ENHANCING INFORMATION SYSTEM SECURITY IN MOBILE PHONE BANKING SERVICES IN KENYA

By:
Alex Musumbi Wambua

A Research Project in Partial Fulfillment of the Requirements for the Post Graduate Diploma in Project Planning and Management

UNIVERSITY OF NAIROBI

JUNE, 2012

DECLARATION

This Research project is my original work and has not been presented for a Post graduate Diploma or any other publication in any other University.

Name: ALEX MUSUMBI WAMBUA Date 26/06/2012

Signature: .....

L42/60014/2007

This Research Project has been submitted for examination with our approval as University Supervisor.

Mr. Bwibo Date 19/07/2012

Department (Extra Mural Studies, University of Nairobi)

Signature: .....

ACKNOWLEDGEMENT

First, I am grateful to God first for the strength, time and good health he gave me to be able to research and write this paper. Secondly, I am grateful to my colleagues, University of Nairobi Postgraduate Diploma (2007) students for their dedicated time in assisting in identifying current researchable areas. Finally, I am grateful to Mr. Bwibo my supervisor for having provided guidelines in order for me to choose this topic.

TABLE OF CONTENTS

DECLARATION i

ACKNOWLEDGEMENT ii

ABSTRACT vi

LIST OF ABBREVIATIONS vii

DEFINITION OF TECHNICAL TERMS viii

LIST OF TABLES x

LIST OF FIGURES xii

CHAPTER ONE 1

1.0 INTRODUCTION 1

1.1 Background of the study 1

1.2 Statement of the problem 3

1.3 Research objectives 4

1.3.1 General objective 4

1.3.2 Specific objectives 4

1.4 Research questions 4

1.5 Significance of the study 4

1.6 Justification of the study 5

1.7 Scope of the study 6

1.8 Limitation of the study 6

CHAPTER TWO 7

2.0 LITERATURE REVIEW 7

2.1 Introduction 7

2.2 History of mobile phone banking 7

2.3 Banking system in Kenya 8

2.4 Mobile phone banking in Kenya 9

2.5 Benefits of mobile phone banking services 10

2.6 Theoretical framework 11

2.6.1 Snooping 12

2.6.2 Phishing 13

2.6.3 Smishing 13
2.6.4 Man-in-the-middle 13
2.6.5 Unencrypted sensitive client-side data on carrier networks 14
2.6.6 Money Launderers 14
2.6.7 Client-Side solutions 15
2.6.8 Password keychains 15
2.6.9 Individual bank security models or risk of preloaded software 16
2.7 Previous studies on mobile phone banking 18
2.7.1 Adoption of mobile phone banking 18
2.7.2 Current existing information systems security 18
2.7.3 Customer awareness & perception 20
2.7.4 Mobile phone technology 20
2.7.5 Derive additional information system security 22
2.8 Research gaps to be filled by the study 23
2.8.1 Enhancement of information system security 23
2.9 Conceptual framework 24

CHAPTER THREE 25
3.0 METHODOLOGY 25

3.1 Research design 25
3.2 The target population 25
3.3 Sample size and sampling procedure 25
3.4 Data types and data collection techniques 26
3.5 Data analysis 27

CHAPTER FOUR 28
4.0 DATA ANALYSIS, FINDINGS AND PRESENTATION 28

4.1 Introduction 28
4.2 Baseline Information of the Study 28
4.2.1 Socio demographic characteristics of study participants (Customers) 28
4.2.2 Use of mobile phone banking services 29

4.2.3 Number of years using mobile phone banking services 30
4.3 Current information systems security in mobile phone banking 31
4.3.1 Adequacy on the use of mobile phone banking services 32
4.3.2 Efficiency on the use of mobile phone banking services 33
4.3.3 Efficiency of the existing mobile phone banking system security 34
4.3.4 Level of satisfaction on the use of mobile phone banking services....35
4.4 Baseline information on mobile phone banking technologies 36
4.4.1 Mobile Data technology 37
4.4.2 Level of satisfaction on the use of mobile phone data technology 37
4.5 Challenges of using mobile phone banking 38
4.6 Enhanced information system security for mobile phone banking 39
4.6.1 Benefits of using enhanced information system security 40

CHAPTER FIVE 41
5.0 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 41
5.1 Introduction 41
5.2 Conclusions 41
5.2.1 Background and demographic characteristics of respondents 41
5.2.2 Current information system securities in mobile phone banking 42
5.2.3 Baseline information on mobile phone banking technologies (Mobile Data) ..42
5.2.4 Enhanced information system security for mobile phone banking 42
5.3 Recommendations 43

REFERENCES 45

Appendix 1: Letter of Introduction to the Bank 48
Questionaire for Bank Customers 48
Appendix 111: List of all commercial banks in Kenya 56
Appendix 1V: Research budget 54
Appendix V: Time schedule 55

ABSTRACT

The mobile phone banking services in Kenya is a relatively new concept in the banking sector and it has the potential to drive banks' success. The introduction of this concept by some commercial banks was aimed at taking advantage of the increased number of mobile phone subscribers. Generally, out of 24,968,891 Kenyans having access to a mobile phone (CCK, 2010), only approximately 9.66 million have bank accounts. Other reasons driving banks to adopt this concept is to increase competitiveness, efficiency and speed in provision of financial services to the banks' customers for both personal and retail banking and offer them a 24 hours and 7 days a week accessibility to their bank accounts.

The purpose of the research study was to enhance information system security in the mobile phone banking services in Kenya with the view of evaluating the current information system security and the mobile phone technologies available in Kenya.

The research adopted the descriptive approach. Questionnaires were used as the main instrument for data collection. Data collected was analyzed using descriptive statistics in form of percentages and frequency distribution tables with the help of SPSS (statistical package for social science) program. Histogram and bar graphs were used to present the data.

The expected outcome of the research study was to derive additional information system security measures that will enhance secure provision of mobile phone banking services in Kenya.

LIST OF ABBREVIATIONS

ATM	-	Automated Teller Machine
CBK	-	Central Bank of Kenya
CCK	-	Communication Commission of Kenya
CDMA	-	Code Division Multiple Access
CRAM	-	Challenge Response Authentication Mechanism
EDGE	-	Enhanced Data rates for GSM Evolution
GPRS	-	General Packet Radio Service
GSM	-	Global System for Mobile
ICT	-	Information and Communication Technology
ITU	-	International Telecommunications Union
PC	-	Personal Computer
PIN	-	Personal Identification Number
POS	-	Point of Sale
SMS	-	Short Messaging Services
SPNP	-	Service Provider Number Portability
WAP	-	Wireless Application Protocol

DEFINITION OF TECHNICAL TERMS

ATM-An unattended electronic machine in a public place, connected to a data system and related equipment and activated by a bank customer to obtain cash withdraws and other banking services.

CDMA- refers to any of several protocols used in so-called second-generation (2G) and third-generation (3G) of wireless communication that allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth.

Diffusion of innovation- refers to rate at which new ideas and technology spread through cultures.

EDGE- is a backward-compatible digital mobile phone technology that allows improved data transmission rates, as an extension on top of standard GSM

GPRS - It is used for various data applications on phones, including wireless Internet (WAP), MMS, and software that connect to the Internet.

GSM – It is a digital mobile telephone system that is widely used in today's world.

Mobile phone banking (also known as SMS Banking)- is a term used for performing balance checks, account transactions, payments etc. via a mobile device such as a mobile phones.

PIN- The secret code which is used to identify the account holder after inserting the card.

POS - Term normally used to describes an automated system which networks to a database of information. Usually via a scanned barcode, the information from the sale of an item is recorded and denotes what product was sold, where it was sold and how many are left in the stock of items.

SPNP - It is a telecommunications network feature that enables consumers to retain their telephone numbers whenever they decide to change their service providers or service types

WAP- is an open international standard for application layer network communications in a wireless communication environment. Its main use is to enable access to the Internet (HTTP) from a mobile phone or PDA.

LIST OF TABLES

Table 2.9: Conceptual Framework 2010: Enhancing Information System Security in Mobile phone Banking Services. 24

Table 4.2.1 Distribution of the respondents in terms of gender and educational level..... 29

Table 4.2.2: distribution of the respondents in terms of gender and use of mobile phone banking services 30

Table 4.3.3: Distribution of the respondents in terms of number of years using the service..... 31

Table 4.3: Distribution of respondents based on the implemented information sytem security by their respective banks 32

Table 4.3.1: Distribution of respondents based on the adequacy use of mobile phone banking sevices 32

Table 4.3.2: Distribution of respondents based on efficiency on the use of mobile phone banking services 33

Table 4.3.3: Distribution of respondents based on efficiency on the existing mobile phone banking information system securities 34

Table 4.3.4: Distribution of respondents based on the level of satisfaction on the use of mobile phone banking services 35

Table 4.4: Distribution of respondents based on transactions conducted at each banking channel 36

Table 4.4.1: Distribution of mobile phone data technologies used in mobile phone banking 37

Table 4.4.2: Distribution of respondents based on the level of satisfaction on the use of mobile phone data 38

Table 4.5: Distribution of respondents based on the challenges of using mobile phone39

Table 4.6: Distribution of respondents based on the information system security implemented in future 39

Table 4.6.1: Distribution of respondents based on benefits derived from enhanced information system securities 40

LIST OF FIGURES

Figure 4.2.1: Percentage distribution of respondents based on their gender and level of education 29

Figure 4.2.2: Percentage distribution of respondents based on their gender and use of mobile phone services 30

Figure 4.2.3: Percentage distribution of respondents based on number of years using the service 31

Figure 4.3.1: Percentage distribution of respondents based on the adequacy use of mobile phone banking sevices 33

Figure 4.3.3: Percentage distribution of respondents based on efficiency of existing mobile phone banking system security 34

Figure 4.3.4: Percentage distribution of respondents based on the level of satisfaction on the use of mobile phone banking services 35

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the study

Over the last few years, the mobile industry has been one of the fastest growing markets in the world and it is still growing at a rapid pace. According to Touré (2010), the number of mobile cellular subscribers worldwide had reached 5 billion mark by the end of 2010. Banks are exploiting the vast market of mobile phone subscribers as a competitive advantage for both personal and retail banking to offer 24 hours , 7 days a week accessibility to their customers. Furthermore, the advent of the mobile phones has revolutionized the way the financial services industry conducts business. It has empowered such institutions with new business models. For instance, new ways to offer 24 hours, 7 days a week accessibility to their customers through the use of customer mobile phone handset. The new business model offers real-time financial transactions, attracting and retaining future customers as there are now able to offer services that would have otherwise needed the full presence of the customers or bank custodian or representative through innovations in the mobile phone technology.

Mohr (2001) asserts that, the newly emerged mobile phone banking services represent an innovation where both intangible services and an innovative medium of service delivery employing high technology are present. Thus, the concept of innovation is even more intricate as technology and service aspects have an effect on the characteristics of mobile phone banking services.

Despite the adoption of this new business model in the banking industry, information system security in bank accounts authentication is a major concern in the provision of an effective mobile phone banking services. Currently, this new banking concept relies on

PIN authentication, updating customers by sending unencrypted SMS or emails. For an effective provision of these mobile phone banking services, research evidence indicates that bank cannot rely on PIN, SMS and Emails as information system security. Javelin Strategy & Research (2008) indicates that mobile banking systems must first actually be secure to increase the perception of security. Institutions must choose carefully to ensure that their various mobile phone banking offerings provide the same level of security or better as other channels such as online banking, ATM and branch networks. Therefore, there was a need to evaluate the current information system security, the mobile phone technologies applied in the provision of mobile phone banking services. The study sought to evaluate and if possible derive additional information system security measures that will enhance secure provision of mobile phone banking services in Kenya.

1.2 Statement of the problem

Recent trends shows that commercial banks in Kenya are exploiting the vast market of mobile phone subscribers by introducing mobile phone banking services as a competitive advantage for both personal and retail banking to offer 24 hours, 7 days a week accessibility to their customers.

Despite the adoption of mobile phone banking services, information system securities are a major concern in the provision of mobile phone banking services. Currently, this new banking concept relies on PIN as a security measure in authenticating customer bank accounts, sending emails or updating customers by sending SMS. Much like emails, text messages are not encrypted. So if customer sign up for regular account balance checks via text message, his/her information is being transmitted in a way that makes it vulnerable to interception. Another security concern is that text messages can be stored in a phone (even if a customer deletes the initial message) and if a phone is stolen, a tech-savvy identity thief's could potentially hack into such customer's phones' hard drive and harvest information from it. The similarities between cell phones and computers seem to imply that identity theft from cell phone banking could still be a real possibility.

For an effective provision of these mobile phone banking services, Ochuma (2007) asserts that, the provision of mobile phone banking is influenced by security concerns whereupon he recommended that additional information system security need to be in place for the mobile phone banking to be effective. It is on this basis that the study sought to enhance information system security in the mobile phone banking services in Kenya with the view of evaluating the current information system security and the mobile phone technologies available in Kenya.

1.3 Research objectives

1.3.1 General objective

The general objective of the study was to enhance information system security in the provision of a secure mobile phone banking services in Kenya.

1.3.2 Specific objectives

i. To evaluate current information system security in mobile phone banking.

ii. To provide baseline information on mobile phone banking technologies.

iii. To derive enhanced information system security for mobile phone banking.

1.4 Research questions

i. To find out the currently implemented information system security by banks that offer mobile phone banking services?

ii. What mobile phone technologies are available in Kenya?

iii. How would the current information system security be enhanced for secure provision of mobile phone banking services in Kenya?

1.5 Significance of the study

The study will help in increasing the general body of knowledge and understanding of the effectiveness of mobile phone banking services. Furthermore, the assessment will in turn form a benchmark against which recommendations to enhance information system security will be made. This study will help the banks identify ways of curbing technological risk involved in mobile phone banking services. It will assist banks to carry

out information audit. Moreover, it will enable banks to explore other avenues of product design and development.

The study will be of significant to bank customers as it will cut down their travelling costs incurred whenever they need to pay utility bills, withdraw or deposit money from or into their bank accounts.

Finally, the findings of this study were to form a basis for further research to be implemented to enhance the effective provision of mobile phone banking services.

1.6 Justification of the study

Currently, mobile phone provides the most reliable way to reach a good number of people and to create loyalty among current customers. This is due to the possibility of providing services anytime and anywhere with a high rate of penetration and potential to grow. Commercial banks in Kenya are exploiting the new business model by introducing mobile phone banking services as part of financial solution. Ochuma, (2007) on his recommendation indicates that this new business model is not fully utilized by banks due to information system security reasons. This limit their customers access to their financial services on a real-time basis. The Personal Identification Number (PIN) which is required to access customer's accounts does not really authenticate the real owner of the accounts leading to fraudulent and infringement of customer account security. In order that this information system security deficiency is addressed, this study was purposely to evaluated and derive additional information system security measures which, when placed will enhance the effective provision of mobile phone banking services.

1.7 Scope of the study

The study was targeting customers of commercial banks offer mobile phone banking services within Nairobi, as most of the banks headquarters were based in Nairobi. It evaluated the current information system security measures enforced by banks that offer mobile phone banking services. It sought to derive additional information system security that was enhance secure provision of mobile phone banking services.

1.8 Limitation of the study

The study did not cover other financial institutions, which had not been desired for the study. It was limited to the banking industry. The study did not focus on the server network security of the financial institutions as this was another broad area to be researched on.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter reviews the literature related to the problem of the study. The chapter specifically, documents history of mobile phone banking, banking system in Kenya, Mobile phone banking services in Kenya and its benefits, General principle behind the Study, Previous studies on the mobile phone banking and finally will look at the research gap to be filled by this study.

2.2 History of Mobile phone banking

The revolution of electronic banking can be traced to the early 1970s. Odinga (2005) asserts that, banks began to look at electronic banking as a means to replace some of their traditional branch functions. Hence, banks have found themselves at the forefront of technology adoption for the past three decades. It is imperative for banks to align their strategies in response to changing customers' needs and development in technology (Sing et al, 2002).

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels.

However, perhaps the most recent development in the electronic banking industry is the ability for bank customers to use their mobile phones to conduct some of banks operations. Ochuma, (2007) asserts that, "with technology changing so rapidly and customers requiring different services, traditional banks have a great deal to do if they are to retain their competitive advantage". According to research by the Gartner Group

(2006), once a customer get used to the convenience of viewing his or her account and making transactions at anywhere and anytime, they tend not switch institutions. Consequently, what services the bank can offer to add value to the customers is more important than what technology they should use.

2.3 Banking system in Kenya

According to statistics by the Central bank of Kenya (2010), as at December 2010, 45 commercial banks, 2 mortgage finance company, 2 representative offices of foreign banks, 5 Deposit-Taking Microfinance Institutions (DTMs) and 126 Forex Bureaus. 32 of the banking institutions are locally owned while 13 are foreign owned. For the period ended 31st December 2010 there were 1,063 bank branches operating in the eight provinces of the country. The 67 new branches opened in 2010 across the various regions of the country will facilitate enhanced financial inclusion by the Kenyan populace. One deposit taking microfinance institution, namely Faulu Kenya was issued with a license to allow it to take deposits from the public during the period under review. The commercial banks and the non-banking financial institutions offer corporate and retail banking services but a small number offer other services which include investment banking.

Dawson (2007), assert that the increasingly advanced levels of information technology embraced by banks have had a positive impact in the sector characterized by innovation of new products and new business model such as the mobile phone banking services. The new business model is meant to provide a convenient real time customer financial transaction on 24 hours, 7 days a week anytime and anywhere e.t.c.

2.4 Mobile phone banking in Kenya

Njenga (2009) asserts that mobile phone banking started with the creation of services by banks which could be accessed through the mobile phone. These facilities aimed to enable customer's access information relating to their accounts. Subsequent innovations have seen the mobile banking phenomena continue to grow steadily. Mobile banking takes several dimensions of execution all representing a new distribution channel that allows financial institutions and other commercial actors to offer financial services outside traditional bank premises.

Porteous (2006) asserts that mobile banking has the potential to be transformational owing to various facts. First, it uses existing mobile communications infrastructure which already reaches unbanked persons. Secondly it may be driven by new players, such as mobile phone industry operators, with different target markets from traditional banks who are able to harness the power of new distribution networks for cash transactions.

Banks in Kenya have noticed the potential in mobile phone technology and are now adjusting their services to the use of mobile phone. Mobile phone banking services was first introduced in Kenya, in 2003, by Co-operative bank of Kenya know as M-banking (http://www.co-opbank.co.ke). Many others banks have now introduced these services. The new business model today enables new revenue opportunities for financial institutions. This provides a new channel that can be used to refresh and expand the customer base, attracting new customers and enhance loyalty.

Some of the commercial banks in Kenya offering this service include; KCB (Connect), National bank (SMS banking), Equity bank (SMS banking), Family Finance bank, Barclays bank, Transnational Bank (SMS banking) e.t.c. According to Equity bank

(www.equitybank.co.ke/products), some of the mobile phone banking services offered includes; salary credit advice, ATM withdrawal advice, Account balance enquiries, Safaricom or Airtel airtime purchase, order for statement, stop cheque or payment instructions, forex rate enquiry, utility bills payments, loan approval, loan repayment notification and limited funds transfer or withdraw e.t.c. Goldstuck (2004) asserts that, many customers use these basic services and demand for more advanced electronic-basic banking services via their mobile phone handset.

A number of banks now have strategies to safeguard their clients' accounts by using mobile alerts services. In addition to checking their balances via text message, banks do notify customers when a withdrawal has been made on their account.

Most of these mobile phone banking services are supported by the SMS support system (CCK, 2006). The most recent support system introduced in Kenya is the EDGE implemented by Equity bank. The challenge, then, is how to integrate the possibility of two industries (mobile phone and banking industry) in terms of information system security in ensuring that customer entrust the mobile phone banking system (Dawson, 2005).

2.5 Benefits of Mobile Phone Banking Services

During the launch of Equity mobile phone banking service (SMS banking), Ndung'u (2008) highlighted, "The service provides an EAZZY 24/7 Mobile Phone Banking services solution to customers as they shall literally be carrying their accounts in their hands". Therefore, this is indeed a revolutionary solution that will provide the following six key benefits:-

i. Banking the unbanked

ii. Convenience

iii. Beyond banking financial solution

iv. Opening new economic frontiers and supporting Vision 2030

v. Growth in new customer base and markets

vi. Growth in number of transaction

2.6 Theoretical Framework

It is clear that technology has, once again, leapfrogged our lethargic legislative and policy institutions. Wireless networks are inherently vulnerable and this includes Global System for Mobile Communications (GSM). Cyber criminals are able to monitor wireless traffic to determine, control and manipulate signal, bandwidth, leakage patterns and so forth (Javelin Strategy & Research (2008). They also engage in mobile sniffing where a vulnerable access point or backdoor is identified.

Taking an example of Habib Bank Zurich, some of its information system security implemented is the use of CRAM-based security model on the bank website. According to Farid (2009), "the model will not only ensure that on-line banking customers of it Habib Bank Zurich web will have four levels of security to protect their information, but will also literally put the power of access only in the hands of the user himself". The model has cascading login system with a multi-level authentication mechanism, typically risks like password or keystroke tracking and even phishing can be eliminated.

The CRAM-model is a program which runs on any java enabled mobile phone. The disadvantage of this system is that not all mobile phones runs on java script therefore it becomes non user friendly to those bank customers who don't have java enable phones.

Other security measures implemented by Dubai bank on its mobile phone services is the use of SSL (Secure Session layer) technology to connect and it uses "High Grade Encryption of 3DES 168 bit" to protect customers financial transactions and information. SSL helps in providing a secure channel for data transmission from customers' Mobile browser to Dubai Bank's systems. The disadvantage of this information system security measure is that its only supporting 3G/GPRS mobile phones such as:

- Blackberry curve 8300
- Samsung E590
- Nokia E61i
- Nokia N95
- Motorola Q 9h
- Motorola RAZR2 V9

Therefore, for those clients with different mobile phone model will have difficulties in accessing banking transactions.

According to Javelin Strategy & Research (2008), some of the common information security systems threats in the provision of mobile phone banking services include the following;

2.6.1 Snooping

As with any financial system, mobile phone banking solutions must provide strong encryption throughout the entire data path between the mobile phone device and the protected zone of the financial institution. Unfortunately some mobile phone solutions allow sensitive financial data to exist in the clear (unencrypted and unprotected) while on

the carrier networks or in gateway servers. In such cases, criminals can obtain and use sensitive information by simply intercepting unencrypted data.

2.6.2 Phishing

With phishing emails, fraudsters trick customers into revealing their bank log-in information. For example; one receives an email on his or her mobile phone supposedly from his bank asking them to update their account number and PIN by clicking a certain link, only to end up revealing them to a fraudster.

2.6.3 Smishing

Similar to phishing, but unique to SMS messaging, in so-called "smishing", criminals pose as the financial institution to trick users into sending sensitive information via a text message. For example, criminals can send phishing-like SMS messages to consumers posing as a legitimate financial institution hoping that recipients will respond to their requests for sensitive information. Additionally, criminals could setup a phony SMS service with a phone number very similar to the financial institution. Initially, SMS was not designed to carry sensitive information. SMS data is almost invariably unencrypted through-out much of the connection between the mobile phone handset and the bank.

2.6.4 Man-in-the-middle

If a system is designed with data flowing through a single component, criminals can access all the information flowing through it if they can find a way to compromise that component. For example, if a carrier had equipment that terminated the encrypted

connection from the mobile device and initiated a new tunnel to the bank; a criminal could gain access to the sensitive information if they found a way to compromise this equipment in the middle.

2.6.5 Unencrypted sensitive client-side data on carrier networks

The rich capabilities of client software running on the phone provide opportunities to enforce existing institutional rules for challenge/response, password length and content, one-time passwords and so on. Unfortunately, some client-side solutions insert gateways between devices and institutions. Gateways introduce a security risk because they require both endpoints (the mobile device and the bank) to authenticate with the gateway instead of each other, thus requiring the endpoints to simply trust that the gateway will protect the data and always send it to the appropriate location. This approach creates the opportunity for a Man-in-the-Middle attack in addition to exposing sensitive information.

2.6.6 Money Launderers

Money launderers will try to recruit bank customers into their racket with emails. Fraudsters contact prospective victims with "*job vacancy*" adverts via spam emails or job search web sites. They offer bank customers the chance to earn some easy money for a few hours work each week, usually just requiring an access to the Internet. When client respond to such, they cut them into the deal and ask for their account details so that they route money to them.

2.6.7 Client-Side Solutions

Client-Side solutions are applications running on the mobile phones. Client-Side solutions could be a binary application downloaded to the phone or Asynchronous JavaScript and XML application launched from a secure site. Client-Side solutions offer the most functionality, best user experience and the most security. Furthermore, Client-Side solutions must be carefully designed to not introduce security risks. For example, a 128-bit Secure Sockets Layer (SSL) tunnel should exist without interruption from the mobile phone to the institution mobile gateway. Each transaction should also use multiple factors of authentication.

In summary, as with any system, mobile phone solutions must be carefully designed use the best of each technology and to ensure the security of sensitive information. Mobile systems are no less secure than other systems when implemented using the same best practices implemented in other channels such as online banking.

2.6.8 Password Key-chains

Some mobile phone solutions keep their own database of user credentials for each institution the user has enabled. Surprisingly, some solutions actually outsource this critical control to the mobile carrier, which is obviously not a financial institution.

In addition to raising serious questions about responsibility and indemnification in the event of an attack, this approach introduces a number of security risks such as:

- Assets at all accounts are affected if the common keychain username and password is compromised

- The security of every institution in the keychain is reduced to the security of the weakest institution
- Key-chains could allow non-financial institutions to control access to financial institutions
- Key-chains prevent institutions from providing their own unique security model, in addition to ceding control to a third-party

The keychain approach not only stores credentials in a second location, violating a basic security best practice, but the credentials are stored at a third-party (the mobile banking provider or even the mobile carrier in some cases). Mobile carriers have proven themselves susceptible to security breaches as witnessed in the HP pre-texting case and in the cracking of Paris Hilton's phone. Therefore, mobile phone companies were not designed to protect financial assets.

2.6.9 Individual Bank Security Models or Risk of Preloaded Software

Every bank has its own security policies and best practices. Often these policies and procedures reflect variations in business models, product mix and customer demographics. Many banks view security as a competitive advantage. Each bank needs the flexibility to implement its own security approach and wants to leverage their expensive security infrastructure as much as possible. Unfortunately, many mobile phone solutions provide few or no options for banks to implement their own security model in their mobile phone channel.

In other cases, some vendors preload software onto phones. Preloaded software introduces some risks. First, preloaded software is almost certainly out-of-date by the

time it reaches the consumer. Out-of-date software may no longer communicate properly to newer versions of software at the bank institution. Furthermore, a distribution model that relies on preloading software has no way to remove bugs from software in the carrier inventory or on consumer handsets.

Secondly, consumers cannot confirm the authenticity of preloaded software. Anyone with access to the device at the carrier or phone store could replace the correct software with criminal software (e.g. spyware) that gains access to the consumer's phone.

Other information system security issue highlighted by Javelin Strategy & Research (2008) is that most cell phones don't come standard with anti-virus protection even if they have the capacity to browse the internet. Some phones aren't even compatible with the anti-virus software available and there are known cases in which people were unable to put anti-virus software registered to them on corporate cell phones. Although identity thieves are still a few steps behind when it comes to learning to implement some of their most successful computer tricks (phishing, spamming, spreading viruses, account hacking, e.t.c.) on a cell phone level, experts agree that is only matter of time and people shouldn't assume that anti-virus software isn't necessary for cell phones.

From the above fraudster's scenarios, mobile phone banking is set to revolutionize the way we manage our money in the same way that Internet banking did. But in an age of rampant cyber crime and fraudulent, information system security is the primary concern of which banks cannot rely on Emails, SMS alerts and PIN alone as an Information System Security in authenticating customer bank account information. It is on this basis that, this study sought to evaluate and derive additional information system security measures that will enhance secure provision of mobile phone banking services.

2.7 Previous Studies on Mobile phone banking

2.7.1 Adoption of Mobile phone banking

The global proliferation of the mobile phone has brought many financial institutions to look at it as a possible channel for delivering financial products and services. These services take a variety of forms- including long-distance remittance, micropayment and informal airtime bartering schemes.

A research study on the mobile phone banking: Usage and experience by Njenga (2009), point out that with the introduction and use of fiber optic cable, it has resulted into faster bandwidth (improved internet connectivity); therefore, most of financial institution networks are now vulnerable to hackers as they are keen to penetrate various financial computer networks and servers to obtain crucial information on individual through their mail servers. These studies have, however, not focus on the information system security concerning the adoption of mobile phone banking. This study goal was a call attention to the gap in the research literature and emphasizes the need for research focusing on the context(s) evaluating and deriving additional information system security that will enhance secure provision of mobile phone banking services.

2.7.2 Current existing information systems security

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, is the most complicated challenges facing many banks in Kenya. As when a customer's conducts a transaction using their PC, wireless or even ATM implies that the customer only needs a PIN to start the operation, and since the PIN itself does not guarantee that the person who is transacting is

actual the real cardholder. According to research findings by Donner (2007), banks customers had a different take on the appeal of using SMS to keep in touch with clients and, particularly, to bill them or update them on credit outstanding. Respondents were more open to the idea of using a mediated message to stay in touch with clients, but the majority of respondents (95%) expressed varying degrees of concern about using an SMS to discuss money matters, particularly credit. Most of the respondents were of the view that, it is not right to use SMS to remind customers about payments because it is too impersonal.

As from the above explanation, this new banking concept relies on PIN authentication, updating customers by sending unencrypted SMS or emails.

Some of the other security implemented in the mobile phone banking services include;

- Limited electronic money transfer
- Use of different PIN for mobile phone banking services
- Security infrastructure i.e. the use of PKI (public key infrastructure) an encryption used by smart phones, the PKI consists of two keys, a public key and private key used to authenticate the user and encrypt the data.

The point to be noted here is that in the next few years, majority of Kenyans will be having mobile phones handsets and will have access or own bank accounts. Hence customers will want to access all their financial services from anywhere at any time regardless who provides the services. To be precise, (Ochuma, 2007) asserts that, linking a portable such as a mobile phones handset and a current account seems to be an obvious way forward".

2.7.3 Customer Awareness & perception

This has been seen as a another limiting factors as banks need to create or increase awareness of mobile phone banking or sell the benefits of this new service to their customers or provide sufficient information on the users of the service.

Previous study by (Morawczynski & Miscione, 2008) relating to trust in mobile phone banking transactions in Kenya, indicates that many customers are not willing to use this service thinking that it might be hacked or lead to giving out information to the wrong individual masquerading as banks' agents. However, there is room for more work that assesses which forms of trust support or is supported by mobile phone banking use, particularly among low-income users. Furthermore, Some potentials bank customers don't use mobile phone banking services because they perceive it as expensive and insecure. To be precise, customers are not using this new service because they don't understand the technological behind this service and some don't trust their phones as security and confidentiality is in doubt in many bank customers mind.

Another study by Ochuma, (2007) on the state of mobile phone banking in Kenya indicates that, "Banks should market more on the use of mobile phone banking since most customers are not much familiar with this new banking service in some of our banks. The marketing strategies should be aimed at increasing awareness".

2.7.4 Mobile phone technology

The mobile phone technology is a limiting factor to the implementation of the new banking services as different phones uses different wireless network (GPRS, Bluetooth, CDMA e.t.c). Therefore banks will be required to be able to support all types of mobile data as they proliferate e.g. SMS and EDGE.

In other words, the compatibility of mobile phones is an issue as different phones have other mode of support systems. To integrate the different mobile banking application, it would be wise for banks to develop application that can connect multiple banks. It would require either the application to support multiple protocols or use of a common and widely accepted set of protocols for data exchange.

Mobile phone banking systems of the future will need to have the ability to communicate with customers on all wireless networks, wherever they are and whatever time of the day. In regard to mobile phone network compatibility, the CCK is planning to implement the regulation on service number portability (SPNP). The commission considers SPNP as a critical feature that would further enhance competition by giving customers the flexibility to choose their provider in a seamless manner without having to worry about the prospects of losing touch with their business associates, friends and family".

The CCK idea of offering phone users flexibility is a noble idea as this will enable banks to implement their network platform without having trouble on the choice of network to use.

Some of the banks that have adopted the use of mobile phone banking services use the GSM technology which is designed with a moderate level of security. The system was designed to authenticate the subscriber using a pre-shared key and challenge-response. Communications between the subscriber and the bank can be encrypted. GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation. Furthermore, GSM uses several cryptographic algorithms for security. The disadvantage of this technology is that it has a fixed maximum cell site range of

35 km, which is imposed by technical limitation. Therefore, it makes it not applicable especially to those phones of 2G which are mainly analogue.

2.7.5 Derive additional information system security

Goldstuck (2004) explored the future of mobile financial services and stated that mobile phone baking systems of the future will need to have the ability to communicate with customers on all wireless networks (GSM, CDMA, PCS e.t.c), wherever they are and whatever time of the day.

Many banks in developed countries already support SMS, smart menus and now wireless internet (WAP) content. Mobile digital signatures will enable customers to sign transactions safely. Mobile phones can either have an application on the smart card inside the phone allowing customers access to banking services or phones can have a browser to access services from a mobile phone banking system.

Voice recognition will be one of the next powerful interfaces that will be used to obtain financial services. Mobile phone banking systems will understand instructions spoken to them. This technology already exists and bank in Europe are very much at the frontier of this, (Goldstuck 2004).

Nevertheless, the areas of information system security in the provision of mobile phone banking had generally not been explored adequately by the current body of literature and therefore have remained rather uncharted territory. Exploring this area of security, it is evident that information system security is a major concern for those banks adopting this new banking service. Therefore, this leads us to the main concern that additional securities are needed for authentication when using mobile phone to access bank account.

2.8 Research gaps to be filled by the study

2.8.1 Enhancement of Information System Security

Currently, the new banking concept security focused on PIN authentication, limited electronic money transfer, updating customers by sending unencrypted SMS or emails. Security of financial transactions, being executed from some remote location and transmission of financial information over the air, is the most complicated challenges facing many banks in Kenya.

Kandie (2003) established that the feeling of security among customers of a bank enhanced their perception of the quality of service. With the feeling of secure, a customer would be able to transact using his mobile phone more freely and use it for more services without fear that their handset might be hacked and steal their details or lead to giving out information to the wrong individual masquerading as banks' agents.

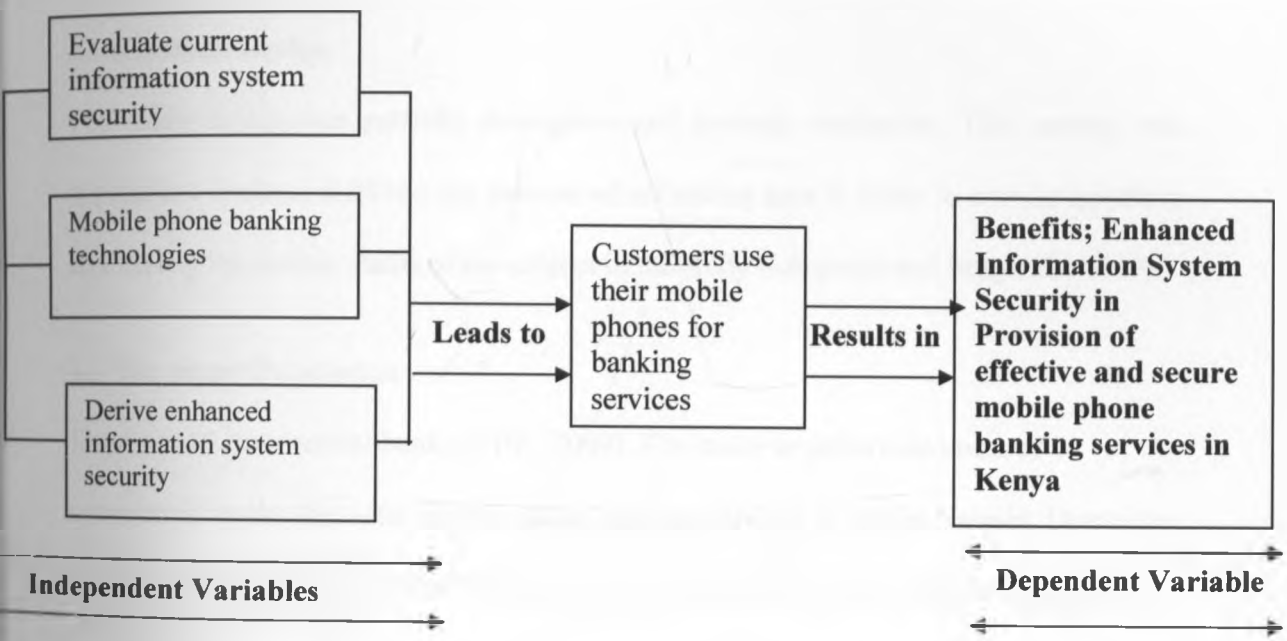
Ochuma (2007) asserts that, the provision of mobile phone banking is influenced by security concerns whereupon he recommended that additional information system security need to be in place for the mobile phone banking to be effective. Therefore it is palpable that the areas of information system security in the provision of mobile phone banking has generally not been explored adequately by the current body of literature and therefore have remained rather uncharted territory.

This study sought to evaluate and derive additional information system security measures that will enhance secure provision of mobile phone banking services.

2.9 Conceptual Framework

The extent of enhancing information system security in mobile phone banking services is determined by factors that include; current information system security in mobile phone banking services, mobile phone banking technologies, and the derive enhanced information system security. The mentioned variables have direct impact on the provision of mobile phone banking services offered by banks in Kenya.

Table 2.9: Conceptual Framework 2012: Enhancing Information System Security in Mobile phone Banking Services.



Source: researcher, 2012

CHAPTER THREE

3.0 METHODOLOGY

This chapter includes: research design, the target population, the sample size and sampling procedure, data collection procedures and tools, and the data analysis techniques.

3.1 Research Design

The study design was partially descriptive and partially evaluative. This method was appropriate because it allows the process of collecting data in order to answer questions concerning the current status of the subject in the study (Mugenda and Mugenda, 1999).

3.2 The target Population

There are 45 commercial banks (CBK, 2009). The study targeted customers of commercial banks that offer mobile phone banking services to within Nairobi. Due to the fact that most banks have their headquarters in Nairobi, much information was gathered. Most of banks customers in Nairobi were presumed to have good knowledge on the use of mobile phones and were aware of the services provided by mobile phone network providers. The study assumed that it is in Nairobi that mobile phone banking services are needed more because most employed people are busy queuing at the banks awaiting for services. Therefore it was easy to access the target population.

3.3 Sample size and sampling procedure

The study used stratified random sampling technique to pick a sample of respondents.

There are 45 commercial banks (See Appendix 111);

Stratified random sampling where;

N = the estimate of the population size.

N= 45

45 * (10/100) = 4.5 ≃ 5 banks

10% to 30% of target population

30 being the minimal number of a sample

5 banks * 30 = 150 commercial bank customers

3.4 Data types and Data collection techniques

The study used self- administered questionnaires and interviews to collect primary data. Questionnaires were distributed to the 150 bank customers. The questionnaires were essential in collecting information from a large population within a relatively short period.

The questionnaires involved both structured and unstructured question items. The structured items enabled the researcher tabulate and analyze data with ease, while the unstructured ones were set to facilitate in-depth responses and opinions beyond the researcher's scope of understanding.

The secondary sources of data were collected from published financial reports, journals and any other relevant documented information related to the study.

3.5 Data analysis

Descriptive statistics including tables, frequencies, percentages and graphs were used to analyze the data.

Findings were analyzed using the statistical package for social sciences (SPSS) and were presented in table, charts and graphs showing where most responses were featured and in the process helped in conclusion on whether there was a need to derive additional information system security measures that will enhance secure provision of mobile phone banking services in Kenya.

CHAPTER FOUR

4.0DATA ANALYSIS, FINDINGS AND PRESENTATION

4.1 Introduction

This chapter presents the research findings in a study of enhancing information system security in the mobile phone banking services in Kenya. The study focused mostly on the commercial banks in Kenya with the aim of the result answering the objectives of the study, which include evaluating current information system securities in mobile phone banking, provide baseline information on mobile phone baking technologies and derive enhanced information system security in mobile phone banking.

4.2 Baseline Information of the Study

The results were based on 150 bank customers whose questionnaires were returned for data analysis. The graphs have been generated by SSPS software from the respondents

4.2.1 Socio Demographic Characteristics of Study participants (Customers)

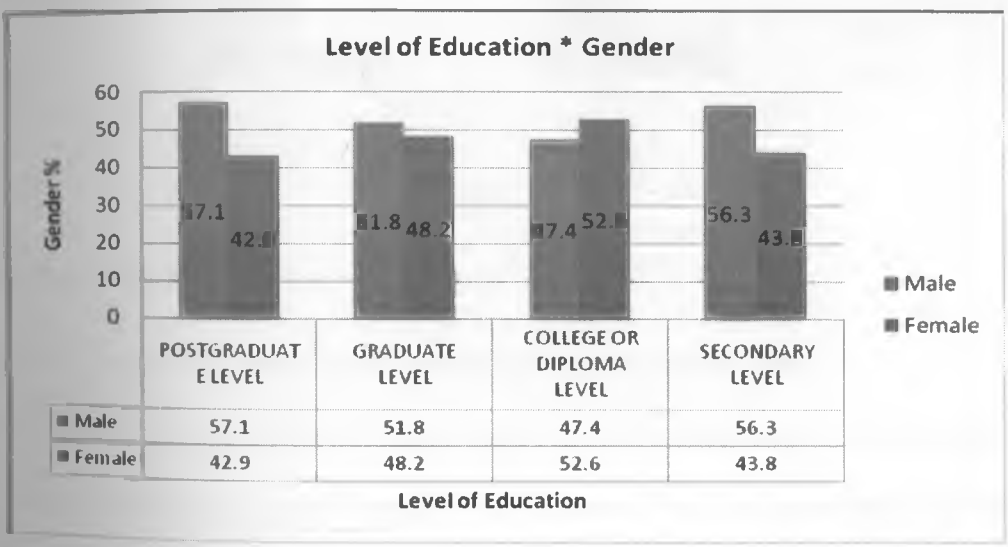
A total sample of 150 bank customers participated in the study. Table 4.1.1 shows the distribution of the respondents in terms of gender and education level. Seventy seven (51.3%) of the participants were male and seventy three (48.7%) being female. Most of the respondents had higher educational level, with the highest level being in the Diploma level 57 (38%), followed Graduate level 56 (37.33%), then postgraduate level 21 (14%) lastly secondary level 16 (10.67%).

Table 4.2.1 Distribution of the respondents in terms of gender and educational level

		GENDER					
		MALE	%	FEMALE	%	Total	%
LEVEL OF EDUCATION	POSTGRADUATE LEVEL	12	57.1	9	42.9	21	14
	GRADUATE LEVEL	29	51.8	27	48.2	56	37.33
	COLLEGE OR DIPLOMA LEVEL	27	47.4	30	52.6	57	38
	SECONDARY LEVEL	9	56.3	7	43.8	16	10.67
Total		77	51.3	73	48.7	150	100

Source: researcher, 2012

Figure 4.2.1: Percentage distribution of respondents based on their gender and level of education



Source: researcher, 2012

Use of mobile phone banking services

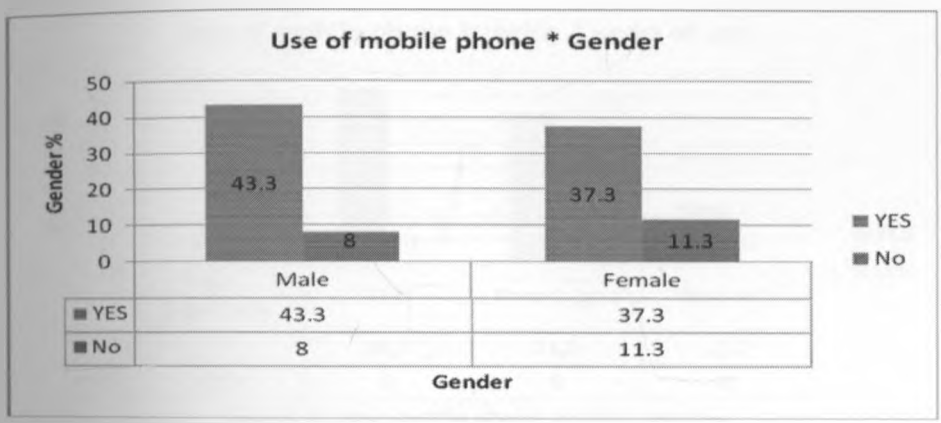
Table 4.1.2 shows that most of the customers were using mobile phone banking services within their respective banks. One hundred and one (80.7%) were using mobile phone banking services while twenty nine (19.3%) were not using mobile phone banking.

Table 4.2.2: distribution of the respondents in terms of gender and use of mobile phone banking services

USE OF MOBILE PHONE * GENDER							
		GENDER					
		MALE	%	FEMALE	%	Total	%
USE OF MOBILE PHONE	YES	65	43.3%	56	37.3%	121	80.7%
	NO	12	8.0%	17	11.3%	29	19.3%
	TOTAL	77	51.3%	73	48.7%	150	100.0%

Source: researcher, 2012

Figure 4.2.2: Percentage distribution of respondents based on their gender and use of mobile phone services



Source: researcher, 2012

4.2.3 Number of years using Mobile phone banking services

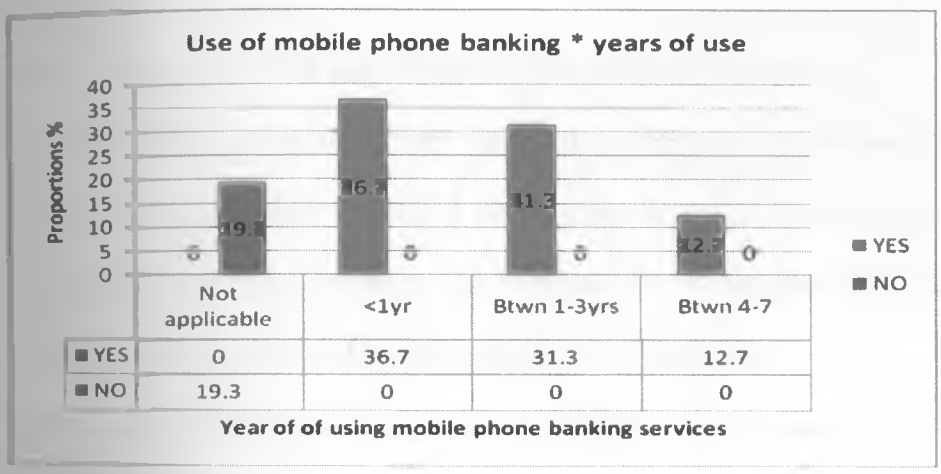
With regard to the number of years customres have been using mobile phone banking services, most of the respondents(36.7%) indicated that they have used it in less than a year. 31.3 % of the respondents indicated that they have used the service in between 1-3 years, while 12.7% have used it for 4 -7 years old. This is as shown in the table and figure below.

Table 4.2.3: Distribution of the respondents in terms of number of years using the service

USE OF MOBILE PHONE * YEARS OF USE											
		YEARS OF USE									
		Not Application	%	< A Yr	%	BTWN 1-3 Yrs	%	Btwn 4-7 Yrs	%	Total	%
E OF MOBILE ONE	YES	0	0.0%	55	36.7%	47	31.3%	19	12.7%	121	80.7%
	NO	29	19.3%	0	0.0%	0	0.0%	0	0.0%	29	19.3%
	TOTAL	29	19.3%	55	36.7%	47	31.3%	19	12.7%	150	100.0%

Source: researcher, 2012

Figure 4.2.3: Percentage distribution of respondents based on number of years using the service



. Source: researcher, 2012

4.3 Current Information Systems Security in Mobile Phone Banking

From the study the respondent were asked to indicate the current information system security implemented by their banks in authenticating and authorizing access to individual bank accounts. Majority of them indicate PIN (54.8%) as the frequently used mode of authentication and authorization access to their accounts. The distribution of respondents based on the implemented security system is shown on the crosstablution tables below:

Table 4.3: Distribution of respondents based on the implemented information sytem security by their respective banks

Current Information System Security	Responses	
	N	Percent
PIN	115	54.8%
SMS	65	31.0%
EMAIL	24	11.4%
LIMIT IN THE NUMBER OF TRANSACTIONS	6	2.9%
Total	210	100.0%

Source: researcher, 2012

4.3.1 Adequacy on the use of mobile phone banking services

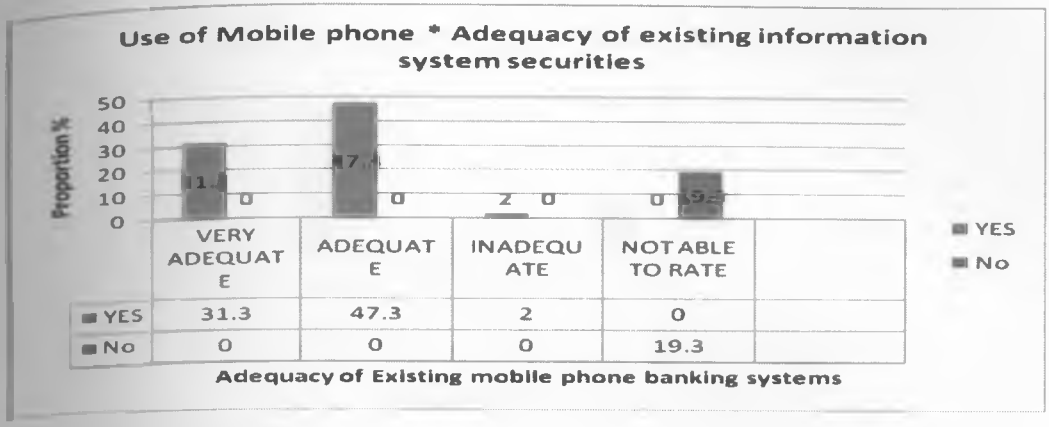
The respondent also provided their views on the adequacy on the use of mobile phone banking services in their respective banks. Forty seven (31.3%) as shown on the table below indicate the services were very adequate, 47.3% adequate while 3% were of the view the current information system security were inadequate.

Table 4.3.1: Distribution of respondents based on the adequacy use of mobile phone banking sevices

USE OF MOBILE PHONE * ADEQUACY USE OF MOBILE PHONE BANKING SERVICES										
OF ILE NE		VERY ADEQUATE	%	ADEQUATE	%	INADEQUATE	%	NOT ABLE TO RATE	%	Total	%
	YES	47	31.3%	71	47.3%	3	2.0%	0	0.0%	121	80.7%
	NO	0	0.0%	0	0.0%	0	0.0%	29	19.3%	29	19.3%
	TOTAL	47	31.3%	71	47.3%	3	2.0%	29	19.3%	150	100%

Source: researcher, 2012

Figure 4.3.1: Percentage distribution of respondents based on the adequacy use of mobile phone banking sevices



Source: researcher, 2012

4.3.2 Efficiency on the use of mobile phone banking services

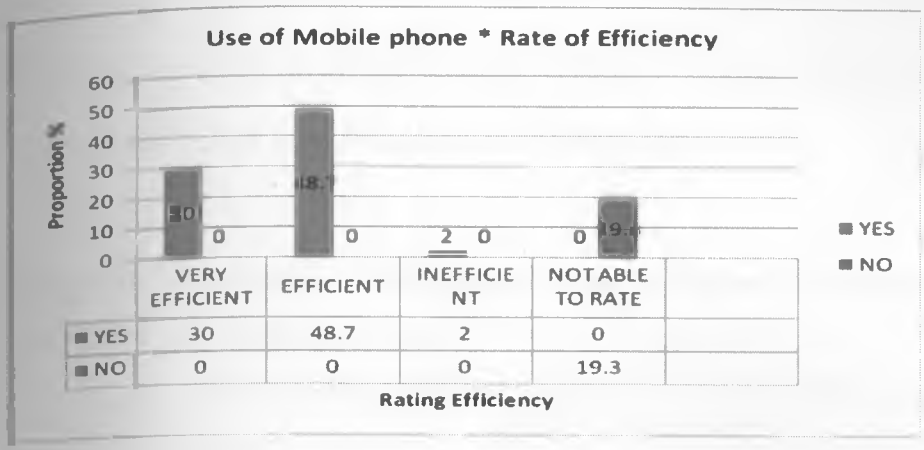
The respondents were asked to rate the level of efficiency on the use of mobile phone banking services. Forty five (30%) as shown on the table below indicate the system security were very efficient, 48.7% efficient while 3% were of the view the current information system security were inefficient.

Table 4.3.2: Distribution of respondents based on efficiency on the use of mobile phone banking services

USE OF MOBILE PHONE * RATING EFFICIENCY											
		RATING EFFICIENCY									
		VERY EFFICIENT	%	EFFICIENT	%	INEFFICIENT	%	NOT ABLE TO RATE	%	TOTAL	%
USE OF MOBILE PHONE	YES	45	30.0%	73	48.7%	3	2.0%	0	0.0%	121	80.7%
	NO	0	0.0%	0	0.0%	0	0.0%	29	19.3%	29	19.3%
	TOTAL	45	30.0%	73	48.7%	3	2.0%	29	19.3%	150	100.0%

Source: researcher, 2012

Figure 4.3.2: Percentage distribution of respondents based on efficiency of existing mobile phone banking system security



Source: researcher, 2012

4.3.3 Efficiency of the existing mobile phone banking system security

Based on the table below it clearly shows that on the overall customers who uses mobile phone banking services (121 respondents), majority uses PIN and (59.50 %) indicated systems to be efficient followed by very efficient (37.19%). This suggests that majority of respondents view the current information system security to be efficient.

Table 4.3.3: Distribution of respondents based on efficiency on the existing mobile phone banking information system securities

RATING EFFICIENCY	Current Information System Security				
	PIN	SMS	EMAIL	LIMIT IN THE NUMBER OF TRANSACTIONS	Total
VERY EFFICIENT	43	24	10	1	45
	37.4%	36.9%	41.7%	16.7%	37.19%
EFFICIENT	68	39	13	4	72
	59.1%	60.0%	54.2%	66.7%	59.50%
INEFFICIENT	3	2	1	1	3
	2.6%	3.1%	4.2%	16.7%	2.48%
NOT ABLE TO RATE	1	0	0	0	1
	.9%	.0%	.0%	.0%	0.83%
	115	65	24	6	121

4.3.4 Level of satisfaction on the use of mobile phone banking services

Sixty three of the respondents (42%) as shown on the table below were satisfied with the use of mobile phone in accessing bank services, 30% very satisfied while 13% were unsatisfied in the use of mobile phone in accessing bank services.

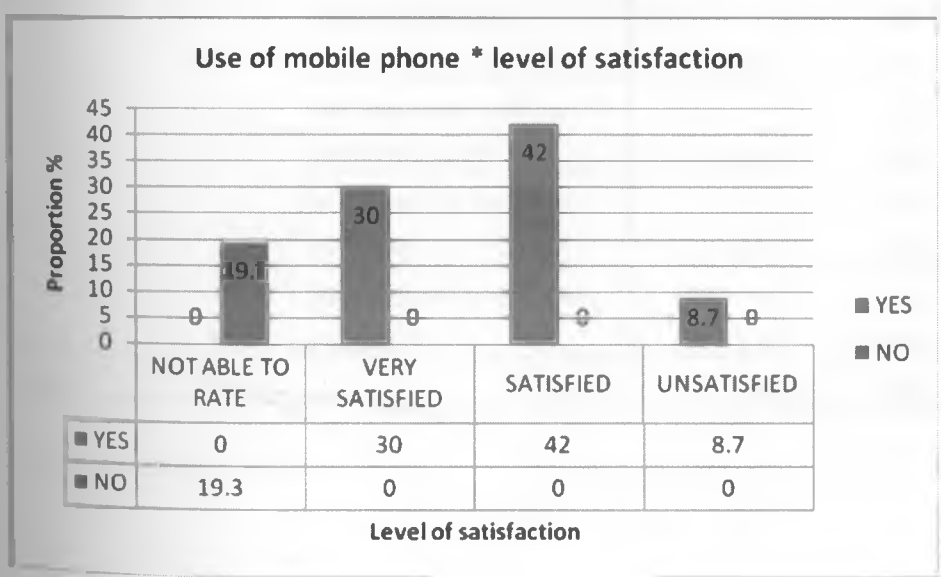
Table 4.3.4: Distribution of respondents based on the level of satisfaction on the use of mobile phone banking services

USE OF MOBILE PHONE * LEVEL OF SATISFACTION Cross tabulation

		LEVEL OF SATISFACTION									
		NOT ABLE TO RATE	%	VERY SATISFIED	%	SATISFIED	%	UNSATISFIED	%	Total	%
USE OF MOBILE PHONE	YES	0	0.0%	45	30.0%	63	42.0%	13	8.7%	121	80.7%
	NO	29	19.3%	0	0.0%	0	0.0%	0	0.0%	29	19.3%
	TOTAL	29	19.3%	45	30.0%	63	42.0%	13	8.7%	150	100.0%

Source: researcher, 2012

Figure 4.3.4: Percentage distribution of respondents based on the level of satisfaction on the use of mobile phone banking services



Source: researcher, 2012

4.4 Baseline Information on Mobile Phone Banking Technologies

The study found out that customers were using the bank in conducting banking services. Most of the respondents were aware of the top up airtime, followed by utility bill payments and ATM withdrawal. Real time stock quotes were not popular among the respondents. The below table shows the banking transactions mobile phone banking services conduct.

Table 4.4: Distribution of respondents based on transactions conducted at each banking channel

Accessibility of services		Conduct services			Total
		POS	BANK	PHONE	
	Top up airtime	16	306	299	621
		24.6%	22.5%	23.7%	
	ATM withdrawal or Salary Credit advice	11	205	189	405
		16.9%	15.1%	15.0%	
	Fund transfers and commercial payments	5	137	128	270
		7.7%	10.1%	10.2%	
	Utility bills payments	12	266	247	525
		18.5%	19.6%	19.6%	
	Order for statements	7	231	203	441
		10.8%	17.0%	16.1%	
	Real time stock quotes or forex rate enquiry	7	45	37	89
		10.8%	3.3%	2.9%	
	Stop cheque or payments instructions	3	59	52	114
		4.6%	4.3%	4.1%	
	Loan approval or repayment notification	4	111	105	220
		6.2%	8.2%	8.3%	
Total		65	1360	1260	2685

Source: researcher, 2012

4.4.1 Mobile Data technology

The study finds out that the most frequent used mobile phone data support technologies were SMS (65.6%). This was due to the fact that other support systems such as WAP (15.8%), EDGE (16%), 3G Services (10%) and GPRS (8%) were still new in the country. SMS services was widely used because most low-end phones in the market are having this support service, while others such as WAP, EDGE, GPRS and 3G services needed specific phones, which are expensive to Kenyans. Below table shows the distribution of respondents based on the mobile data they used.

Table 4.4.1: Distribution of mobile phone data technologies used in mobile phone banking

Mobile banking technologies	Responses	
	N	Percent
SMS	120	65.6%
WAP	29	15.8%
EDGE	16	8.7%
GPRS	8	4.4%
3G	10	5.5%
SERVICE		
Total	183	100.0%

Source: researcher, 2012

4.4.2 Level of satisfaction on the use of mobile phone data technology

Based on the table below it clearly shows that on the overall customers who uses mobile phone banking services (121 respondents), majority uses SMS as a mobile phone data and 53.72% were satisfied with the mobile phone data, followed by very satisfied (36.36%). This suggests that majority of respondents view the current mobile data to be satisfactory.

Table 4.4.2: Distribution of respondents based on the level of satisfaction on the use of mobile phone data

LEVEL OF SATISFACTION		Mobile phone data					
		SMS	WAP	EDGE	GPRS	3G SERVICE	Total
	VERY SATISFIED	43	15	11	3	6	4
		36.1%	51.7%	68.8%	37.5%	60.0%	36.36%
	SATISFIED	65	11	3	3	3	6
		54.6%	37.9%	18.8%	37.5%	30.0%	53.72%
	UNSATISFIED	11	3	2	2	1	1
		9.2%	10.3%	12.5%	25.0%	10.0%	9.92%
Total		119	29	16	8	10	12

Source: researcher, 2012

4.5 Challenges of Using Mobile Phone Banking

Majority of the respondents said that lack of security and confidentiality (30.3%) on the usage of mobile phone banking was the biggest challenge they were facing in the use of mobile phone banking services, followed delay in system response time (26.6%). System breakdown (25.8%) was third, fourth as fast changes in technology (9.2%) this is because new technologies in the support systems are invented every day. From the analysis, it shows that customers were still not at ease to use the mobile phone banking service due to fact they are not assured of their funds being in safe hands while making the transactions. The below table shows views on the challenges of using mobile phone banking services

Table 4.5 Distribution of respondents based on the challenges of using mobile phone

Challenges using mobile banking services	Responses	
	N	Percent
Lack of security and confidentiality	108	30.3%
Lack of knowledge on the usage	29	8.1%
Fast changes in technology	33	9.2%
System breakdown	92	25.8%
Delay in system response time	95	26.6%
Total	357	100.0%

Source: researcher, 2012

4.6 Enhanced Information System Security for Mobile Phone Banking

From the table below, 16.7% of the respondent suggested biometric methods to be introduced as information system security in authenticating customer's bank accounts. Second method suggested was the use of codes and passwords (12.7%), this was followed by tracking system (7.3%), and mobile portability (2.7%), the rest of 57.3% did not give any suggestions as shown on the table below.

Table 4.6: Distribution of respondents based on the information system security implemented in future

INFORMATION SYSTEM SECURITY IMPLEMENTED IN FUTURE			
	Frequency	Percent	Valid Percent
No ideas	86	57.3	57.3
Biometric methods	25	16.7	16.7
Limited Number of transactions	5	3.3	3.3
Mobile phone portability	4	2.7	2.7
Tracking system	11	7.3	7.3
Use codes and passwords	19	12.7	12.7
Total	150	100.0	100.0

Source: researcher, 2012

4.6.1 Benefits of using enhanced information system security

The respondents were asked to suggest on the benefits derived from using enhanced information system security. 27.21% of the respondents said that if the current system securities are improved it will save a lot of time in visiting the bank. While 26.05% of the respondents indicated that they will have easy access to banking information. 25.35% were of the view the improved system will minimize queues in the bank. The rest 21.4% indicated it the improved information system security will help in real time access of their money as shown on the table below.

Table 4.6.1: Distribution of respondents based on benefits derived from enhanced information system securities

		Benefits of using mobile phone banking				
		Real time to access money	Easy access to banking information	Time Saving	Less queues in banks	Total
USE OF MOBILE PHONE	YES	92	112	117	109	121
		21.4%	26.05%	27.21%	25.35%	100%
Total		92	112	117	109	121

Source: researcher, 2012

CHAPTER FIVE

5.0 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter gives a summary of the major findings, makes conclusion and recommendations of the study.

5.2 Conclusions

It is clearly evident that state of art technologies (mobile phone banking) offer immense potentials for banks to redefine their processes, re-position themselves as agile, fleet-footed organizations and enable them to achieve their strategic and financial imperatives in cost effective manner. As illustrated in the research, financial success in banking industry is dependent on the potential of new technology and alignment to fully leverage the technology capabilities. The finding of the study can be summarized or concluded as follows:

5.2.1 Background and demographic characteristics of respondents

A total sample of 150 customers participated in the study. 77 (51.3%) of the participants were male and 73 (48.7%) being female. Most of the respondents had higher education level, with the highest being diploma 38%, followed by graduate 37.33%, postgraduate level 14% and secondary level 10.67%.

121 (80.7%) of the respondents were using mobile phone in accessing banking services while 29 (19.3%) didn't use it.

5.2.2 Current information system securities in mobile phone banking

The study finds outs that 54.8% of the respondents indicate that their bank uses PIN as a security authentication of their accounts, the least method of security used was limitation on number of transaction (2.9%). This limits fraudsters from getting to withdraw high amounts of money from transactions by confirming first with the account holders through alerts sent to their mobile phones. On these methods, the 121 respondents who are using mobile phone banking, 42% were satisfied while 13% were unsatisfied with the current information system securities. This shows that other methods can be deployed to enhance the current information system securities.

5.2.3 Baseline information on mobile phone banking technologies (Mobile Data)

The study revealed that changes in support systems have been a vital in provision of mobile phone banking services. The banks have deployed SMS 65.6% as mobile data technology; this has been true with the fact that most customers own mobile phones that can handle SMS services. The usage of the other mobile data (EDGE, WAP, GPRS, 3G services) is at low percentage because some of the customer's phones are not compatible with the new mobile data technologies.

5.2.4 Enhanced information system security for mobile phone banking

The study found out that based on the number of those using mobile phone banking services, 42% were satisfied but they still faces a challenge; lack of security and confidentiality (30.3%) therefore the respondents suggested further enhancement of information system security. 16.7% were of the view of biometric methods to be

deployed in provision of mobile phone banking services as each human being has a unique biometric identification. From the analysis, when this new method of authentication is deployed, it will help in time saving; easy access of bank information, less queues in bank and it will facilitate real time access of customer money.

5.3 Recommendations

The existing information system security within the mobile phone banking business model as established by this study are still not effectively implemented. There is need for stakeholders to play an effective role in assisting the banks in necessary professional and technical assistance towards the implementation of these opportunities. The stakeholders especially the mobile phone services providers and developers should provide more avenues on data support systems to the banks apart from the use of SMS, which is the most used technical at the moment. The developers will help in coming up with support systems that are compatible in all the mobile phones.

Furthermore as recommended by the respondent in the use of biometric methods as shown on the table below, mobile phone software developers can seize this opportunity by coming up with simple biometric methods that are compatible with the mobile phones.

RECOMMENDATIONS TO EXISTING MOBILE PHONE BANKING SERVICES		
	Frequency	Percent
No ideas	90	60.0
Biometric methods	6	4.0
Educate customers on mobile phone banking	12	8.0
Employ qualified personnel	5	3.3
Government policy	3	2.0
Improve confidentiality &security	7	4.7
Minimize Number of entering password	3	2.0
Mobile phone portability	6	4.0
Tracking system	8	5.3
Use codes n passwords	10	6.7
Total	150	100.0

Source: researcher, 2012

As indicated on the table above, it's paramount for banks to educate their customer on the use of mobile phone banking since most customers were not aware on the provision of these services by their banks.

Since most of the respondents were not 100% secure with the use of mobile phone banking, banks should device security and fraud measures that can build more consumer confidence e.g. use of different PIN numbers and minimize the number of entering the password.

There should be continuous training on bank staff on the use of mobile phone banking as they can be good agents of selling the new banking business model.

REFERENCES

Central Bank of Kenya (2010), Bank Supervision Annual report 2010 (http://www.centralbank.go.ke/downloads/bsd/annualreports/bsd2010.pdf)

Communication Commission of Kenya (2010), 2nd Quarter October-December 2010/2011. (http://www.cck.go.ke/resc/statistics/SECTOR_STATISTICS_REPORT_Q2_2010-11_x2x_x3x_x2x.pdf)

C-operative bank of Kenya http://www.co-opbank.co.ke/ Accessed 25th February 2010.

Dawson, J. (2005). *"Mobile banking with cell phones" An innovation tool for grassroots mobilization.*

Donner, J. (2007). "*Customer acquisition among small and informal businesses in urban India: Comparing face to face, interpersonal, and mediated channels"* The Electronic Journal of Information Systems in Developing Countries, 32(3), 1-16.

Equity bank http://www.equitybank.co.ke/products/ Accessed 25th February 2010

Farid. A. Amer, (2009) "*Mobile phone Security Challenges*" financial journal (V6, 2009)

Gartner Group, (2006). *"Customer Adoption of tele-banking technology: the case of Saudi Arabia. International Journal of Bank Marketing".* Vol. 19 (5), pp 191-200.

Goldstuck, A. (2004). *"The Future of Mobile Financial Services",*

Javelin Strategy & Research (2008). "*Security threats in Mobile phone banking*"

Kandie, P (2003). *"An investigation of customer perception and expectation of quality"* Case study of selected banks in Kenya.

Maurer, B. (2008). *"Retail electronic payments systems for value transfers in the developing world"* Retrieved 27 May 2008.

Mohr, J. (2001), *"Marketing of high-technology products and innovations"*, Upper Saddle River: Prentice Hall.

Morawczynski, O. & Miscione, G. (2008). *"Examining Trust in Mobile Banking Transactions in Kenya: The Case of M-PESA in Kenya"*. Paper presented at the IFIP.

Mugenda, O. and Mugenda, A (1999), *"Research Methods"* revised Edition, Kenya Arts press, Nairobi, Kenya.

Ndemo B. (2009), *"The future of mobile phone banking systems"*, journal paper, ICT stakeholders.

Ndung'u N. (Sept, 2008) *"Launch of Equity mobile banking services"*, CBK governor,http://www.equitybank.co.ke/News/EquityLaunches_Cellphone_Banking.pdf. Retrieved 13 September, 2008.

Njenga, A.D. Kamotho (2009), *"Mobile phone banking: Usage experiences in Kenya"*.

Ochuma, E. (2007), *"An analysis of the State of Mobile Phone banking in Kenya": A case of Selected Banks in Kenya* (Unpublished).

Odinga, B. (2005) *"Factors Influencing Adoption of Electronic Banking By Commercial banks in Kenya"* (Unpublished).

Porteous, D. (2007). *"Just how transformational is mobile banking?"* Retrieved 10 January, 2008, from http://www.finmarktrust.org.za/accessfrontier/Documents/transformational_mbanking.pdf

Sing, S et al (2002). "*Dynamics of Innovation in E-banking*" Gdarisk. Poland.

Touré, H. (2010), "*United Nations International Telecommunications Union (ITU)*", financial journal (V76, 2010).

Appendix 1: Letter of Introduction to the Bank

Alex Musumbi Wambua,
University of Nairobi,
Extra Mural Studies,
Nairobi.

Dear Respondent,

RE: ENHANCING INFORMATION SYSTEM SECURITY IN MOBILE PHONE BANKING SERVICES IN KENYA

I am a Post graduate student at University of Nairobi undertaking the above research.

This is to request you kindly to fill in this questionnaire by responding to the questions concerning your financial institution. The information gathered shall be treated with confidentiality and will not be used for any purpose other than those outlined here.

Thank in advance for your kind support.

Yours faithfully,

Alex Musumbi
(Researcher)

QUESTIONAIRE FOR BANK CUSTOMERS

This questionnaire is meant to collect information on "*Enhancing Information System Security in Mobile Phone banking Services in Kenya*". The information gathered shall be treated with confidentiality and will not be used for any purpose other than those outlined in the research. Kindly answer the questions to the best of your knowledge.

Section A: Background Information

1. Gender
   a. Male [ ]
   b. Female [ ]
2. What is your highest Level of education
   1) postgraduate level [ ]
   2) Graduate level [ ]
   3) College or Diploma level [ ]
   4) Secondary level [ ]
   5) Others (please Specify).....
3. What type of account do you hold in your bank?
   1) Saving account [ ]
   2) Current account [ ]
   3) Salary account [ ]
   4) Business account [ ]
   5) Others (please Specify).....
4. Do you use mobile phone banking services?
   1) Yes [ ]
   2) No [ ]
5. If yes, for how long have you used this service?
   1) Less than a year [ ]
   2) Between 1-3 years [ ]
   3) Between 4-7 years [ ]

4) Above7 years [ ]

6. How did you know about mobile phone banking in your bank?
   a) Newspaper and magazines [ ]
   b) From friends, relatives or neighbours [ ]
   c) Through TV and radio adverts [ ]
   d) Though a bank staff [ ]
   e) Bank brochures and forms [ ]
   f) Others (please Specify).....

Section B: Current Information System Security in Mobile Phone Banking

7. Which of the following information system security are implemented by your bank in authenticating and authorizing bank customers' accounts?
   a. Use of PIN numbers [ ]
   b. Use of SMS [ ]
   c. Use of Email [ ]
   d. Limit in the number of transactions [ ]
   e. Others (please Specify).....
8. How would you rate the adequacy of the existing mobile phone banking system security in your bank
   1) Very adequate [ ]
   2) adequate [ ]
   3) inadequate [ ]
   4) Very inadequate [ ]
   5) Not able to rate [ ]
9. How would you rate the level of mobile phone banking efficiency in provision of banking services by your bank?
   1) Very efficient [ ]
   2) Efficient [ ]
   3) Inefficient [ ]
   4) Very inefficient [ ]
   5) Not able to rate [ ]

Section C: Information on Mobile Phone Banking Technologies

10. Which of the following services are you aware of in mobile phone banking?

    a. Top up airtime [ ]
    b. ATM withdraw or Salary credit advice [ ]
    c. Fund transfers and commercial payments [ ]
    d. Utility bills payment [ ]
    e. Order for statement [ ]
    f. Real time stock quotes or forex rates enquiry [ ]
    g. Stop Cheque or payments instructions [ ]
    h. Loan approval or repayment notification [ ]
    i. Others (please Specify).....

11. Have you ever used any of the above mentioned services

    1) Yes [ ]
    2) No [ ]

12. If yes, which service a. [ ] b. [ ] c. [ ] d.[ ] e.[ ] f.[ ] g.[ ] h.[ ] i.[ ]

13. Where do you conduct the following services? *Please tick the appropriate box*

	POS	**Bank**	**Phone**
a. Pay utility bills	[ ]	[ ]	[ ]
b. Buy or top up airtime	[ ]	[ ]	[ ]
c. Check account balance	[ ]	[ ]	[ ]
d. Transfer money between a/c	[ ]	[ ]	[ ]
e. Electronic money transfer	[ ]	[ ]	[ ]

14. What of the following mobile data service do you make use of when transacting via mobile phone banking?

    a. SMS [ ]
    b. WAP [ ]
    c. EDGE [ ]
    d. GPRS [ ]
    e. 3G service [ ]
    f. Bluetooth service [ ]

g. Others (please Specify).....

Section D: Enhanced information system security for mobile phone banking

15. How would you rate your level of satisfaction with the system security of the mobile phone banking service?

1) Very satisfied [ ]
2) Satisfied [ ]
3) Unsatisfied [ ]
4) Very unsatisfied [ ]

16. What benefits do you derive from utilization of mobile phone banking services?

a. Real time access to my money [ ]
b. Easy access to banking information [ ]
c. Time saving [ ]
d. Less queues in banks [ ]
e. Others (please Specify)

.....

.....

.....

17. To what extent would you agree or disagree with the following statement as relates to Mobile phone banking service. ***Please tick as follows;1=strongly agree,2=agree, 3=Neutral, 4=disagree, 5=strongly disagree.***

		1	2	3	4	5
a)	Mobile phone banking is the way to go in future					
b)	With mobile phone banking my money is secure					
c)	Mobile phone banking makes banking more affordable					
d)	Mobile phone banking is confusing to use					
e)	Mobile phone banking can be trusted if backed by cell phone firms					
f)	Mobile phone banking can be trusted if backed by bank					

18. Which of the following challenges do you face when using mobile phone banking services?

    a. Lack of Security and confidentiality [ ]
    b. Lack of knowledge on the usage [ ]
    c. Fast changes in technology [ ]
    d. System breakdown [ ]
    e. Delay in system response time [ ]

19. What other challenges do you face when using mobile phone banking services?

    .....

    .....

20. What other information system security would want to see enacted to help in more secure provision of mobile phone banking services?

    .....

    .....

    .....

21. What recommendations would you make to help enhance Information System Security in Mobile Phone banking Services in Kenya?

    .....

    .....

    .....

    .....

Appendix 1V: Research Budget

Activity	Quality	Total cost (Kes)
Typing, printing and binding proposal	6 copies@300	1,800
2 Research Assistants Allowance	2@7000	14,000
Materials:		
Photocopy papers	3 reams @600	1800
Ball pens	10@15	150
Full scaps	1 ream @300	300
Travel expense:		
Principal investigation	20 days@400	8,000
2 Researchers	2 (20 days@400)	16,000
Data entry and analysis		10,000
Report preparation:		
Compilation of report		2000
Typing		3000
Photocopying of final project	6 copies @500	3000
binding report	6 copies @ 500	3000
Total		**63,050**

Appendix V: Time Schedule

Phase	Description	Month				
		June(2012	June(2012	June(2012	June(2012	June(2012
I	The Pilot Study					
II	Data Collection					
III	Data Coding					
IV	Data Analysis					
V	Report Writing & Compilation					
VII	Presentation					

Appendix 111: List of All Commercial Banks in Kenya

Data as at 04.03.2011: Source: Central Bank of Kenya

1. African Banking Corporation Ltd.
2. Bank of Africa Kenya Ltd
3. Bank of Baroda (K) Ltd
4. Bank of India
5. Barclays Bank of Kenya Ltd
6. CFC Stanbic Bank Ltd
7. Chase Bank (K) Ltd.
8. Citibank N.A Kenya
9. City Finance Bank Ltd
10. Commercial Bank of Africa Ltd
11. Consolidated Bank of Kenya Ltd
12. Co-operative Bank of Kenya Ltd
13. Credit Bank Ltd
14. Development Bank of Kenya Ltd
15. Diamond Trust Bank (K) Ltd.
16. Dubai Bank Kenya Ltd
17. Ecobank Kenya Ltd
18. Equatorial Commercial Bank Ltd.
19. Equity Bank Ltd
20. Family Finance Bank Ltd
21. Fidelity Commercial Bank Ltd
22. Fina Bank Ltd
23. First community Bank Limited
24. Giro Commercial Bank Ltd
25. Guardian Bank Ltd
26. Gulf African Bank Limited
27. Habib Bank A.G Zurich
28. Habib Bank Ltd.
29. Housing finance Ltd
30. Imperial Bank Ltd
31. Investment & Mortgages Bank Ltd
32. Jamii Bora Bank Limited
33. Kenya Commercial Bank Ltd
34. K-Rep Bank Ltd
35. Middle East Bank (K) Ltd
36. National Bank of Kenya Ltd
37. NIC Bank
38. Oriental Commercial Bank Ltd
39. Paramount Universal Bank Ltd
40. Prime Bank Ltd
41. Southern Credit Banking Corporation Ltd
42. Standard Chartered Bank (K) Ltd
43. Trans-National Bank Ltd
44. Victoria Commercial Bank Ltd
45. UBA Kenya Limited