries by customers?

iii. What are the solutions that will make mobile phone companies to formulate and implement effective security strategies that will ensure maximum safety of customer's money deposited and transacted through their financial network?

1.8 Research Methodology

This chapter presents methodology of the research. The information gained from this chapter will be used to facilitate data analysis and Presentation, Findings, Conclusion and Recommendations of the study.

1.8.1 Definition of Key Terms

1.8.1.1 Mobile Phone Company

A company that deals with portable telephone dives that does not require the use of landlines, Mobile phones utilize frequencies transmitted by cellular towers to connect the calls between two devices 'the 'first mobile phone operated on analog service and was developed by Motorola inc, Mobile phone have grown to be the most widely used portable devices in the world,

1.8.1.2 Bank

Is a corporation empowered to deal with cash, domestic and foreign, and to receive the deposits of money and to loan those monies to third-parties. In the Case of *Joachimson v. Swiss Bank Corporation,* 1921 AIIER 92 and at 3KB 110, Justice Atkin wrote "the bank undertakes to receive money and to collect bills for its customer's account."

Again, in the case of bank of Chettinad Ltd of Colombo v. Income Tax Commissioner, 1948 A.C. 378, the Privy Council (England) describe a bank as "….a company which caries on its principal business the accepting of deposits of money on current account or otherwise, subject to withdrawal by cheque, draft or order…."

Moreover, in the case of *Union Dominions Trust v. Kirkwood* (1966) 1 All English Reports, at page 968, Lord Denning deferred to these words to define a bank; "an establishment for the custody of money received from or on behalf of its customers. Its essential duty is to pay their draft on it; its profits arise from the use of money left unemployed by them."

1.8.1.3 Mobile Phone Banking

Is the use of a smart phone or other cellular device to accomplish tasks such as checking account balances, transferring funds between accounts, bill payment and finding an ATM while away from a computer

1.8.1.4 Security Measures in Mobile Phone Banking Sector

These are security measures that are formulated and implemented in mobile banking sector in order to ensure that customers and their money transacted are safe to the maximu possible level.

1.8.1.5 Frauds Deposits of Customers Money with Mobile Phone Banking Sector.

These frauds conducted on mobile banking customers money by criminals either alone or sometimes in collaborations with mobile phone employees, or a combination of both.

1.8.1.3 Financial Transactions in the Mobile Phone Banking Sector

These are financial services conducted through a mobile phone banking system and consists money deposits, sending money, receiving money and payments of various fees such as electricity fees, school fees, medical fees, water bills etc through a network of mobile phone banking system

1.8.2 Area of the Study

This study is going to cover Mbeya region in Tanzania. This area has been chosen because it is one of the region in Tanzania that has been reported to be affected more

by theft of customer's money stored within their accounts managed by the mobile phone banking firms namely Vodacom, Airtel, Tigo, Zantel and TTCL. Mbeya region activities are dominated by food crop production, cash crops production, trade, financial sector, Government public administration and social services. Increase use and expansion of these sectors in Mbeya region as is the case with other parts of Tanzania has caused more and more people to increasingly join and use the services of mobile phone banking system for the combination of purposes of keeping money, transferring-sending money to other people in other distant areas and receiving money sent from other distant areas.

1.8.3 Period of Study Date

This study is focusing from the year 2008 – 2012 periods. This period has been chosen because it is the period that has been witnessed massive loss of customers money stored within the network of mobile phone banking system in the country, and particularly in Mbeya region.

1.8.4 Types of Data used

In Research, data is information that is used to compile research report. This study used a combination of data specified as follows: Qualitative data, Quantitative data, primary data and Secondary data. These were further subdivided into cross section data and time series data. The study use a combination of primary data and secondary data. Primary data are those that were for the first time collected by the researcher, while secondary data are those data obtained from published and

unpublished documents which in turn implied that these data were already collected by other researchers. On the other hand, time series data are those data that are expressed in a single point of time such as days, month, years etc. Cross section data are those data that are expressed across different category of the same variable. Quantitative data are those data that can be measured in quantities such as tons, money values etc. Qualitative data are those data that cannot be measured well in quantities but are expressed in qualities such as bigger, smaller etc.

1.8.5 Methods of Data Collection

Primary data is collected using a combination of the following methods: Interview Methods, Questionnaire methods and Observation methods Secondary data will be obtained from published and unpublished documents in private and Public institutions.

1.8.6 Tools of Data Analysis

The collected data will be analysed using tables, charts, graphs, mathematical calculations and Computer programs like excel and Spss.

1.8.7 Conceptual Framework

To what extent does mobile banking system is Tanzania has covered the financial inclusion?

In this study many models have been proposed to explain and predict the use of a system but for the case of environment that the researcher chose to conduct her sty, the Techninology acceptance Model was taken into account since it has been the

only one which has captured the most attention of the Information Systems community (Venkatesh & Davis, 200).

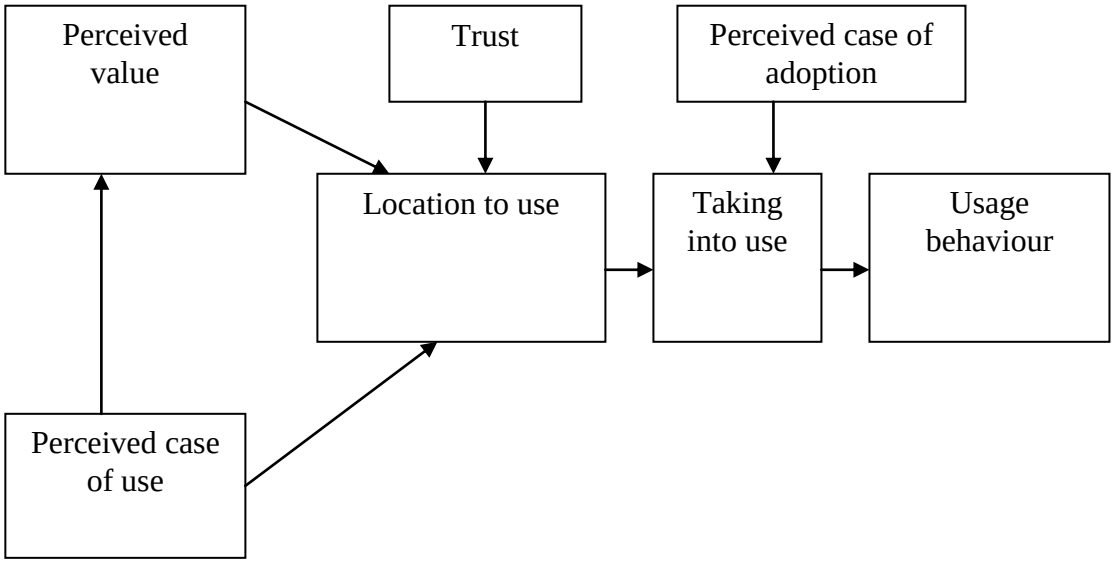

Figure 1.1: The Technology Acceptance Model

Source: From field researcher, 2012

The model suggests that when users are presented with new technology, a number of factors influence their decision about how and when they will use it (Venkatesh & 2008). Hence from the above model the usage behaviour of mobile subscribers (customers) in using a technology (M-Banking) are predicted to be much dependable on the perceived value of the technology and the perceived case use of it that will bring forward the intention to use the perceived technology. The following are defined factors influences users with the usage behaviour of the new technology:

1.8.7.1 Perceived Usefulness (PU)

This was defined as degree to which person believes that using a particular system will enhance his or her job performance (Fred Davis, 1989).

The major Conceptual frameworks of this study are expressed below:

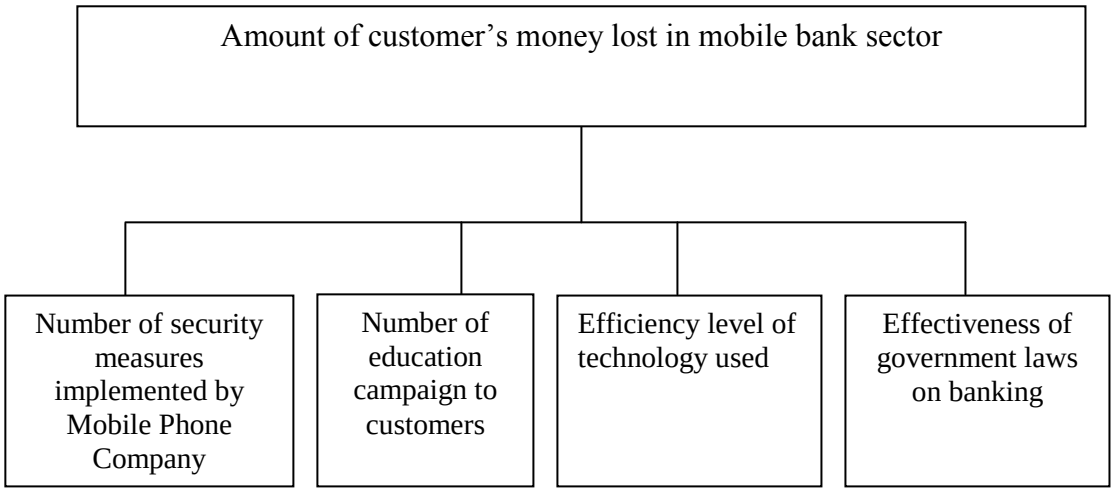

Figure 1.2: The Major Conceptual Frameworks of this Study

Source: From field researcher, 2012

From the above conceptual frame work this study will use the following model:

$AML = a_0 + a_1 NSM + a_2 NED + a_3 ET + a_4 BL$

Whereby:

a1= Coefficients of the variables

AML = Amount of customers money lost in mobile phone banking system each year.

NSM = Number of education campaigns to customers.

ET= Efficient level of technology.

BL = Effectiveness of banking laws.

1.8.8 Population

Population is the possible units or variables whose data will be collected and that will be used in the analysis of the research. In This research, Population of the

study will consist 4 mobile phone companies which are Vodacom, Tigo, Airtel, and Zantel. Ten banks operating in mbeya region which have linkage cooperation with mobile phone. Companies to facilitate money transactions between customers, mobile phone companies and banks, 200 customers who have used and experience money loss in the conduct of mobile phone banking Company and 600 customers using mobile phone banking services but have not yet experience any financial loss, 20 employees of banks, 40 employees of mobile phone companies.

1.8.9 Sampling

In Research, a sample is few items that have been selected from the population and this is done for the purpose of facilitating data analysis. This study will use a new probability sampling method known as value judgment sampling method. Where by items for final selection for the purpose of analysis will be selected based on views of researchers. In this case sample will be 150 customers that have experienced financial loss, 200 Customers not yet experiencing financial loss, 10 employees of banks and 20 employees mobile Phone Companies in Mbeya region that offer mobile phone banking services.

i. To investigate the effectiveness of mobile phone banking companies security strategies on preventing frauds of customer's deposits within their companies in Tanzania with reference to Mbeya region for the year 2008-2012 period.

ii. To investigate the effectiveness of mobile phone banking companies security strategies on preventing loss of customer's money through conduct of incorrect entries by customers.

iii To suggest solutions that will make mobile phone companies to formulate and

implement effective security strategies that will ensure maximum safety of customers money deposited /transacted through their financial network

CHAPTER TWO

2.0 HISTORICAL DEVELOPMENT OF MOBILE PHONE COMPANY

2.1 Performance of Mobile Phone Companies in Mbeya

Mbeya Region is served by five mobile phone companies which are Vodacom Tanzania, Tigo, Airtel, Zantel and TTCL. These mobile phone companies apart from offering traditional mobile phone services, they also offer mobile phone banking services which are known under various names such as M Pesa for vodacom, Tigo Pesa for Tigo and Z-Pesa for Zantel. Like other parts of Tanzania, most customers of these mobile phone companies have increasingly complaining about the loss of their money while making transactions, or through frauds made by other criminals and sometimes in collaborations with unfaithfully employees of mobile phone banking operating in Mbeya. In general, this has motivated the researcher to undertake this study.

Table 2.1: Performance of Vodacom M- Pesa Mobile Banking Services in Tanzania, 2008- 2012

Year	NO. of M-pesa customers (Registered and unregistered)(Million)	Amount of money transferred (Tsh. Million)	Amount of money lost (Tsh. Million	Number of customers lost money through unknown theft	Number of customers lost money through entry	Number of customers left money through incorrect entry
2008	6.00	13,700	1507.00	15,100	98,200	38,795
2009	7.4	25,100.00	3,012.00	18,750	170,600	104,278
2010	10.0	598,300	2,1626.00	31,258	230,540	168,402
2011	15.4	778,600	5,1794.00	48,945	350,650	258,387
2012	18.0	870,500	10,085.00	58,230	490,258	368,698

Source: Vodacom (T) Annual reports, International finance corporation reports and own calculations

Table 2.2: Performance of Airtel Money Mobile Banking Services in Tanzania, 2008 – 2012

Year	NO. of Airtel Money customers (Registered and unregistered) (Million)	Amount of money transferred (Tsh. Million)	Amount of money lost (Tsh. Million	Number of customers lost money through unknown theft	Number of customers lost money through entry	Number of customers left money through incorrect entry
2008 2009	4.02 5	5,845 10,768.00	6.9 11.20	9,000 8,500	12,900 65,400	6,500 7,200
2010	7.85	254,256	25.80	7,600	25,700	8,640
2011	10	365,852	38.90	15,700	33,450	8,652
2012	11.7	452,896	79.80	23,100	65,800	6,800

Source: Source Airtel (T) Annual reports, International finance corporation Annual reports and own calculations

Table 2.3: Performance of Tigo Pesa Mobile Banking Services in Tanzania, 2008 – 2012

Year	NO. of Tigo Pesa customers (Registered and unregistered)(Million)	Amount of money transferred (Tsh. Million)	Amount of money lost (Tsh. Million	Number of customers lost money through unknown theft	Number of customers lost money through entry	Number of customers left money through incorrect entry
2008 2009	1.92 2,405	4,800.80 5,200.60	10 11.00	8,000 9,600	1,500 1,700	33,500 25,400
2010	2.36	1,758.40	17.00	6,500	5,000	65,100
2011	5	2,580.80	9.00	5,700	4,000	45,600
2012	6.7	3,495.60	18.00	14,300	25,000	57,300

Source: Source Tigo (T) Annual reports, International finance corporation Annual reports and own calculations

CHAPTER THREE

3.0 LAW AND PRACTICE ON THE MOBILE BANKING IN TANZANIA

3.1 Functions of Tanzania Communications Regulatory Authority (TCRA)

The Tanzania Communications Regulatory Authority (TCRA), established by the TCRA Act No. 12 of 2003, is an independent Authority for the postal, broadcasting and electronic communications industries in the United Republic of Tanzania. It merged the former Tanzania Communications Commission and the Tanzania Broadcasting Commission. The TCRA is accountable to the Communications and Technology Ministry. The Information Communication and Technology (ICT) sector reform in Tanzania is notable in that development was influenced by regional, political (national) and technological factors.

Tanzania is one of the few African countries to liberalise the communications sector whereby the Converged Licensing Framework (CLF) is used as a key strategy, in terms of the Tanzania Communications Regulations. Since inception in 2003, the TCRA has issued a number of Regulations to administer the sector, but still faces a number of challenges such as the roll-out of services to under-serviced rural areas. The TCRA's mandate is to regulate the postal, electronic communications and broadcasting industries in the United Republic of Tanzania, which includes:

i. promotion of effective competition and economic efficiency;
ii. protecting the interests of consumers;
iii. promoting the availability of regulated services
iv. licensing and enforcing licence conditions of broadcasting, postal and Telecommunications operators;

v. establishing standards for regulated goods and services;

vi. regulating rates and charges (tariffs);

vii. managing the radio frequency spectrum;

viii. monitoring the performance of the regulated sectors; and

ix. monitoring the implementation of ICT applications,

3.2 Functions of Supervision Department of Central Bank of Tanzania (B.O.T)

3.2.1Supervisory Methodologies, Acts, Regulations and Circulars in Place

The Bank of Tanzania uses both on-site and off-site inspection in supervising banks and financial institutions.

3.2.1.1 Supervisory Methodologies

3.2.1.1.1 On-site Inspection

Full scope or targeted examination on individual banks or financial institutions. The risk management framework of the individual bank or financial institution especially Credit, Liquidity, Interest Rate, Foreign Exchange and Operational Risks are reviewed. Apart from the risk framework review of the five key components of the institutions, that is Capital adequacy, Asset quality, Management quality, Earnings capability and **L**iquidity (CAMEL) at least once a year for every institution done on site. In addition, supervisors do verify compliance with laws and regulations and assess the effectiveness of the institutions' internal control system.

3.2.1.1.2 Off-Site Inspection

In the off-site inspection assessment of financial soundness through analysis of the statistical and other returns covering key areas of the institutions is done. From the

analysis an Early Warning Report is produced. The statistical returns are submitted periodically (i.e. Daily, Weekly, Bi-weekly, monthly, quarterly, semi-annually and annually or on ad hoc basis if the circumstances so demand).

3.2.2 Supervisory According to the ACTS in Place

The Bank of Tanzania Act, 2006**,** was enacted in 2006, the Act specifies functions and objectives among others as to the regulation and supervision of banks and financial institutions in Tanzania, the Act is to provide more responsive regulatory role of the Bank of Tanzania in relation to the formulation and implementation of monetary policy; to provide for the supervision of banks and financial institutions and to provide for other related matters.

As at 31st December 2011, there were four providers of Mobile payment services name Vodacom(T) Limited (M-Pesa), Airtel(T) Limited (Airtel Money) MIC(T) Limited (Tigo Pesa) and Zantel (Ezy Pesa),during the period under review, the total value of transactions reached TZS 5,563.28 billion compare to TZS 1,002.43 billion in the previous year being an increase of 452.77%. A Significant increase in the use of mobile payment services was mainly due to consumers awareness of mobile payment services, which are more cost-effective, efficient and have wider outreach to the public, including remote/rural areas of the country,

The strong growth of mobile payment services in the country has led to the signing of the Memorandum of Understanding (MoU) on the services' joint supervision by the Bank of Tanzania (BoT) and Tanzania Communication Regulatory Authority (TCRA). BoT has, in its maiden Financial Stability Report, attributed the sharp

increase in the number of subscribers to the mobile payments mainly to limited access to formal banking services, especially in rural areas. "... in this regard, the mobile payment provides an avenue for linking bank account holders to the unbanked population," the central bank says in its 33- page report, which the bank's governor, Professor Benno Ndulu**, launched in Dar es Salaam over the weekend.**

According to provisional data, as of June 30, 2010, the number of mobile phone subscribers stood at 18.5 million, with 9.2 million of them registered for mobile payment services, mobile payment schemes involve not only funds transfers but also payment for retail goods and services, mobile payment services are specifically used to top-up mobile phone credits, airtime transfers between mobile phones and corporate bill payments - water and electricity.

For instance four mobile network operators - Vodacom, Airtel, Tigo and Zantel - are currently offering the mobile payment services. The service provision however requires that the phone companies partner with commercial banks, "the existing arrangement creates gaps in the regulatory framework because two regulators - BOT and TCRA - each with a limited scope of coverage, oversee the mobile payment services," the report says, noting that the signed MoU provides a mechanism for regulatory and supervisory coordination between the two regulators. While the central bank regulates the financial transactions, the TCRA focuses on the communication infrastructure. Industry analysts say that the significant growth in the usage of mobile phones offers great opportunity to extend financial and other services to millions of those in the unbanked community.

Security and safety of customers money in the banks is of more importance in increasing confidence of customers in the banking system. This will attract more customers to join banks by increasing their deposits, while also helping to attract new customers to join the banking business. When banking financial savings increases in the economy, more funds will be available to give as loans to other borrowers in the economy and this will in general accelerate overall economic development of the country. This security means that customers money are fully protected against theft by banks employees and also by outsiders, or by the collaboration of both bank employees and outsiders. To be effectively, this means that management of banks should effectively formulate and implement both internal and external audit programs.

In order to detect and prevents frauds of customers money that may be conducted by banks employees, outsiders or collaborations of both outsiders and banks employees. When there is poor formulations and implementations of both internal and external audit, then customers money and banks own money will be in a greater risk of being frauded by collaboration of unfaithfully employees and outsiders. Increasing frauds of customers money kept in banks will make more people to lose confidence in the both traditional banking system and mobile phone banking system causing more and more people to keep their huge amounts of money within their homes.

When a customer open accounts at mobile phone and in the traditional banking firm with the accounts operated through ATM (Automated Teller machine) he is given a password which is unique from other customers password, and uses this to open his accounts whenever wants to deposit or withdrawal money from his accounts. When

that password become access to other people, then it becomes easy for the customers money to be stolen by banks employees and also by outsiders, or by the collaboration of both bank employees and outsiders.

Since the introduction of mobile phone banking system in Tanzania in 2006, a lot of incidences involving customers money kept in mobile banking accounts operated and managed by mobile banking system, being stolen have been reported all over the country. This occurs in both types of operations namely those involved within only mobile banking system; and also from those transfers between accounts of traditional banking firms and mobile banking system accounts. At the same time more people have been questioning on the effectiveness of the Central Bank of Tanzania on protecting customers money kept in both traditional banking system and mobile phone banking system since the central bank of Tanzania, though its bank supervision departments, department of national payments system and Insurance deposits departments, exercise overall responsibilities of supervising all institutions involved in the banking business in the country.

CHAPTER FOUR

4.0 FINDINGS, INTERPRETATION OF DATA AND DISCUSSION OF DATA ANALYSIS

4.1 Introduction

This chapter tries to examine, interpret and discuss on how the mobile phone banking companies security strategies is enough to prevent frauds of customer's deposit within their companies. And also to see various procedures used on sending customers money. And also security strategies of mobile phone companies through incorrect entry done by customers.

4.2 Research Findings

From specific objective number one, which was concerned with investigation to find the effectiveness of mobile phone banking companies security strategies on preventing frauds of customer's deposits within their companies by companies employees, in Tanzania with reference to operations of Vodacom, Airtel and Tigo in Mbeya region for the year 2008-2012 period; the study found that this strategy is still more weaker since more and more customers money continue to be lost through frauds of customers money by mobile companies employees, despite the frequent conduct of the management of mobile phone companies.

From specific objective number two which was concerned with investigations to find the effectiveness of mobile phone banking companies security strategies on preventing loss of customers money through conduct of incorrect entries by customers, the study found that, mobile phone banking companies security strategies

on preventing loss of customer's money through conduct of incorrect entries by customers, with reference to operations of Vodacom, Airtel and Tigo, Mbeya region for the year 2008-2012 period; the study found this strategy is still also more weak since as shown in table s 8,9 and 10.

More customers continue to lose their money through increasing mistakes done by customers of making incorrect entry when they are sending their money to their relatives. The only strategy the companies use is the text word strategy which asks the customers to confirm, is the amount he/she sends and the name of receiver is correct, and when the customer proceeds with Ok the money is sent. But, this is only done by one reminder and not followed by word voice message, so that when it happens that the customer is in hurry, or does not pass more than once, he may send more than what he had planned or send to the wrong persons.

4.3 Data Presentation

Specific objective number one was concerned with the effectiveness of mobile phone banking companies security strategies on preventing frauds of customer's deposits within their companies by their employees, in Tanzania with reference to Mbeya region for the year 2008-2012 period. Data presentation from this specific objective is summarized in the Table 4.1.

Specifc objective number two was concerned with investigate the effectiveness of mobile phone banking companies security strategies on preventing loss of customer's money through conduct of incorrect entries by customers. Data Presentation from this specific objective is summarized in the Table 4.1.

Table 4.1: Mobile Phone Banking Companies Security Strategies on Preventing Frauds

Year	Mobile Phone Companies strategies on preventing frauds of customers deposits		
	Voda Com Strategies	Airtel Strategies	Tigo Strategies
2008	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.
2009	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.
2010	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.
2011	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.

Year	Mobile Phone Companies strategies on preventing frauds of customers deposits		
	Voda Com Strategies	Airtel Strategies	Tigo Strategies
2012	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.	Make Frequent Audit of Customers Money at the required time to ensure that the customers money is safe.

Source: Respective Mobile Phone Companies HeadQuaters Dar es Salaam

Table 4.2: Procedures of Mobile Phone Companies on Sending Customers Money

Year	Mobile Phone Companies security strategies on preventing loss of customer's money through conduct of incorrect entries by customers		
	Voda Com Procedures used on sending money by customer	Airtel Procedures used on sending money by customer	Tigo Procedures used on sending money by customer
2008	1.*150*00# press ok 2.Send money free 3.Enter phone number 4.Put the amount 5.Enter PIN number 6.Confirm by putting 1 7.give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*60#press ok 2.Send money free 3.Enter phone number 4.Amount in Tsh. 5.Send money to… 6.Yes by putting 1 7. give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*01# ok 2.Send Money 3.Send Money for Mobile 4.Enter phone number 5.Put the Amount 6.Enter PIN Number give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request

Year	Mobile Phone Companies security strategies on preventing loss of customer's money through conduct of incorrect entries by customers		
	Voda Com Procedures used on sending money by customer	Airtel Procedures used on sending money by customer	Tigo Procedures used on sending money by customer
2010	1.*150*00# press ok 2.Send money free 3.Enter phone number 4.Put the amount 5.Enter PIN number 6.Confirm by putting 1 7.give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*60#press ok 2.Send money free 3.Enter phone number 4.Amount in Tsh. 5.Send money to… 6.Yes by putting 1 7. give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*01# ok 2.Send Money 3.Send Money for Mobile 4.Enter phone number 5.Put the Amount 6.Enter PIN Number give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request
2011	1.*150*00# press ok 2.Send money free 3.Enter phone number 4.Put the amount 5.Enter PIN number 6.Confirm by putting 1 7.give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*60#press ok 2.Send money free 3.Enter phone number 4.Amount in Tsh. 5.Send money to… 6.Yes by putting 1 7. give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*01# ok 2.Send Money 3.Send Money for Mobile 4.Enter phone number 5.Put the Amount 6.Enter PIN Number give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request

Year	Mobile Phone Companies security strategies on preventing loss of customer's money through conduct of incorrect entries by customers		
	Voda Com Procedures used on sending money by customer	Airtel Procedures used on sending money by customer	Tigo Procedures used on sending money by customer
2012	1.*150*00# press ok 2.Send money free 3.Enter phone number 4.Put the amount 5.Enter PIN number 6.Confirm by putting 1 7.give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*60#press ok 2.Send money free 3.Enter phone number 4. Amount in Tsh. 5.Send money to… 6.Yes by putting 1 7. give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request	1.*150*01# ok 2.Send Money 3.Send Money for Mobile 4.Enter phone number 5.Put the Amount 6.Enter PIN Number give a password to customer 8.sign a document when a customer sends or receives money 9. give a customer money statement only when a customer request

Source: Respective Mobile Phone Companies Head Quaters Dar es Salaam.

Table 4.3: Security Strategies of Mobile Phone Companies to Prevent Loss of Customers Money through Incorrect Entry by Customers

Year	Mobile Phone Companies strategies on preventing loss of customer's money through conduct of incorrect entries by customers		
	Voda Com security strategy to prevent customers loss of money through incorrect entry	Airtel security strategy to prevent customers loss of money through incorrect entry	Tigo security strategy to prevent customers loss of money through incorrect entry
2008	1. In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver
2009	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver
2010	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer

Year	Mobile Phone Companies strategies on preventing loss of customer's money through conduct of incorrect entries by customers		
	Voda Com security strategy to prevent customers loss of money through incorrect entry	Airtel security strategy to prevent customers loss of money through incorrect entry	Tigo security strategy to prevent customers loss of money through incorrect entry
	correct. When the customer presses OK then the amount of money is sent to receiver	correct. When the customer presses OK then the amount of money is sent to receiver	to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver
2011	1. In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver, and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver
2012	.In text word, the customer is asked if the name of receiver and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver	.In text word, the customer is asked if the name of receiver and the amount of money he wants to send are correct. Then It asks the customer to press OK if he thinks that it is correct. When the customer presses OK then the amount of money is sent to receiver

Source: Respective Mobile Phone Companies Head Quaters Dar es Salaam.

4.4 Data Analysis and Discussion

This section presents that part of data analysis and presentation of the research. The information obtained from that section will enable the researcher to draw meaningful findings, conclusions and recommendations of the research, with findings presented in this chapter, while conclusions and recommendations are presented in chapter five of this research.

Table 4.4 shows that the amount of customers money kept in mobile phone banking of Airtel money lost through cyber frauds in Mbeya region increased from an amount of Tanzania Shillings 1,807 million in the year 2008 to Tanzania Shillings 1,880,000 Million in the year 2012. The number of customers also whose money have been lost while in the mobile phone banking system of Airtel mobile phone company also increased from 17,600 in the year 2008 to 20,300 in the year 2012.

Table 4.4: Money Lost from Airtel Money in Mbeya Region

Year	NO. of Airtel Money customers in Mbeya Region(Registered and unregistered)	Amount of money transferred (Tsh. Million)	Amount of money lost (Tsh. Million	Number of customers lost money through unknown theft	Number of customers lost money through entry by Employees of the company	Number of customers left money through customers incorrect entry
2008	40,000	1,507	300	2,500	5,400	9,700
2009	50,000	2,761	450	1,900	5,500	7,300
2010	70,000	53,847	575	1,800	6,700	5,200
2011	90,000	85,646	685	3,200	8,200	6,700
2012	100,000	95,755	880	4,600	7,600	8,100

Source: Respective Mobile Phone Companies Head Quarters Dar es Salaam.

Table 4.5: Money Lost from Tigo Pesa in Mbeya Region

Year	NO. of TIGO PESA Money customers in Mbeya Region (Registered and unregistered)	Amount of money transferred (Tsh. Million) in Mbeya Region	Amount of money lost (Tsh. Million) in Mbeya region	Number of customers lost money through unknown theft in Mbeya Region	Number of customers lost money through entry by Companies Employees in Mbeya Region	Number of customers left money through customers incorrect entry in Mbeya Region
2008	390,000	647	1.17	974	1,800	1,200
2009	460,000	978	1.90	985	4,100	900
2010	570,000	1,354	4.39	1,500	2,300	600
2011	60,000	1,674	6.61	2,300	2,200	1,100
2012	730,000	3,800	13.57	3,100	3,100	1,400

Source: Respective Mobile Phone Companies Head Quaters Dar es Salaam.

Table 4.6: Money Lost from M-Pesa in Mbeya Region

YeaR	NO. of M-pesa customers in Mbeya Region(Registered and unregistered)(Million)	Amount of money transferred (Tsh. Million)	Amount of money lost (Tsh. Million	Number of customers lost money through unknown theft	Number of customers lost money through entry by Employees of the company	Number of customers left money through customers incorrect entry
2008	0.04	1,507	300	2,500	5,400	9,700
2009	0.05	2,761	450.00	1,900	5,500	7,300
2010	0.07	53,847	575.00	1,800	6,700	5,200
2011	0.09	85,646	685.00	3,200	8,200	6,700
2012	0.1	95,755	880.00	4,600	7,600	8,100

Source: Respective Mobile Phone Companies HeadQuaters Dar es Salaam

Table 4.5 shows that the amount of customers money kept in mobile phone banking of Tigo money lost through cyber frauds in Mbeya region increased from an amount of Tanzania Shillings 648.17 million in the year 2008 to Tanzania Shillings

13,813.57 Million in the year 2012. The number of customers also whose money have been lost while in the mobile phone banking system of Airtel mobile phone company also increased from 3,978 in the year 2008 to 7,600 in the year 2012.

Table 4.6 shows that the amount of customers money kept in mobile phone banking of M-pesa money lost through cyber frauds in Mbeya Region increased from an amount of Tanzania Shillings 1,807 million in the year 2008 to Tanzania Shillings 96,635 Million in the year 2012. The number of customers also whose money have been lost while in the mobile phone banking system of Airtel mobile phone company also increased from 17,600 in the year 2008 to 20,300 in the year 2012

Table 4.7: Total Amount of Money Lost from three Mobile Companies Tigo, Airtel Money

Yea	NO. of M-pesa customers in Mbeya Region(Registered and unregistered)(Tsh.Million)	Amount of money transferred (Tsh. Million)	Amount of money lost (Tsh. Million	Number of customers lost money through unknown theft	Number of customers lost money through entry by Employees of the company	Number of customers left money through customers incorrect entry
2008	610,000	2,428.0	350.5	6,041	10,600	15,500
2009	760,000	4,241.0	547.3	6,073	15,400	15,500
2010	1,010,000	67,167.0	830.7	8,614	15,900	11,000
2011	610,000	102,892.0	1,031.1	13,821	18,600	15,200
2012	1,360,000	116,965.0	1,311.4	17,599	20,800	18,800

Source: Respective Mobile Phone Companies Head Quaters Dar es Salaam.

From Table 4.7, shows the number of customers who have lost their money through the network of mobile phone banking system , from the sampled, three mobile phone companies in Mbeya region namely, Airtel , Tigo and Vodacom in Mbeya region have been increasing since the year 2008. Total number of customers from three mobile phone companies surveyed namely Vodacom, Airtel and Tigo who lost their money increased from 6,041 in the year 2008, to 6,073, 8,614, 13,821 and 17, 599 in the respective years 2009, 2010, 2011 and 2012**.** Likewise, the amount of customer money lost from the three mobile phone companies increased from shillings 350.5 million in 2008, to shillings 547.3,million, shillings 830.7 million, shillings 1031.1 million and shillings 1311.4 million in the respective years of 2009, 2010, 2011 and 2012.

To investigate the effectiveness of mobile phone banking companies security strategies on preventing loss of customer's money through conduct of incorrect entries by customers.

To suggest solutions that will make mobile phone companies to formulate and implement effective security strategies that will ensure maximum safety of customers money deposited /transacted through their financial network

From Table 4.8, while the total number of promotion campaign carried on by the mobile phone companies in Mbeya region has been increased from the year 2007, the only campaign that the mobile phone companies have been doing are those that are concerned with promotion and marketing of their products and services for the purpose of convicting customers to buy them. But since the year 2007, there have

been no any education campaign done by any mobile phone baking company to educated their customers and the general public on how to protect their money accounts within the network of mobile phone banking system to protect their money from being stolen by criminals involved employees of the mobile phone banking companies and outsiders criminals.

Table 4.8: Security Education Programmes Carried by Mobile Phone Banking

Year	Education campaign on Security of Customers Money Kept in Mobile Phone Banking System	Education campaign on Promotion of Mobile Companies Products and Services	Total Number of Promotion Campaigns
2007	0	258	258
2008	0	456	456
2009	0	625	625
2010	0	587	587
2011	0	865	865
2012	0	5642	5642
By June 2013	0	7354	7354

Source: Vodacom, Airtel and Tigo Mobile Phone Companies in Mbeya Region.

4.5 Respondents Views Based on Research Hypothesis

The first research question asked the respondents to give their views on the effectiveness of mobile phone banking companies security strategies on preventing frauds of customers deposits within their companies in Tanzania. The respondents views on this research question is summarized in the Table 4.9.

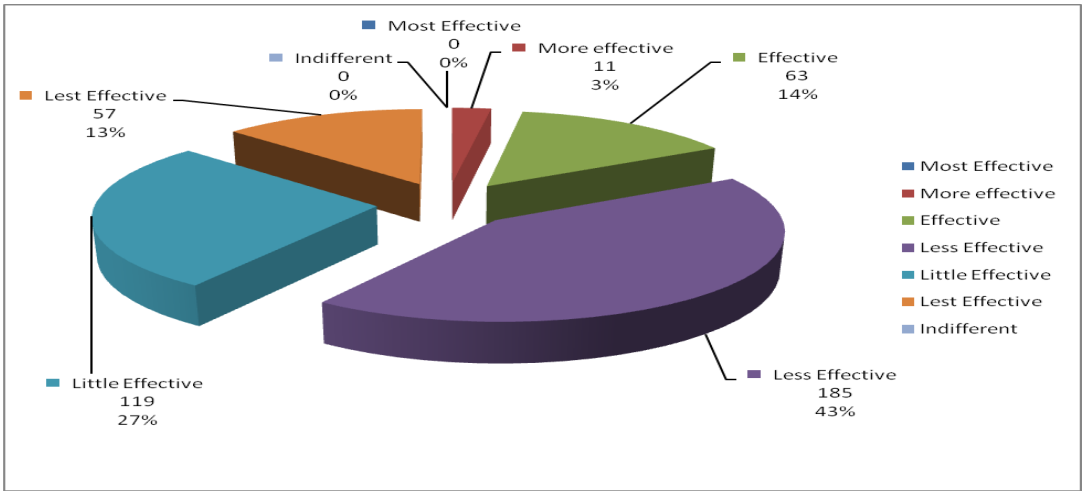

Figure 4.1: Respondents Views on the effectiveness of mobile phone banking

Source: From field research, 2012

Table 4.9: Respondents Views on the effectiveness of mobile phone banking

		Most Effective	**More effective**	**Effective**	**Less Effective**	**Little Effective**	**Less Effective**	**Indifferent**
Mobile Phone Customers experienced loss of Money kept in Mobile Phone Bank Accounts	150	0	0	20	60	50	20	0
Mobile Phone Customers who have not experienced loss of Money kept in Mobile Phone Bank Accounts	200	0	0	20	90	60	30	0
Employees of the Bank	10	0	0	4	3	2	1	0
Employees of Mobile Phone Company in Mbeya City	20	0	6	7	4	3	0	0
Police officers in Mbeya City	50	0	5	12	25	3	5	0
Magistrate in Mbeya High Court	5	0	0	0	3	1	1	0
Total	**435**	**0**	**11**	**63**	**185**	**119**	**57**	**0**
Percentage	**100**	**0.00**	**2.53**	**14.48**	**42.53**	**27.36**	**13.10**	**0.00**

Source: From field research, 2012

From Table 4.9, 0 percent of the respondents said that mobile phone companies strategies on preventing frauds of their customers money stored in their accounts are most effective. 2.53 percent said that they are more effective. 14.48 percent said that they are effective. 27.36 percent said that they re little effective. 13.10 percent said that they are least effective and 0.00 percent said that they were indifferent.

The second research question asked the Respondents to give their views on the effectiveness of mobile phone banking companies security strategies on preventing loss of customers money through conduct of incorrect entries by customers. The respondents views on this research question is summarized in the Table 4.10.

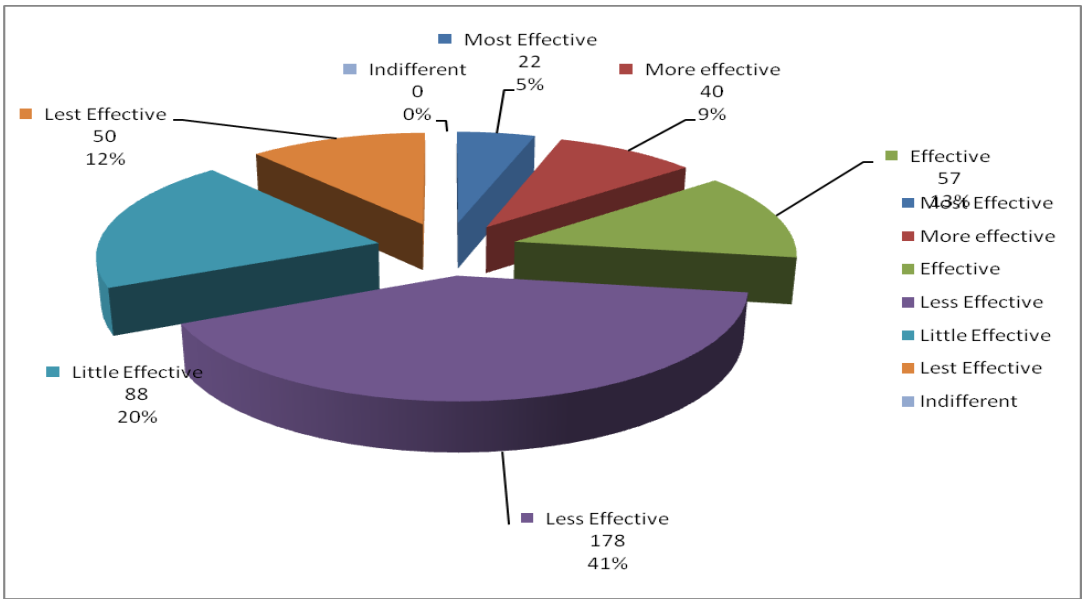

Figure 4.2: Respondents of Mobile Phone Banking Companies

From Table 4.10, 5 percent of the respondents said that mobile phone companies strategies on on preventing loss of customers money through conduct of incorrect entries by customers. are most effective. 9.20percent said that they are more effective. 13.10 percent said that they are effective. 40.92 percent said that they re

little effective. 11.49 percent said that they are least effective and 0.00 percent said that they were indifferent

The Third research Question asked the Respondents to give their views on the solutions that will make mobile phone companies to formulate and implement effective security strategies that will ensure maximum safety of customers money deposited and transacted through their financial network. The results from this research question are summarized in the Table 4.11.

Table 4.10: Respondents on the Effectiveness of Mobile Phone Banking

Type of Respondents	Sample	Respondents Views						
		Most Effective	More effective	Effective	Less Effective	Little Effective	Lest Effective	Indifferent
Mobile Phone Customers experienced loss of Money kept in Mobile Phone Bank Accounts	150	10	30	30	30	30	20	0
Mobile Phone Customers who have not experienced loss of Money kept in Mobile Phone Bank Accounts	200	0	0	20	110	50	20	0
Employees of the Bank	10	1	1	2	3	2	1	0
Employees of Mobile Phone Company in Mbeya City	20	5	5	3	3	3	1	0
Police officers in Mbeya City	50	6	3	1	30	3	7	0
Magistrate in Mbeya High Court	5	0	1	1	2	0	1	0
Total	**435**	**22**	**40**	**57**	**178**	**88**	**50**	**0**
Percentage	**100**	**5.06**	**9.20**	**13.1**	**40.92**	**20.23**	**11.49**	**0.00**

Source: Field Research, 2013

Table 4.11lutions to Protect Customer's Money

Type of Respondents	sample	Respondents Views						
		Legal Measures should be taken against mobile Phone Companies	Tough Legal measures against offenders including Mobile Phone Companies	Review penalties given to offenders	Mobile Phone Companies Conduct frequent face to face public awareness campaign	TCRA Should effectively intervene	Bank of Tanzania , Mobile Phone companies and commercial banks Should collaborate	All of the Mentioned answers
Mobile Phone Customers experienced loss of Money kept in Mobile Phone Bank Accounts	150	10	20	30	30	30	20	10
Mobile Phone Customers who have not experienced loss of Money kept in Mobile Phone Bank Accounts	200	20	10	50	70	30	10	10
Employees of the Bank	10	1	1	2	2	2	1	1
Employees of Mobile Phone Company in Mbeya City	20	4	3	3	3	3	1	3
Police officers in Mbeya City	50	4	2	1	30	3	7	3
Magistrate in Mbeya High Court	5	0	1	1	1	0	1	1
Total	435	39	37	87	136	68	40	28
Percentage	100	8.97	8.51	20.00	31.26	15.63	9.20	6.44

Source: Phone Banking

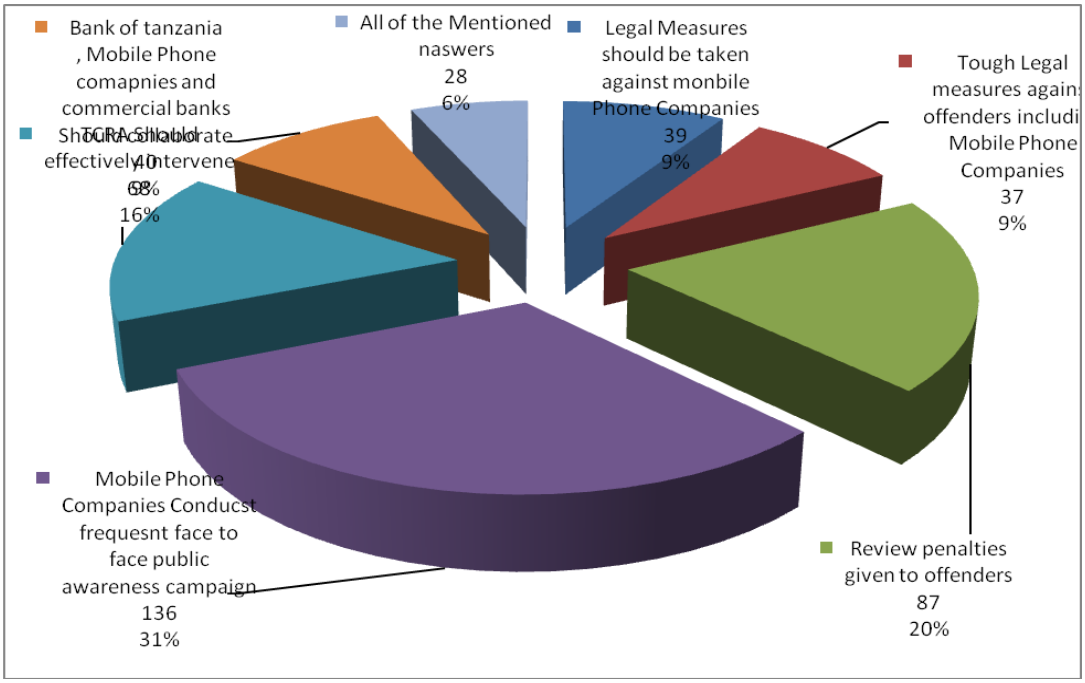

Figure.4.3: Solutions to Protect Customers Money Stored in the Accounts of Mobile System in Mbeya Region of Tanzania

Source: From research field, 2012

From Table 4.11, 8.97 percent of the respondents said Legal Measures should be taken against mobile Phone Companies, 8.51 percent said that Tough Legal measures against offenders including Mobile Phone Companies.. 20.00 percent said that there should be a review on Review penalties given to offenders. 31.26 percent said that 15.63 percent said that TCRA Should effectively intervene 9.20 Percent said that Bank of Tanzania , Mobile Phone companies and commercial banks Should collaborate and 6.44 percent said that All of the Mentioned answers should bee effectively implemented.

CHAPTER FIVE

5.0CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

Due to the development of technology, mobile phone banking system has become a bigger network of conducting financial services, in both rural and urban areas, than the traditional fixed premises banking system. Thus the issue of security for customer money kept within the network of ,mobile phone banking system has become of more importance to both policy makers, mobile firms operating banking services to the general public, the financial regulators such as the Central Banks, Communication Authorities and legal officers such as the police forces, investigators and courts system. This has made governments all over the world including Tanzania to start to make research on how to protect customer's money kept in the network of mobile phone banking system. This chapter presents Conclusions and Recommendations of the study, Section 5.2 Presents Conclusion of the Study. Section 5.3 Presents Recommendations of this research.

5.2 Conclusion

Increasing formulations of poor strategies of safety within mobile phone banking companies in Tanzania have resulted into increasing number of customers who lose their money and also increasing the amount of money lost, through frauds by untrustworthy mobile phone companies, and incorrect entry made by customers during the exercise of sending money inside and outside Tanzania. Hence immediate measures should be undertaken to solve this problem in order to reduce loss of customer's money through a network of mobile phone banking system in Tanzania.

Since increasing loss of amount of money of customers in the network of mobile phone banking system causes a big financial loss to customers and in most cases increases poverty through reducing monetary income of customers who have lost their money through the network of mobile phone banking system.

5.3 Recommendations

The recommendations of this study are modeled according to specific objectives and findings of this study. Accordingly, this study recommends that in order to reduce loss of customer's money who use a network of mobile phone banking system in Tanzania, the following should be done:

From specific objective number one and Findings number one, the following are recommended:

(i) The mobile phone companies should make sure that employees who are employed in the mobile phone banking sections are very trustful.

(ii) Frequent internal and external Audit Check should be conducted by mobile phone management in order to make sure that they discover any kind of frauds which may be in the process to be done by unfaithful employees who steal their customer's money.

(iii) Heavy legal punishments should be taken against employees who steal customers money

(iv) The management of mobile phone companies should establish process of sending weekly statements about financial positions of their customers so that the customers may be in good conditions to discover early if their money have been stolen.

(v) The Central Bank of Tanzania as the major regulator of all banking activities in the country, should establish strong measures which will lead to reduction of amount of customers money that is lost through a network of mobile banking system.

(vi) The Tanzania Communication Regulatory Authority (TCRA) as a regulator in the Communications sector should establish strong measures which will lead to reduction of amount of customer's money that is lost through a network of mobile banking system.

From specific objective number two and Findings number two, the following are recommended;

i. The companies should establish the system whereby the customer is reminded at least three times in order to enable the customer avoid sending money to wrong person or send more money unnecessary than whether was planning to send.

ii. The companies should establish the system whereby the customer is reminded with two approaches namely text words and word voices about the amount he is sending and the person to whom he is sending money.

iii. The Government should establish strong legal system dealing with frauds in the mobile phone banking system.

iv. Mobile phone banking firms should constantly carry on security promotions for the public in order to enable more public to understand well on how to protect their money against frauds.

v. Mobile phone companies should make sure that they employ well qualified

and innocent employees who do not collude with criminals to steal customers money

vi. The Government in collaboration with the Central Bank of Tanzania and Tanzania Communication Regulatory Authority and the Police force should jointly collaborate with the mobile firms companies that operate mobile banking system in order to identify the network involved in the theft of customers money kept in mobile phone banking firms, and thus be in a good position to design measures to stop them items, hence helping the public to prevent their money from being stolen by these criminals involved in stealing customers money kept in the network of mobile phone banking system.

vii. The customers who keep their money in the network of mobile phone banking system should also take additional precautionary measures which will ensure that their sensitive information on their accounts within the mobile phone banking system are not revealed to any other unwanted persons in order to help their accounts be more safe from their money being stolen by criminals involved in the network of cyber frauds within the network of mobile phone banking system.

viii. The mobile phone banking firms should also collaborate with the traditional banking firms in order to find on how they can protect well the customer money kept in the network of mobile phone banking firms.

ix. It is time now to introduce a broad electronic Communications legislation to protect individuals and customer's money in mobile-banking operations against threats posed by modern information practices. For example in Tanzania, there is Tanzania Communications Regulatory Authority Act, No.

12 of 2003, and the Electronic and Postal Communications Act, no. 3 of 2010, whereby, all of these Acts, were not drafted in a sustainable way, as it can be seen that there is no provisions which provides for mobile banking services. The Bank of Tanzania (B.O.T) and the Tanzania Communications Regulatory Authority (T.C.R.A) must come together and discuss to advice the government on the need to draft such legislation.

x. An effective legal framework must be put in place in order to protect consumers who are depositing a lot of money in the SIM card. The effective law is that which will addresses the problems concern.

xi. Based on lessons drawn from various countries like in the United Kingdom (U.K), United States of America (U.S.A) and other countries in the European Union, and in view of the existing uncertainties on current laws and regulations, the government in Tanzania should enact a broad and general purpose piece of legislation to give legal recognition to M-Pesa, Tigo Pesa and Airtel Money transactions generally. Again, lessons may be drawn from other jurisdictions in order to have the best legal framework for mobile-banking.

xii. On top of having a general legislation on those transactions in mobile Banking, it is recommended that specific piece of legislation should be enacted to cover specific areas or aspects like mobile Banking in M-Pesa, Tigo-Pesa and Airtel-Money in Tanzania in order to protect consumer in this area. For example is like in Malaysia where there is Malaysia EFT Act, and India where there is Indian Information Technology Act, of 2000, which provides a clear guidance. Again in the United States of America (U.S.A),

there is EFT Act, 1978, this is a consumer protection in the electronic fund transfers system oriented law in U.S.A. EFT Act establishes the rights, liabilities and responsibilities of the electronic fund transfer participants. Therefore basing in this form, this should form the basis for enactment of a specific piece of legislation on Mobile Banking in Tanzania.

xiii. A piece of legislation that provides for effective and appropriate resolution of M-Pesa, Tigo-Pesa and Airtel-Money disputes will increase confidence and trust. Thus, if consumers are confident enough on resolution of such disputes, it means any dispute that arises will be resolved effectively and efficiently, here consumers will increase confidence in using mobile-banking transactions mechanism in Tanzania.

REFERENCE

Abdoul. R.B, et al, (2011), "*Examine the Customers Attitude to Mobile Banking Based on Extended Theory of Planned Behavior, (A case study in EN Bank in Iran"*. International Bulletin of Business Administration. ISSN: 1451-243X Issue 10 (2011). http://www.scribd.com>research>business&Economics. Retrieved on 2nd.June, 2013.

Adrian. D. N, (2007), "*Mobile phone banking: Usage experiences in Kenya*", Catholic University of East Africa, Nairobi.http://www.w3.org/2008/10/mw4D-ws/papers/njenga.pdf. Retrieved on 7th. June, 2013.

Akindele R.I. (2011), "Fraud *as a Negative Catalyst in the Nigerian Banking Industry",* Journal l of Emerging Trends in Economics and Management Sciences (JETEMS) 2 (5): 357-36 http://www.jetems.scholarlinkresearch.org/…/fraud%20a%20Negative%cat. pdf. Retrieved on 23rd.June, 2013.

Carnell, R. S, (2011), "*Law of Banking & Financial Institutions*", 2011 Statutory Supplement: Aspen Publishers. London

Carnell, R.S. et al, (2008), "*The Law of Banking and Financial Institutions",* Aspen Publishers, Inc. London

Central Bank of Tanzania (2013), "*Central Bank of Tanzania Annual Reports*". Central Bank of Tanzania (2013), "*Central Bank of Tanzania Fraud Prevention Unit Report, 2012*".http://www.bot-

tz.org/Bankingsupervision/Report/DBS ANNUAL- Report 2011.pdf. Retrieved on 15th. July, 2013.

Gautam, I and Mark, P, (2006), *Mobile Phone Banking and low- Income Customers*: Evidence from south Africa, the world Bank washingtone Dc.http://www.cgap.org/…/CGAP-mobile-phone-banking-and-law-income-customers.pdf. Retrieved on 26th.June,2013

http://www.balancingact-africa.com/…/bank-of-tanzania…/e…Retrieved on 20th.June, 2013.

http://www.bot-tz.org/Bankingsupervision/Report/DBS ANNUAL- Report 2011.pdf. Retrieved on 10th.July, 2013.

http://www.businessdictionary.com/definition/mobile-phone.htm. Retrieved on 10th.June, 2013.

http://www.duhaime.org/legaldictionary/b/bank.aspx. Retrieved on 26th.May, 2013.

http://www.google.co.tz/search?q=memorandum of understanding between B.O.T and TCRA. Retrieved on 12th.May, 2013.

http://www.investinganswers.com/financial-dictionary/personal-finance/mobile-phone-banking-20611. Retrieved on 12th.july, 2013.

Kruger, P.J.H (2011), " *Cellphone banking at the bottom of the pyramid*": A Thesis presented in partial fulfillment of the requirements for the degree of Master of Science at the university of Stellenbosch: South Africa. http.www.scholar.sun.ac.za./btstream/handle/10019…/kruger-cellphone-2012.pdf? Retrieved on 15th.May, 2013.

Pavan, D, (2013), " *Mobile Banking & Mobile Law*", Saakshar Law Publications, Edition 2013 edition.New Delhi.

Pednault, S (2009), " *Fraud 101: Techniques and Strategies for Understanding Fraud*", Wiley-New York. http://www.wiley.com….>accounting>special Topics. Retrieved on 10th.June, 2013.

Porteous, D, (2006), "The Enabling Environment for mobile Banking in Africa", London, http:// www. Bankable frontier.com/assets/ee.mobile .banking. report. v3.1.pdf.Retrieved on 25th.May, 2013.

Sackers, A and wells, J.D, (2003), "*Understanding Frauds in mobile Phone Banking System*, LAP LAMBERT Academic Publishing, London .

Samuel.M.et al, (2010), "*Facilitating Cross-Boarder Mobile Banking in Southern Africa*", The World Bank, Washington DC.

Summers, R.S and James, J. W, (2008), "*Principles of Payment Systems (Concise Hornbook)* , West; London.

Tanzania Communication Regulatory authority (2013), "*Tanzania Communication Regulatory authority Annual Reports",* http://.www.tcra.go.tz/index.php/about-tcra/tcra-profile.Retrieved on 8th.May, 2013.

Victoria, Y. P (2011), " *Mobile Banking Security Services: E-Mobile Banking*", LAP LAMBERT Academic Publishing, London.

APPENDICES

Appendix i: Questionnaire to customers of Mobile phone Banking

i.) Introduction

This questionnaire aims at investigating the effectiveness of security strategies on promoting safetyness of customers money, deposited and transacted through a network of mobile banking system. You have been identified as a potential data provider and hereby requested to supply data by filling in the questions below.

ii.) Personal Information.

Name……..Age…….Occupation…….

Name of banks used……..

Name of mobile phone company getting bank……..

Service……

Date…….

iii) Research questions

i) How long have you been using mobile phone banking services?

(a) one year (b) Two years (c) Three years (d) Four years ( )

(e)More than Four years.

ii) How much amount of money you frequent per year deposit with your mobile bank system?

a) 0-100.000/= Tshs. (b) 101,000-200,000=Tsh.

(c) 201,000-300,000=Tsh. (d) More than 300,000=Tsh. ( )

iii) Have you experienced any problem with regard to your money deposited/ send /received by you through a net work of mobile phone banking system?

(a) Yes b) No ( )

iv) If the answer in the question (iii) above is Yes, explain……

……

v) How frequently (on average) per year have you experience a loss of your money through a network of mobile phone banking services you use?

(a) Once (b) Two times (c) three times

(d) Four times (e)more than four times ( )

vi) Have you ever reported this problem to management of your mobile company?

(a) Yes (b) No. ( )

vii) After reporting the event what actions did the management of Mobile Phone Company took?

.....

.....

viii) Suggest solutions that will improve more safetyness of customers money deposited

Within mobile phone banking systems…….

……

……

ix) Provide other information that are useful to this research……

…….....

Thank you for your cooperation

Appendix ii: Questionnaire to employees of mobile Phone Company in Mbeya Region-Tanzania.

(i) Introduction

This questionnaire aims at collecting primary data in order to enable the researcher complete his academic research which intends to final how mobile phone company have established security measures of their customers money , you are requested to assist him by filling /answering in the questions below:

(ii) Personal Details

Name…….. Name of company…….

Title ……. Date……..Tel……..Fax….....

E-mail……

iii) Research Questions.

(i)For how long has your company offering mobile phone banking services in Mbeya Region

(a) one year (b) Two years (c) Three years (d) More than three years ( )

(ii) Mentioned types of banking services offered to your customers by your mobile banking;

(a)…….

(b)…….....

(c)……

(d)……

(e)……

(iv). Provide the number of your customers using mobile phone banking services in Mbeya region since you start your business, giving in each year number of Customers against amount of money deposited sent received or withdrawn.

(v). Has your customers brought to you any complaints about facing insecurity with regards to the amount of money they transact through your network of mobile Phone banking?

a) Yes (b) No ( )

(vi).If yes, explain the type of complaints and the nature of their causes……..……

……..……..

(vii). For how many times in a year does your office receive such Complaints…… ……..

(viii). Explain measures that have been taken by your company to solve the indicated Problems in order to ensure maximum security of customers……

……..

……

(viii) Provide other information that are useful to this study……

Thank you for your Cooperation.