الآية

قال تعالى:

(وأن ليس للإنسان إلا ما سعى

وأن سعيه سوف يرى ثم

يجزاه الجزاء الأوفى)

المستخلص

إستخدام الهاتف النقال في الدفع الإلكتروني للمعاملات النقدية أصبح ينمو بشكل متزايد في جميع أنحاء أفريقيا مما ساعد على إحداث ثورة في الاقتصاد النقدي السائد في هذه القارة أن يكون إلكترونيا. مع زيادة استخدام خدمات الدفع الإلكتروني عبر الموبايل وزيادة إستخدام الأعمال المصممة في هذا الجانب كل يوم، لا بد من تصميم نهج شامل لأمن خدمة الدفع عبر الموبايل المحمول من شأنه أن يقلل مخاطر الأمن ومنع الإحتيال.

التهديد المتزايد لمخاطر الإحتيال كلف بعض مزودي خدمة الدفع عبر الموبايل الملايين من الدولارات. لذلك هذا البحث، يدرس التدابير التي يستخدمها مشغلي الشبكات المتنقلة التي توفر خدمات الدفع الإلكتروني عبر الموبايل لمنع مخاطر الإحتيال.

وجاء هذا البحث لدراسة حالة الأمن للدفع الإلكتروني عبر الهاتف النقال في السودان واستخدام البيانات الكمية والنوعية التي تم جمعها من خلال الاستبيانات والمقابلات الشخصية من الموظفين الرئيسيين لمشغلي شبكة الهاتف المحمول (MNO) .

وتم إستخدام حزمة الإحصاء التطبيقي (SPSS) لإستخلاص النتائج والتقارير المتعلقة بالبحث ،

وقد أشارت النتائج الرئيسية للبحث أنه يوجد ارتباط مباشر بين حماية الهاتف المحمول وأمن عملية الدفع الإلكتروني وأيضا تم التعرف على أن واحدا من أهم الأسباب الرئيسية المؤدية للإحتيال على المستهلكين هو التشارك في رقم (PIN).

من خلال البحث يقترح أن مزود الخدمة يجب أن يعطي نصائح أمنية لمستخدمي خدمة الدفع الإلكتروني عبر الموبايل على الأقل مرتين في السنة من خلال خدمة الرسائل القصيرة (SMS) لتنبيههم وتمليكهم الطرق السليمة لتعزيز أمن الهواتف النقالة.

Abstract

Mobile money usage for transactions is steadily growing across Africa with the potential to revolutionize the cash-dominant economy of this continent to be cashless. With the increased use of mobile money services and number of business use cases designed each day, it is imperative to design a holistic approach to mobile money security that will reduce security exposures and prevent fraud, as some mobile money service providers have lost millions of dollars to this growing threat. This research, therefore examines the measures that mobile network operators providing mobile money services can employ to prevent fraud.

The research was a case study of mobile money security in Sudan and used qualitative and quantitative data collected through questionnaires and structured interviews of key staff of the mobile network operator (MNO)

The Statistical Package for the Social Sciences (SPSS) was used to capture the questionnaire data and to produce the necessary reports.

Some of the main findings of this research include the general perception that there is direct linkage between mobile phone protection and mobile money security. It was further identified that one of the major causes of consumer driven fraud is PIN sharing. In addressing mobile money fraud, it is suggested that the service provider should give mobile money security tips to the users at least twice in a year through short message service (SMS) to alert them of ways to enhance the security of their mobile phones.

Acknowledgments

First, I give thanks to God for protection and ability to do work. And I cannot find the words to express my special gratitude to all the people who have generously supported me throughout the stages of writing this thesis.

I really want to express my utmost gratitude to my Supervisor Dr.Osama Ahamed Ibrahim for his patient guidance and help.

I am thankful to Sudan University of Science and Technology, college of graduate studies and scientific research, computer department for making provision me the opportunity to study with them.

Finally, a big thank you to my family for the support provided.

Table of Contents

List of Tables

List of Figures

Table of abbreviations

ATM	**Automated Teller Machines**
DSTK	**Dynamic Sims Toolkit**
E-commerce	**Electronic Commerce**
GSM	**Global System for Mobile**
M-ecommerce	**Mobile Electronic Commerce**
M-money	**Mobile Money**
MM	**Mobile Money**
MNOs	**Mobile Network Operators**
M-Payment	**Mobile Payment**
NFC	**Near-Field Communication**
SIM	**Subscriber Identity Module**
SMS	**Short Message Service**
STK	**SIM Toolkit Application**
UMTS	**Universal Mobile Telecommunications System**
USSD	**Unstructured Supplementary Service Data**

CHAPTER ONE
INTRODUCTION

1. Introduction

This chapter examines Background of the study, the Problem statement, as well as the research questions that the researcher sought to answer, and Research Objective, It also highlights the Scope of the research work, and Expected Contribution as well as Methodology and lastly the organization of the research.

1.1. Background of the study:

Recent developments of communications technologies and business models raised concerns about mobile payment systems in terms of usability and security.

Rising smart mobile devices with variety of usage and privacy and easy access to communication protocols have provided the potentials for growing development of mobile commerce. Furthermore, new business models in daily activities have increased the need of comprehensive mobile e-commerce system.

Mobile payment is the use of telecommunication platforms or networks by mobile phone Subscribers to perform banking services. In short, mobile money enables subscribers to bank directly from their mobile phones without physically being in a financial institution to pay bills, receive money, and transact business all through virtual mobile accounts known as mobile money wallets. The use of mobile money for transactions has been steadily growing across Africa, positioned as the next “big thing” to revolutionize the cash dominant economy of Africa. A recent survey revealed that there are 20 countries in which more than 10% of adults used mobile money at some point in 2011, of which 15

are in Africa. For example, in Sudan, Kenya, and Gabon, more than half of adults used mobile money[1]. From this survey, it is evident that mobile money has become one of the "must offer" services for telecom companies in Africa. For example the top ranked telecommunication companies in Sudan – MTN, Zain and Sudani all offer mobile money services to their clients and usage statistics are increasing daily. The mobile payment refers to payment services operated under financial regulation and performed from or via a mobile device.

Internet environment and mobile devices make merchants and customers around the world connected. With the information technology, the mobile payment can simplify payment procedure tremendously. Users of mobile payment can get rid of the limitation from real currency and geography.

Therefore, a variety of security risks will emerge in mobile payment because of the huge potential market. Since transactions and currencies are stored and transmitted in the mobile and internet environment, security of mobile payment has been the pivotal factor in it.

1.2 Problem statement:

With the growing use of mobile payment services and new use cases arising, it has become important to research into the security practices of mobile network operators and users to ensure mobile payment is secured, to prevent fraud, Fraud is risk of financial loss for one of the parties involved in a payment transaction arising from wrongful or criminal deception. The risk that a transaction cannot be properly completed because the payee does not have a legitimate claim on the payer .There are risks that exist

in every mobile money service around the world, such as the potential theft of customer information or manipulation in e-money reconciliation.

1.3 Research question:

What measures can be put in place to enhance mobile money security in order to prevent fraud.

It is important to identify the security practices of the service provider and the user needed to ensure a secured mobile money service and to prevent fraud by putting some Hypotheses to prove Research question as the following:

i. There is no statistically significant relationship between the variables of type, age, occupation and the time period with the measures can be put to enhance mobile money security.
ii. There is a statistically significant relationship between Uses of mobile money and fraud.
iii. There is a statistically significant relationship between the lacks of confidentiality (sharing of PINs) in mobile phone and fraud in mobile payment.
iv. There is a statistically significant relationship between improving the security activities of the users and reducing risk of fraud.
v. There is a statistically significant relationship between a secret mobile phone and mobile money protection.

1.4 Research Objective:

i. This research put up to provides some insight into the security Controls and practices implemented by the MNO to secure the mobile money service.
ii. Identify risk areas.
iii. Put some Measures to improve security and to prevent fraud.

1.5 Research Scope:

There are two categories of mobile money users -registered and non-registered. However, this research is focused on only the registered users, who use the service from their mobile phones. There are three telecommunication companies in Sudan out of which three provides mobile money services; however this research is limited to only one of them.

1.6 Expected Contribution:

i. Minimize the occurrence and cost of fraud within an organization and individuals.
ii. The mobile money subscriber's awareness of their responsibility towards the security of the service on their mobile phone could have influence on some of the actions they take in protecting their mobile money wallet.

1.7 Methodology:

The methodology employed for the research and includes research design, strategy and approach. It also involves Case study Company and population and sampling processes.

Research Design:

Research designs come in the following three forms - exploratory, descriptive or explanatory. However, the sequence of these research types by purpose is progressive, from exploratory research to descriptive research to explanatory research.

Research strategy:

There are various forms of research strategies available for a researcher to use; these are survey, case study and action research.
The research strategy chosen for this research work is a case study.

Research approach:

Research approach is collecting, aggregating and analyzing data by using graphs and figures.

Case study Company:

A case study company was identified that was willing to support the research on the basis of anonymity because of the need to prevent security exposure due to the research work.

Population and sampling process:

Deliberate convenient sampling was employed by selecting ten contact centers from the capital of Sudan. The head of these contact centers were given the questionnaires and were administered to any customer that walks in and uses mobile money on their phones.

The Statistical Package for the Social Sciences (SPSS) was used to capture the questionnaire data and to produce the necessary reports.

Table 1-1 Summary of the research methodology

Approach		Types And Chosen	
Research design:	Exploratory	Descriptive	Explanatory
Research strategy:	Survey	Action	Case study
Research approach:	Quantitative	Qualitative	
Data source:	Observation	Personal interview	Mailing questionnaire
Sampling:	Deliberate	Sequential	

1.8 Organization of the research:

The remaining work is organized under the following chapters: chapter 2 is focused on the literature review on the research topic. While chapter 3 is based on data presentation Chapter 4 covers the findings and discussions of the study. The last chapter is devoted to conclusions, recommendations and suggestion on further studies.

CHAPTER TWO
LITERATURE REVIEW

2. Literature Review

In this chapter, literature on mobile payments, m-ecommerce or e-commerce, general uses of mobile money, security of mobile phones, mobile money and m-payment services, the security of mobile phones, mobile money and m-payment systems is reviewed. Also included in the review are other scholarly works directly related to this research topic?

2.1 Mobile Payments, M-Commerce or E-Commerce:

A mobile payment or m-payment is any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services[2]. Mobile devices in this case include mobile phones, tablets or any other devices that are able to connect to mobile telecommunication networks and enable payment to be made[3]. Depending on the channels the MNO makes available for providing the service, a consumer may be limited to the use of mobile phone only or all the other mobile devices aforementioned. M-Payments use what is called e-money or m-money is mobile money (m-money) any different from Electronic Money (e-money)? E-money has been described as a broader concept that refers to payments made using the near -field communication (NFC) contactless cards, credit cards, prepaid cards, debit cards, automated teller machines (ATM), as well as mobile phones. Mobile money is seen as a subset of e -money that refers to financial services and transactions made using technologies integrated into mobile phones. These services may or may not be directly tied to a personal account, or linked to ATM, prepaid, debit or credit

cards[4].The rapid growth in the use of mobile phones and the lack of access to formal bank services in most African countries are contributing factors t o the rapid growth and the use of mobile money services in most parts of the continent. More than one billion customers in developing markets have access to a mobile phone but do not have a formal bank account[5].

2.2 General Uses of Mobile Money:

The use of mobile money services is gradually becoming part of people's day-to-day transactions, and is safe to say that it is making money transfer services quite easier and at cheaper cost. In Sudan for example, one can deposit money in his/her mobile money wallet and transfer this to either mobile money subscribers or non-mobile money subscribers. This reduces the time spent in travelling long distances, queuing at the bank before making a deposit or using unsafe methods such as sending money through bus services for recipients in other towns and villages. Mobile money transfers can be made by pressing few keys on the mobile phone and recipient receives money almost instantly. It can be said that most consumers like the convenience and ease of use of the service for transactions and payments from their mobile phones; as a result, the market for m-payment seems to be growing rapidly[6]. Mobile money is a promising innovation for driving mobile payment and the cashless society of a large percentage of African countries, including Sudan. The following are the main uses of mobile money:

2.2.1 Funds Storage:

Some mobile money services allow their users to store funds either through a bank account held with a traditional bank or an account held with the mobile network operator[7]. In Sudan, some mobile money subscribers can transfer money from their traditional bank account to their mobile wallet and vice versa. This implies mobile wallets could also become a medium of 'holding' funds and not only the traditional bank accounts savings.

2.2.2 Transfer – Domestic and International:

Domestic money transfer is funds remitted from one person to another where both parties are in the same country[7]. In Sudan, all the mobile money service providers – MTN, Zain and Sudani offer this money transfer service to enable people transfer money to others at their convenience. Mobile money transfer could be carried out by either a registered user or non-registered user to either parties. A transfer from a registered user is done by debiting his or her mobile money wallet of funds to be transferred to the mobile money recipient or generating a token and secret code, which is sent to a non registered user to use in withdrawing the money from a merchant or the bank. Anon-registered user may carry out mobile money transfer by using the services of a merchant or MNOs service centre. In Sudan, one cannot transfer funds across networks; for example, a user cannot transfer funds from MTN Sudan mobile money service to Zain mobile money service.

2.2.3 Payments for Goods and Services:

Mobile payments can be used to pay for items purchased from shopping malls and merchants. At the point of sales, payment is done by crediting the mobile money accounts of shop owners which reflects almost instantly. However, in Sudan since no transaction can be performed across networks, such payments can only be made if both the merchant and the buyer are using the same mobile money service.

Mobile money service also enables users to pay for basic utility services such as electricity, water, DSTV subscriptions, which provides greater convenience and efficiency for consumers of these services[7]. Using mobile money to pay for utilities is one of the services in Sudan that is available on all the mobile service providers' list of services rendered. Using mobile money to pay for utilities can be done in either the offices of the utility company, at banks, at the outlets of specialized payments networks, or at retail shops that have an agency agreement with these utility companies[8]. By the use of mobile money, consumers can easily pay utility bills and avoid the inconvenience of traditional methods of payment. Mobile money could also be used for public transport payment[9], though not currently available in Sudan.

2.3 Security of Mobile Phones, Mobile Money, M -Payment Services:

Mobile payment is enabled by a variety of emerging technologies, many of which are still maturing[10]. These technologies are needed to address various payment industry needs which includes secure authentication infrastructure on mobile devices, secure transmission

infrastructure for wireless payment, trust/validation directories and virtual "wallets" stored on a mobile device or accessible over a network[11].

Despite all the technological advancement in mobile technology, security is still an important issue with M-payment. For example, near-field communication (NFC) has been identified to have the vulnerability of a man-in-the-middle attack; in which an attacker could intercept exposed information during the communication with the reader, which is usually within 10cm radius[12]. Basic phones with mobile money capability could be described as GSM (Global System for Mobile) compatible phones with embedded services such as SMS and USSD[13]. There is however, no end-to-end security for SMS, protection ends in the GSM or UMTS (Universal Mobile Telecommunications System) network. Furthermore, unstructured supplementary service data (USSD), has no separate security properties; instead it relies on the GSM/UMTS signaling plane security mechanism (just like SMS). It is further argued that the security mechanisms of authentication, message integrity, replay detection and sequence integrity, proof of receipt and proof of execution, message confidentiality and indication of security mechanisms exists; however, it depends on the applications whether these security mechanisms are implemented and whether their cryptographic strength is sufficient[14].

2.3.1 Mobile Money Fraud and Scams:

Fraud in the context of mobile money can be said to be the intentional and deliberate actions undertaken by players in the mobile financial services ecosystem, aimed at deriving financial

gains, denying other players revenue or damaging the reputation of other stakeholders. The occurrence and prevalence of fraud is dependent on the stage of implementation of the mobile money service. Thus, as deployment evolves, the types of fraud evolve with it[15].

Key enablers of mobile money fraud include maturity of the mobile money services, weak or non-standard processes, cultural issues, lack of compliance monitoring [15] and any new value added services not thought through properly, for example, the post-paid scheme in which the transaction is applied to the user's phone bill to be paid later[16].

2.3.2 M-Payment, E-Commerce and User Perception about Security:

Many studies on security in the information systems arena focus mainly on technical and implementation related issues. However, most consumers only perceive security from the subjective realm[11], which is usually incubated through advertisements and public information[17]. Security and trust are among the key considerations for adoption of M-Payment systems. For example, in a focused group study [18] into mobile payment adoption has shown that lack of perceived security is one reason for inhibition to adoption of the solution. Addressing this inhibitor to the adoption of mobile payment solutions or any electronic payment systems means security must be extensively addressed; but security from whose point of view, the service provider or the user?

The concept of security has been split into two dimensions by researcher, objective and subjective security. Objective security is a

platform or applications security based on concrete technical characteristics[19]. These security characteristics are mainly the concerns of security professionals, system owners and backend IT staff. It has been argued that not every customer is able to comprehend or evaluate the technicalities of objective security[20].

2.4 Related Work:

Researcher has performed some studies which have findings relevant for this research. The following are some of these important findings:

a. **Uses of Mobile Money:** A 2012 survey conducted among 2,980 households in Tanzania revealed that the general perception about mobile money usage by registered users both in the urban and rural areas is that the service is for sending or receiving money .Interestingly, 55% of nonusers also think the service is for sending or receiving money only. Despite the general believe that mobile money is used for transfer and receiving money, it is the second most popular means of savings in Tanzania and in Kenya[19]. Aside using mobile money for remittance purposes, in Tanzania 14% of the 2,980 households surveyed use it for non-remittance purposes such as school fees payments, government fees and taxes, utility bills, and salaries. This is followed by 12%of users who use the platform to purchase goods and services in shops[9]. The general uses of mobile money in the middle to high income countries such as Brazil, Sri Lanka, Thailand and USA are for transport fare payment. Mobile money transfers (P2P) is considered the least usage[9].

b. **Educational background of mobile money users:** From a study conducted in Kenya[21], it was concluded that mobile money users

are more likely to be literate than non-users. This was also confirmed in another study conducted in Tanzania, which revealed that the more educated individuals are, the more likely they are to use m-money. Out of the 2,980 households surveyed, 65% had primary education, 22% had secondary education while 14% had no formal education.

c. **Sharing of mobile money PINs:** The Tanzanian survey further revealed that 33% of households shared their mobile money PIN (password) with other persons. One-third reported sharing their PIN "always," and another quarter reported sharing their PIN "very often." Of those who shared their PINs, 55% do so with agents while 45% shared with close relations such as spouse, siblings and friends. Furthermore, 78% of those who shared their PINs also indicated they do not know how to change their PIN[9]. This Tanzanian survey further revealed that 14% of mobile money users might have carried out m-money transactions with the help of the agent and could have shared their PINs with the agent.

d. **Fraud situations in mobile money:** In another study in Kenya, [4] it was concluded that though mobile money operators had company and industry principles guiding them, they have not been implemented and fully adopted, leading to the possibility of technological savvy people using their technologies to achieve their illegal targets of fraud and scam. For example, an average of 18% of respondents in the 2,980 household survey in Tanzania have had money stolen from their m-money account due to fraud or a scam [9]

CHAPTER THREE
DATA PRESENTATION

3. **Data presentation**

Questionnaires and interview were used as the sources of collecting data for this research work. This chapter presents the findings of the data from the questionnaires and interviews conducted.

Data presentation from questionnaire:

The researcher planned to use 50 questionnaires from the capital of the country, all 50 were retrieved, and Data presented here mainly covers demographic information of respondents, duration of mobile money usage, fraud and actions susceptible to fraud, and mobile phone security and mobile money security.

R E L I A B I L I T Y A N A L Y S I S - S C A L E (A L P H A)

Degree of internal consistency and reliability

Scale: all variables

Case processing summary

	Number	Percent
Valid	50	100.0
Excluded	0	0
Total	50	100.0

Reliability statistics

Alpha	N of items	N of Cases
. 958	34	50

The above table display truth and the internal consistency using SPSS program for test the questions and items study, alpha value reached to (0 . 958) This means the degree of validity and reliability of this study is high and this enables us to analyze data and get correct and truthful results.

Analysis based on Likart Scale:

A method of ascribing quantitative value to qualitative data, to make it amenable to statistical analysis. A numerical value is assigned to each potential choice and a mean figure for all the responses is computed at the end of the evaluation or survey. Used mainly in training course evaluations and market surveys, Likert scales usually have five potential choices (strongly agree, agree, neutral, disagree, strongly disagree) but sometimes go up to ten or more as below :

Table 4-1: Likert scales have five potential choices

Value	Weighted average
Strongly agree	From 5.00 to 4.20
agree	From 4.19 to 3.40
Neutral	From 3.39 to 2.60
Disagree	From 2.59 to 1.80
Strongly disagree	From 1.79 to 1.00

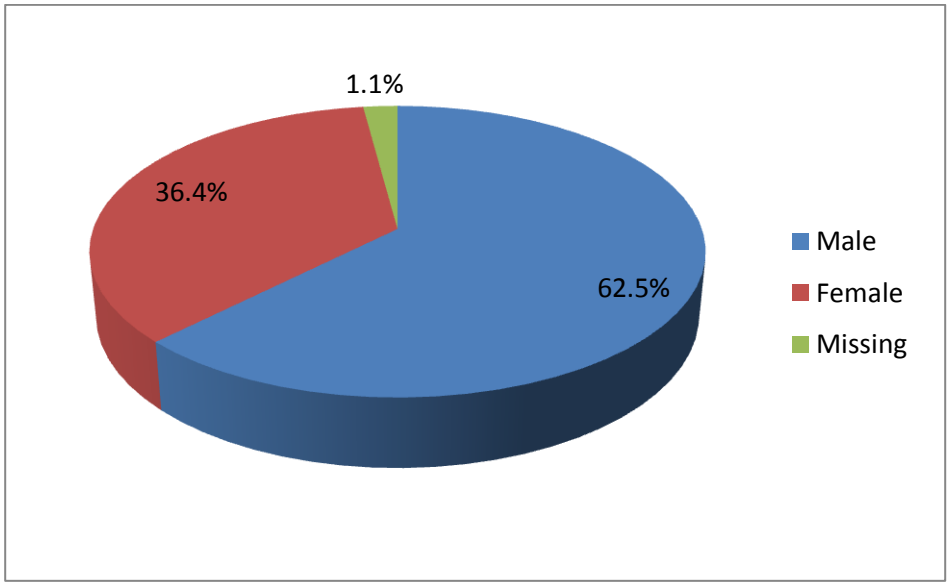
The following are the data collected from the questionnaires:

4.1 Demographic information of respondents:

In all, 62.5% of the total respondents are male, while 36.4% are female.

The Figure (4-1): below shows how to represent Gender of respondents

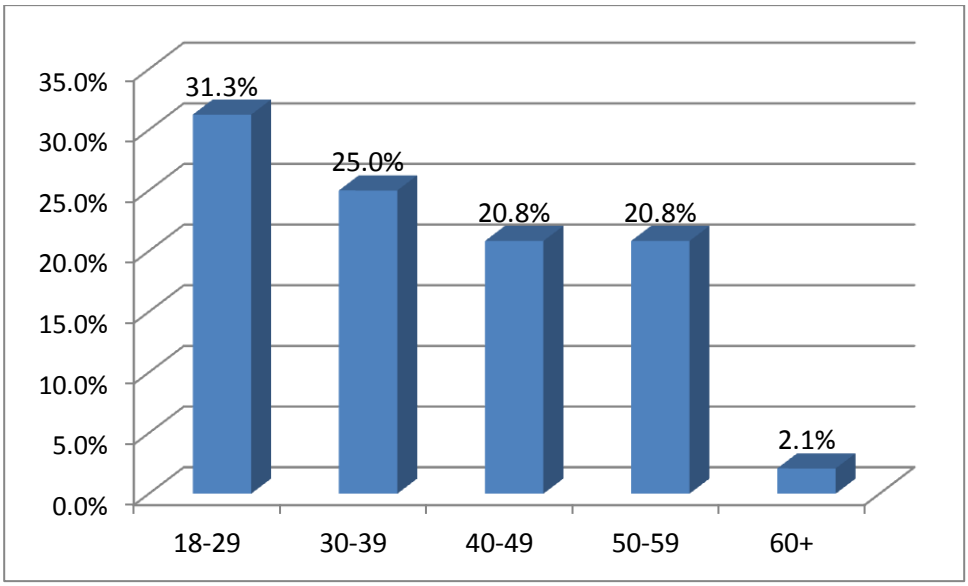
Figure (4-1): Gender of respondents



With regards to the age groups of respondents, 31.3% of the total respondents are between 18 and 29 years, 25.5% are also in the age range of 30 and 39 years, whiles 20.8% are between 40 and 49 years. 20.8% are between 50 and 59 years, latest 2.1% in the age range above 60 years.

The Figure (4-2): below shows how to represent Age of respondents

Figure (4.2): Age of respondents



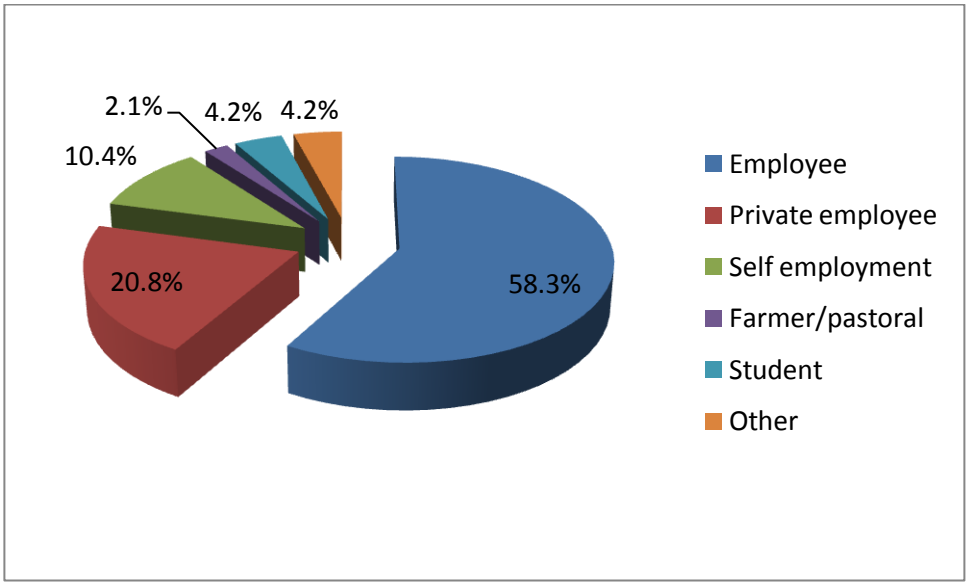
Majority of the respondents, 34%, have Diploma level educational qualification, followed by 33% respondents with a bachelor's degree. Secondary School (SS) level education, those followed by educational qualification and 2ndDegree holders represents 21%, 7% and 5% of total respondents respectively.

Occupation of respondents:

58.3% of the total respondents are Employee, while 20.8% are private employee, and 10.4 are Self employees, 2.1% are Farmer/Pastoral, while 4.2% are Student, latest 4.2% are other.

The Figure (4-3): below shows how to represent Occupation of respondents

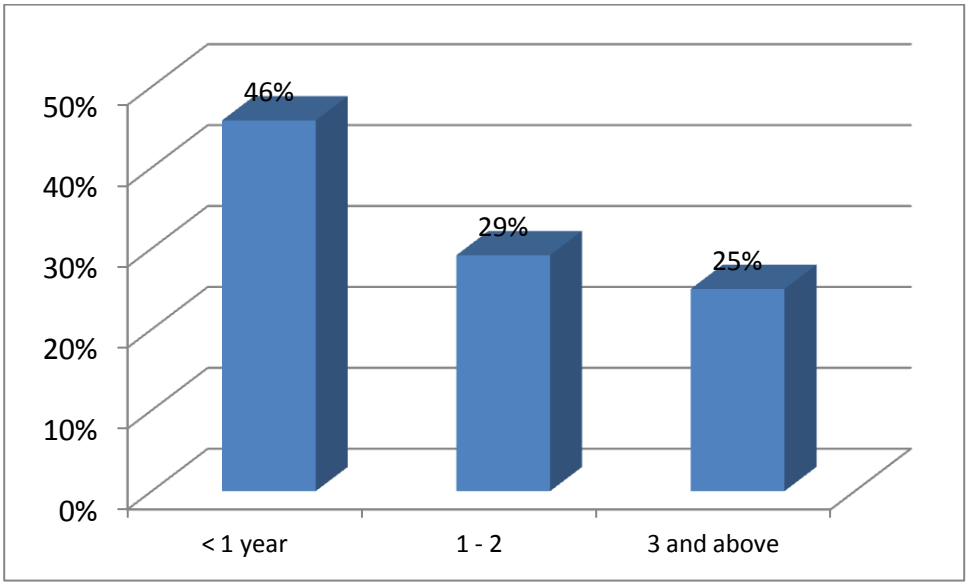
Figure (4-3): Occupation of respondents



The time period of using mobile payment:

The Figure (4-4): below shows how long the respondents had subscribed to the mobile money service.

Figure (4-4): The time period of using mobile payment



4.2 Mobile money usage:

Preferred point of loading money on phone

Table 4-2 preferred point of loading money

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviatio	Result
Company's service centers	Frequency	17	13	10	8	2	50	3.70	1. 216	**Agree**
	percent	34.0	26.0	20.0	16.0	4.0	100.0			
Banks	Frequency	20	10	9	10	1	50	3.76	1.238	**Agree**
	percent	40.0	20.0	18.0	20.0	2.0	100.0			
Peer-to-peer	Frequency	12	32	3	2	1	50	4.4	0.807	**Agree**
	percent	24.0	64.0	6.0	4.0	2.0	100.0			

The above table Display the result of three Options is Agree

From table 4-2 identify the preferred points of loading money on the mobile money wallet of the respondents. The tables show that Mean 4.4 of the respondents prefer the Peer-to-peer to the other sources available, Mean 3.70, 3.76 of the respondents preferred service provider's service centre and Banks respectively.

Table 4-3 various uses of mobile money

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviatio	Result
Pay for utilities	Frequency	8	33	5	2	2	50	3.86	. 881	**Agree**
	percent	16.0	66.0	10.0	4.0	4.0	100.0			
Local money transfer	Frequency	6	39	3	1	1	50	3.96	0.669	**Agree**
	percent	12.0	78.0	6.0	2.0	2.0	100.0			
Pay for goods bought in shops	Frequency	22	15	8	3	2	50	4.4	1.106	**Agree**
	percent	44.0	30.0	16.0	6.0	4.0	100.0			

The above table 4-3 Display the result of three Options is Agree

From Table 4-3 above represents the distribution of respondents for the various uses of mobile money, the table shows that majority of users Mean 4.4 use mobile money for the Pay for goods bought in shops , Mean 3.96 of respondents use mobile money for money transfer, and Mean 3.86 use the service to Pay for utilities.

4.3 Fraud and actions susceptible to fraud:

4.3.1 Mobile money PIN sharing and request:

Table 4-4 have you ever shared your mobile money PIN number?

variable	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviation	Result
	Frequency	6	6	0	30	8	50	2.44	1. 248	**Disagree**
	percent	12.0	12.0	0.0	60.0	16.0	100.0			

The above table Display the result of question is Disagree

The respondents were asked to disclose if they have ever given their mobile money PIN to anyone. The responses obtained, as shown in Table 4-4, indicates that respondents Mean 2.44 have no shared their mobile money PINs.

Table 4-5 has anyone ever requested for your mobile PIN number?

variable	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviation	Result
	Frequency	1	3	3	34	9	50	2.6	1. 818	**Disagree**
	percent	2.0	6.0	6.0	68.0	18.0	100.0			

The above table Display the result of question is Disagree
In response to the question 'has anyone ever requested for your mobile PIN number?' Mean 2.6 of the respondents answered in the negative, as seen in the Table 4-5.

4.3.2 unauthorized transaction:

Table 4-6 has anyone ever transferred money from your mobile wallet

variable	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviatio	Result
	Frequency	2	2	2	21	23	50	1.78	.996	**Strongly disagree**
	percent	4.0	4.0	4.0	42.0	46.0	100.0			

The above table Display the result of question is strongly disagrees

From the Table 4-6, mean 1.78 of respondents experienced mobile money transfer from their wallet without their permission.

4.4 Mobile Phone Security:

The following are responses to the various considerations and actions employed by the respondents to keep their mobile phone secured.

4.4.1 Considerations for buying a mobile phone:

Table 4-7 what users look out for when buying a mobile phone?

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviatio	Result
fashion of the day	Frequency	4	30	8	3	5	50	3.50	1. 074	**Agree**
	percent	8.0	60.0	16.0	6.0	10.0	100.0			
considers security	Frequency	7	35	3	3	2	50	3.84	0.889	**Agree**
	percent	14.0	70.0	6.0	6.0	4.0	100.0			

The above table 4-7 Display the result of three Options is Agree

From Table 4-7 above shows that, mean 3.84 considers security as the major factor in selecting a phone whilst the mean 3.50 base their decision on the fashion of the day. The main consideration for users in buying their mobile phones is the security features.

4.4.2 Concerns for mobile phone users regarding their mobile device security

Table 4-8 Concerns for mobile phone users regarding their mobile security

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviatio	Result
High importance	Frequency	13	30	2	3	2	50	3.98	. 958	**Agree**
	percent	26.0	60.0	4.0	6.0	4.0	100.0			
Moderate importance	Frequency	11	34	4	1	0	50	4.8	0.695	**Agree**
	percent	22.0	68.0	8.0	2.0	0.0	100.0			
Low importance	Frequency	4	6	4	26	10	50	2.36	1.174	**Disagree**
	percent	8.0	12.0	8.0	52.0	20.0	100.0			

The above table 4-8 Display the result of first two Options is Agree and Disagree of last action

Table 4-8 shows several concerns for mobile phone users regarding their mobile device security. It shows that a majority of participants agreed about the importance of the information that they have in their mobile devices. The level „ Moderate importance ‟ was chosen most frequently and mean 4.8 as an important level of the information stored in the participants‟ mobile devices, Next was „ High importance ‟ at mean 3.98 and the lowest was „Low importance‟ at mean 2.36.

4.4.3 What makes a mobile phone secured?

Table 4-9 what makes a mobile phone secure?

variable	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviatio	Result
	Frequency	24	18	3	3	2	50	4.18	1.063	**agree**
	percent	48.0	36.0	6.0	6.0	4.0	100.0			

The above table Display the result of question is agree

From the Table 4-9 above gives the opinion of respondents on what makes a mobile phone secure. It can be seen from this Table that Mean 4.18 of respondents believe passwords/ PINs or pattern provides better security for the mobile phone.

Table 4-10 preferred authentication method by mobile phone users

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviation	Result
Password/PIN	Frequency	30	14	2	4	0	50	4.40	. 904	**Strongly agree**
	percent	60.0	28.0	4.0	8.0	0.0	100.0			
pattern	Frequency	12	26	4	5	3	50	3.78	1.112	**Agree**
	percent	42.0	52.0	8.0	10.0	6.0	100.0			
biometric	Frequency	15	18	5	8	4	50	3.64	1.290	**Agree**
	percent	30.0	36.0	10.0	16.0	8.0	100.0			

The above table 4-10 Display the result of the first Option is Strongly agree and agree of the two last actions

From the Table 4-10 above gives the opinion of respondents on another question in the survey investigated the most preferred authentication method by mobile phone users for the information security of their mobile device. The PIN or password method mean 4.40 was the preferred authentication method, followed by the pattern mean 3.78, while mean 3.64 of the participants agreed that biometric authentication. However, a majority of the participants agreed that PIN or password method authentication will meet their need to protect sensitive information on their mobile device.

4.4.4 Level of protection of privacy that the users require for their information in their mobile devices:

Table 4-11 Level of protection of privacy

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviation	Result
High protection	Frequency	24	18	2	4	2	50	4.16	1.095	**Agree**
	percent	48.0	36.0	4.0	8.0	4.0	100.0			
Moderate protection	Frequency	16	17	4	9	4	50	3.64	1.321	**Agree**
	percent	32.0	34.0	8.0	18.0	8.0	100.0			
Low protection	Frequency	2	5	6	30	7	50	2.30	.974	**Disagree**
	percent	4.0	10.0	12.0	60.0	14.0	100.0			

The above table 4-11 Display the result of first two Options is Agree and Disagree of last action

The table 4.11 illustrates the level of protection of privacy that the users require for their information in their mobile devices. „High protection" was an important level at mean 4.16. The second most important protection level was „Moderate protection" at mean 3.64. „Low protection" ranked last level at mean 2.30.

4.4.5 Actions taken when a mobile phone is lost:

Table 4-12 Actions taken when a mobile phone is lost

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviation	Result
service provider's call center	Frequency	23	18	3	4	2	50	4.12	1.100	**Agree**
	percent	46.0	36.0	6.0	8.0	4.0	100.0			
service provider's service "Mobile Protect"	Frequency	19	18	5	5	3	50	3.90	1.199	**Agree**
	percent	38.0	36.0	10.0	10.0	6.0	100.0			
GPS tracker	Frequency	12	21	10	5	2	50	3.72	1.070	**Agree**
	percent	24.0	42.0	20.0	10.0	4.0	100.0			

The above table 4-12 Display the result of three Options is Agree

From Table 4.12 shows the actions respondents will take in case they lose their mobile phone. As shown, mean 4.12 of respondents assert that they will call the service provider's call center to block the phone. Whereas mean 3.72 will use the GPS tracker to locate the mobile phone, mean 3.90 of respondents will use the service provider's service "Mobile Protect" to block the phone.

4.5 Mobile money security:

This section presents responses on the quest ions: whose responsibility it is to keep the mobile money secured, whether a secure phone makes

MM service secured and the linkage between mobile phone access and risk of exploiting MM service. The following are the responses:

4.5.1 Responsibility to secure mobile money service:

Table 4-13 Responsibility to secure mobile money service

	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviation	Result
shared responsibility of the user and the service provide	Frequency	22	20	3	4	1	50	4.16	.997	**Agree**
	percent	44.0	40.0	6.0	8.0	2.0	100.0			
responsibility of the service provide	Frequency	13	18	8	7	4	50	3.58	1.247	**Agree**
	percent	26.0	36.0	16.0	14.0	8.0	100.0			
personal responsibility	Frequency	5	25	5	9	6	50	3.28	1.230	**Agree**
	percent	10.0	50.0	10.0	18.0	12.0	100.0			

The above table 4-13 Display the result of three Options is Agree

The Table 4-13 gives respondents' views on whose responsibility it is to protect the mobile money service. As can be seen from this table, the respondents assert that the protection of the mobile money service is a shared responsibility between them the users and the service provider, forming mean 4.16 of the responses, that mean 3.28 of the respondents think it is their personal responsibility to protect their mobile money and not the responsibility of the service provider, Finally mean 3.58 of the respondents are of the opinion that it is the sole responsibility of the service provider to protect the mobile money service.

Table 4-14 does secure phone make MM service secured?

variable	scale	Strongly agree	agree	Neutral	Disagree	Strongly disagree	Total	Mean	Std. Deviatio	Result
	Frequency	22	20	3	3	2	50	4.14	1.050	agree
	percent	44.0	40.0	6.0	6.0	4.0	100.0			

The above table Display the result of question is agree

The table (4-14) shows that mean 4.14 of the respondents agree that having a secure mobile phone definitely ensures the safety of their mobile money.

Hypotheses number one:
There is no statistically significant relationship between the variables of type, age, occupation and the time period with the measures can be put to enhance mobile money security.
Variables:
I used Spearman correlation for inspecting the relationship between Age Group and gender with secured phone.

Table 4-15: Spearman correlations Age Group and gender with secured phone

		gender	Age Group	does secure phone make MM service secured
gender	Pearson Correlation	1	.850(**)	-.699(**)
	Sig. (2-tailed)	.	.000	.000
	N	50	50	50
Age Group	Pearson Correlation	.850(**)	1	-.855(**)
	Sig. (2-tailed)	.000	.	.000
	N	50	50	50
does secure phone make MM service secured	Pearson Correlation	-.699(**)	-.855(**)	1
	Sig. (2-tailed)	.000	.000	.
	N	50	50	50

** Correlation is significant at the 0.01 level (2-tailed).

From the above correlation table, there are significant correlations between gender and secured phone.

From the same table we see that no significant correlation between Age Group and secured phone.

Table 4-16: Association between gender and purposes of mobile payment and protection

	Contingency coefficient	P-value
sales and bought	0.259	0.508
money transfer	0.278	0.416
Pay utilities	0.409	0.051
High protection.	0.307	0.189

No significant association.

Hypotheses number 2:

The 'null hypothesis' might be:

H0: There is no a statistically significant relationship between Uses of mobile money and fraud.

And an 'alternative hypothesis' might be:

H1: There is a statistically significant relationship between Uses of mobile money and fraud.

Mobile money usage

Variables:

1- Do you agree to be one of the following points are a preferred point you have to loading balance on your mobile phone?
   i. Company's service centers
   ii. Banks
   iii. Peer-to-peer
2- Which of the following do you use your mobile money to do?
   i. Pay for utilities
   ii. Local money transfer
   iii. Pay for goods bought in shops

Table 4-17: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Peer-to-peer anyone ever transferred	4.04	50	.807	.114
	money from your mobile wallet	1.78	50	.996	.141

Table 4-18: Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Peer-to-peer & anyone ever transferred money from your mobile wallet	50	.570	.000

Table 4-19: Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Peer-to-peer - anyone ever transferred money from your mobile wallet	2.26	.853	.121	2.02	2.50	18.743	49	.000

Presents the output for the Paired-Sample T Test:

This output consists of three major parts:

- Paired Samples Statistics.
- Paired Samples Correlations.
- Paired Samples Test.

From the output, T= 18.743 with 49 degrees of freedom.

Confidence interval = 95%

Significance Level: a = 0.05

P-value=Sig. (2-tailed) = 0.000

(P-value $\approx 0.000 \leq 0.05 = a$), I shall reject the null hypothesis.

Result: There is a statistically significant relationship between Uses of mobile money and fraud.

Hypotheses number 3:

The 'null hypothesis' might be:

H0: There is no a statistically significant relationship between the lacks of confidentiality (sharing of PINs) in mobile phone and fraud in mobile money.

And an 'alternative hypothesis' might be:

H1: There is a statistically significant relationship between the lacks of confidentiality (sharing of PINs) in mobile phone and fraud in mobile money.

Mobile money fraud:

Variables:

1- Have you ever shared your mobile money PIN number with anyone?
2- Has anyone ever transferred money from your mobile wallet without your knowledge?

Table 4-20: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	have you ever shared your mobile money PIN number	2.44	50	1.248	.176
	anyone ever transferred money from your mobile wallet	1.78	50	.996	.141

Table 4-21: Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	have you ever shared your mobile money PIN number & anyone ever transferred money from your mobile wallet	50	.802	.000

Table 4-22: Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	have you ever shared your mobile money PIN number - anyone ever transferred money from your mobile wallet	.66	.745	.105	.45	.87	6.262	49	.000

Presents the output for the Paired-Sample T Test:

This output consists of three major parts:

- Paired Samples Statistics.
- Paired Samples Correlations.
- Paired Samples Test.

From the output, T= 6.262 with 49 degrees of freedom.

Confidence interval = 95%

Significance Level: a = 0.05

P-value=Sig. (2-tailed) = 0.000

(P-value ≈ 0.000 ≤ 0.05 = a), I shall reject the null hypothesis.

Result: There is a statistically significant relationship between the lacks of confidentiality (sharing of PINs) in mobile phone and fraud in mobile money.

Hypotheses number 4:

The 'null hypothesis' might be:

H0: There is no a statistically significant relationship between improving the security activities of the users and reducing risk of fraud.

And an 'alternative hypothesis' might be:

H1: There is a statistically significant relationship between improving the security activities of the users and reducing risk of fraud.

Mobile Phone Security:

Variables:

1- What do you look out for in buying a phone?
   i. considers security
   ii. fashion of the day
2- Secured mobile phone, are need Mobile Money just for Payment?
3- Concerns for mobile phone users regarding their mobile security.
   i. High importance
   ii. Moderate importance
   iii. Low importance
4- What makes a mobile phone secured?

Table 4-23: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	considers security Secured priority to buying a secured mobile phone	4.14	50	.857	.121
		3.84	50	.889	.126

Table 4-24: Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	considers security & Secured priority to buying a secured mobile phone	50	.833	.000

Table 4-25: Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	considers security - Secured priority to buying a secured mobile phone	.30	.505	.071	.16	.44	4.200	49	.000

Presents the output for the Paired-Sample T Test:

This output consists of three major parts:

- Paired Samples Statistics.
- Paired Samples Correlations.
- Paired Samples Test.

From the output, T= 4.200 with 49 degrees of freedom.

Confidence interval = 95%

Significance Level: a = 0.05

P-value=Sig. (2-tailed) = 0.000

(P-value $\approx 0.000 \leq 0.05 = a$), I shall reject the null hypothesis.

Result: There is a statistically significant relationship between the lacks of confidentiality (sharing of PINs) in mobile phone and fraud in mobile money.

Hypotheses number 5:

The 'null hypothesis' might be:

H0: There is no a statistically significant relationship between mobile money protection and responsibility to ensure mobile money secured.

And an 'alternative hypothesis' might be:

H1: There is a statistically significant relationship between mobile money protection and responsibility to ensure mobile money secured.

Variables:

1- What Level of protection of privacy that the users require for their information in their mobile devices?
   i. High protection
   ii. Moderate protection
   iii. Low protection
2- Which of the following actions will you take if you lose your mobile phone?
   i. Call the call centre to block the mobile phone
   ii. Call the company to block the mobile money account
   iii. Use GPS tracker to locate the mobile phone
3- Whose responsibility in your opinion is it to ensure your mobile money is secured?
   i. My responsibility
   ii. The responsibility of the mobile money operators
   iii. Shared responsibility between me and the mobile money operators

Table 4-26: Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Moderate protection	3.64	50	1.321	.187
	personal responsibility	3.28	50	1.230	.174

Table 4-27: Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Moderate protection & personal responsibility	50	.930	.000

Table 4-28: Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Moderate protection - personal responsibility	.36	.485	.069	.22	.50	5.250	49	.000

Presents the output for the Paired-Sample T Test:

This output consists of three major parts:

- Paired Samples Statistics.
- Paired Samples Correlations.
- Paired Samples Test.

From the output, T= 5.250 with 49 degrees of freedom.

Confidence interval = 95%

Significance Level: a = 0.05

P-value=Sig. (2-tailed) = 0.000

(P-value $\approx 0.000 \leq 0.05$ = a), I shall reject the null hypothesis.

Result: There is a statistically significant relationship between mobile money protection and responsibility to ensure mobile money secured.

Data presentation from the interviews:

This section presents the data from the interviews conducted. Structured interview format was adopted where respondents answered predetermined questions. Each interview lasted for about 50 to 60 minutes. Recording, as well as notes were made during the interview. The following personnel were interviewed:

- The Information Security Manager,
- The IT Auditor,
- The Mobile Money Operations Manager and
- The Assistant Mobile Money Operations Manager.

Valuable information and documents were provided by these officers during the interview to expatiate on answers relevant to questions posed. These interviews began with a range of questions related to the interviewees' job profile and their view with respect to the end-to-end security of the mobile money. The data collated is presented covering - understanding how mobile money works; security incidents/fraud

4.6 Understanding how mobile money works:

The interview sessions were started by asking the respondents to provide information on how the mobile money works. The responses covered the registration processes, mobile money architecture and the transactional processes.

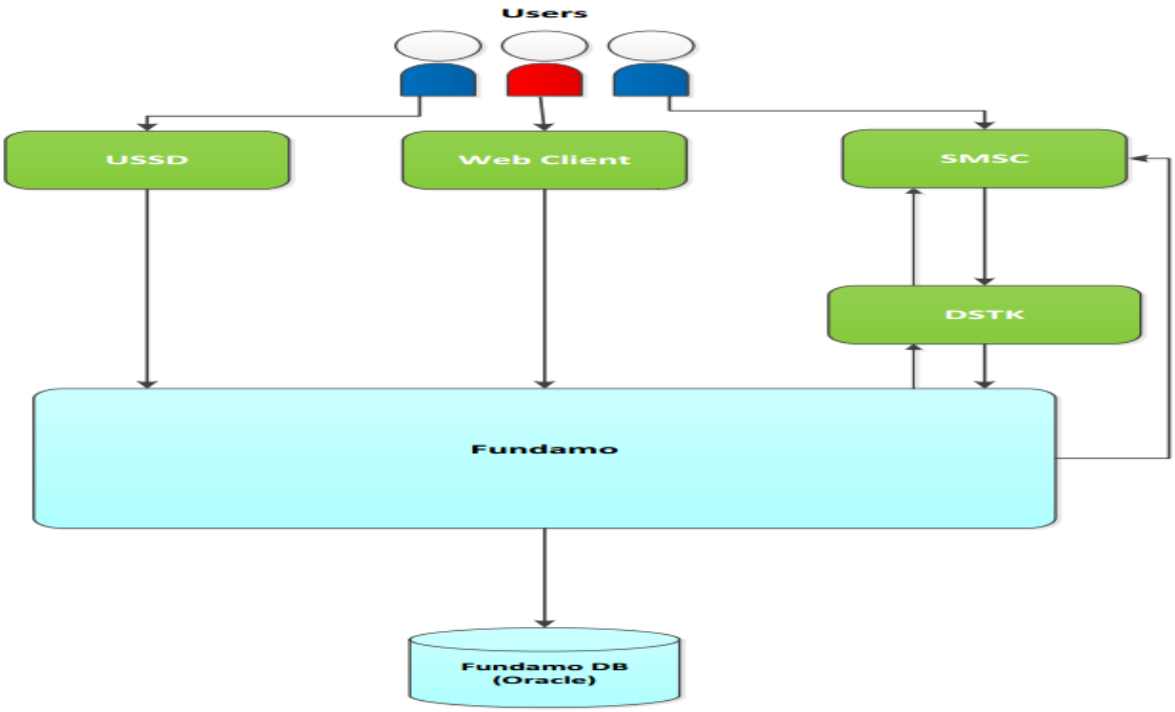
4.6.1 Registration processes:

From the response received, it was realized that if someone wants to use the mobile money on their phone, the person goes the service centers and request for this service to be made available on his or her phone. The person must present an identity card, such as valid passport, voter ID card or driving license. After their identity is confirmed, the contact agent does the registration on the Axon system. According to the respondents, the registration is done by either a SIM swap, which requires a new SIM card to replace the old one or the existing SIM card of the customer is maintained. When a SIM swap is done, it enables the user to do transactions through the STK channel, but when the person does not allow the SIM swap, transactions are done through the USSD channel.

4.6.2 Mobile money enterprise architecture:

It was made clear that the mobile money enterprise architecture is the various hardware and software components of the mobile money infrastructure and the channels for accessing the service. The feedback received indicates that the mobile money platform is made up of three major applications: Fundamo, DSTK and Axon as shown in the Figure 4-5 below.

Figure 4-5 Mobile money enterprise architecture

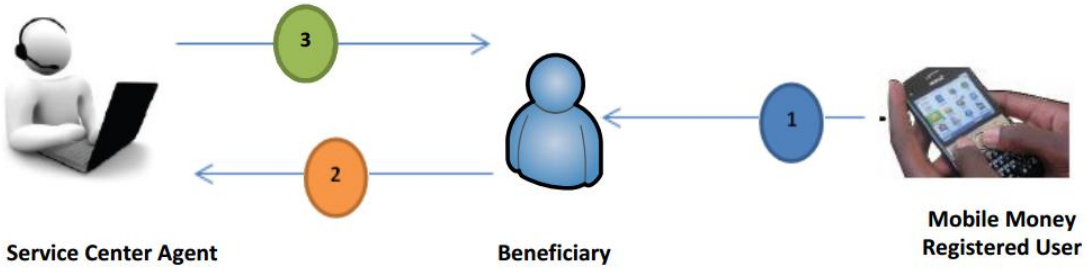


Fundamo was described by the respondents as a banking solution that enables the service provider to make cash management services available on the mobile phone or through the internet. DSTK on the other hand, is the technology used b y the service provider to manage a list of mobile services on the SIM menu. It was also explained that it is used for encrypting and decrypting mobile money transactions. As one of the channels to the mobile money services, the list of services it provides include bill payment, cash out and mobile money transfers. The other mobile money channels were identified as USSD and web services. It was made clear that the most commonly used channel is the DSTK, which normally requires a special SIM through SIM swap. It was indicated that the Axon system is the platform through which the user is registered onto the mobile money service.

4.6.3 Transaction processes:

It was identified that a mobile money user can use the service to transfer money, pay bills, and allow cash. However, in doing any of these activities, the user must enter their PIN and have available funds in the mobile money wallet to undertake any of these services. It was clear that the PIN the user provides on the first day of use becomes the only authentication medium to undertake any transaction on the user's phone. It was discovered during the interview that a registered mobile money user can either load money on their mobile wallet or withdraw funds from their mobile wallet at the banks, service centers or through the merchants. Similarly, when they want to withdraw funds from their account, they either use the STK or the USSD to allow cash out and give the required information to the agent to receive the money given to them.

Figure 4-6 Mobile money transaction (registered MM user)

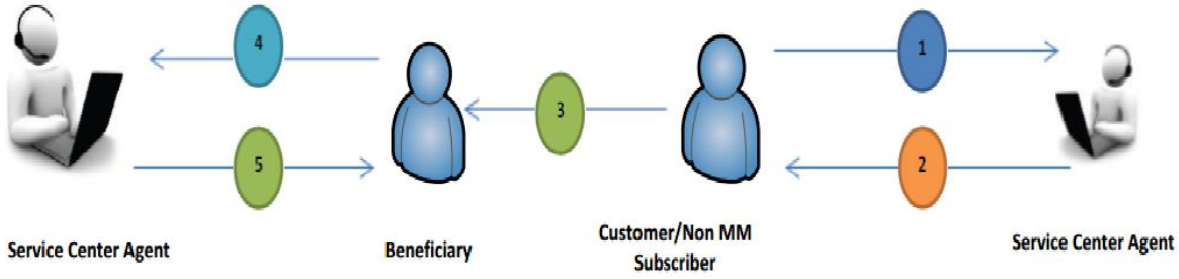


The above figure 4-6 shows how a registered mobile money user withdraws money from their wallet. The registered mobile money subscribers can perform a list of transactions from the STK on their phone directly. They select from a list of services on the STK; for example, to transfer money,

the user provides the relevant information, including the secret code and enters PIN to allow the transaction. If they have sufficient fund s in their account and provide the correct PIN, the transaction is performed and a token is generated and sent to their mobile phone via SMS. The person then sends the security code and token to t he beneficiary (1). Beneficiary contacts a merchant or service centre to cash out money (2) and provides the token and secret code to the service centre agent. The agent confirms the transaction on the mobile money platform and pays the beneficiary the transferred amount (3).

A non-registered mobile money user can also withdraw funds transferred to him or her at the service centre, merchants or at banks. A non-registered user will need to provide token and the secret code from the person sending the money; this information must accurately be given to an agent, who will then confirm these and cash out the money. The Figure 4 -7 below shows how the non registered mobile money user transfers money:

Figure 4-7 Mobile money transaction (non-registered mobile money user)



A customer or non-registered mobile money user goes to a service centre to do transfer, provides the detailed information required for the transaction

(1), including the amount to transfer and enters the secret code himself. The service centre agent generates the token and provides it to the customer (2). The customer transmits s or sends token and secret code to beneficiary (3). Beneficiary contacts a merchant or service centre to cash out money (4) and provides the token and secret code to the service centre agent. The agent confirms the transaction on the mobile money platform and pays the beneficiary the amount transferred (5).

4.7 Security Controls:

The next question focused on the technical and process controls implemented to ensure security on the mobile money platform. This question solicited responses on the available controls in place needed to ensure adequate security for the mobile money services.

The respondents assert that security is very important to the delivery of the mobile money service, as such several measures; both technical and non-technical have been introduced to secure the platform. The Information Security Manager indicated that due to the sensitive nature of the mobile money platform, it has its own-segmented network with its own firewalls and web application firewalls for the web service channel isolated from the Local Area Network (LAN). According to him, a number of security assessments are conducted throughout the year to detect and deal with vulnerabilities that may lead to security exposures. For example, vulnerability assessment and penetration testing are performed at least once a year to detect and address identified vulnerabilities. It was further noted that Group Technology of the company also performs an annual security assessment on the

It was identified that the following security measures have been put in place:

- "We have operational and training guide on day-to-day process. The operational guide contains all the activities of the mobile money team and contains controls relevant for the service." Mobile Money Operations Manager. Mobile money platform.
- Segregation of duties: one person does not initiate and complete the creation of electronic cash on Fundamo. For example, an officer may be able to enter electronic cash on the system but requires a senior officer to approve and commit the transaction.
- Daily reconciliations: this is done at the close of business each day to ensure that the amount of electronic cash generated tallies with the cash at the bank.
- User account management: user accounts are created on the platform only after request form is filled, a photo ID provided and the requisite approvals are been given by a senior manager. Accounts are also checked on monthly basis to clean the system of dormant account and resigned staff. All users are assigned to relevant profiles designed based on the principle of segregation of duties and minimum access privilege.
- Audit trails are done every week to see what is happening on the platform.
- Change control: all changes to the mobile money platform are approved by a change control board. This prevents disruptive changes and ensures the integrity of the system and system availability.

CHAPTER FOUR
Data Analysis and Discussion

4. Data Analysis and Discussion

4.1 Uses of mobile money:

From Table (4-22) (P-value ≈ 0.000 ≤ 0.05 = a), I shall reject the null hypothesis and Accepted an 'alternative hypothesis':

There is a statistically significant relationship between Uses of Mobile Money and fraud.

Using mobile money comes with its own vulnerabilities. As such, for anyone to successfully have any mobile money fraud carried out, for example, customer driven fraud the person would have to use any of the services the users are familiar with to get it executed. From Table (4-2) identify the preferred points of loading money on the mobile money wallet By comparing the means. The tables show that mean (4.4) of the respondents prefer the Peer-to-peer to the other sources available. Means (3.70), (3.76) of the respondents preferred service provider's service centre and Banks respectively.

For this the research reveals that the preferred point of loading money on phone especially affects on the level of secrecy.

When we note to this means, we find that the vast majority prefer to deal through the selling points (Peer-to-peer) more than the banks and service provider's service centre, as we see the selling points does not care about security procedures. As can be seen, in the Sudan, most people do not Prefer banks and service provider's service centre in transferring funds where stipulate filling out forms private and personal check to ensure that the transfer to the right person and in a manner more secret to prevent fraud; On the other hand we find that the (P2P) is more vulnerable to fraud.

This research also From Table(4-3) represents the distribution of respondents for the various uses of mobile money, the table shows that majority of users Mean (4.4) use mobile money for the Pay for goods bought in shops , Mean (3.96) of respondents use mobile money for money transfer, and Mean (3.86) use the service to Pay for utilities.

Reveals that the main usage of mobile money among users in Sudan is for local remittance purposes, International remittance is not yet available in Sudan though it is the desire of most users to have this service.

4.2 Understanding Fraud:

From Table (4-25) (P-value $\approx 0.000 \leq 0.05 = a$), I shall reject the null hypothesis and Accepted an 'alternative hypothesis':

There is a statistically significant relationship between the lacks of confidentiality (sharing of PINs) in mobile phone and fraud in electronic payment via mobile device.

The researcher asked few questions to know the users' awareness of fraud, and what it means to them to expose themselves to any act that can be a potential source of fraud. These questions are: a) have you ever shared your mobile money PIN with anyone, b) has anyone ever requested for your PIN and finally (c) whose responsibility is it to ensure the mobile money is secured. Analyses of these questions are shown as follows:

The respondents were asked to disclose if they have ever given their mobile money PIN to anyone. The responses obtained, as shown in

Table (4-4), indicates that respondents Mean (2.44) have no shared their mobile money PINs.

However, sharing the PINs exposes users to fraud, as one of the main causes of consumer driven fraud is PIN sharing. The good news in Sudan that the majority of the respondents (Disagree) indicated they do not share their PINs, because they want to prevent fraud on their mobile wallet.

- In response to the question 'has anyone ever requested for your mobile PIN number?' Mean (2.6) of the respondents answered in the negative, as seen in the Table (4-5).
- On the other hand, it can be argued that, Mean (2.44) have no shared their mobile money PINs, as indicated earlier, the Possibility of those who might have been asked to provide their PINs.
- More so, in answering the question as to whose responsibility it is to secure the mobile money service forming mean (4.16) of majority respondents indicated it is a shared responsibility between the user and the service provider. However, that mean 3.28 of the respondents think it is their personal responsibility to protect their mobile money and not the responsibility of the service provider, finally mean 3.58 of the respondents are of the opinion that it is the sole responsibility of the service provider to protect the mobile money service.

  From these discussions, it is evident that majority of the mobile money users mean (2.44) have the basic understanding that sharing of their PINs could expose them

to fraud, hence they take precautions not to share. It is also interesting to note that those who shared their PINs did so at will without anyone requesting for it. This could mean that there is no intention of a third party perpetuating fraud by requesting users' PINs. On the other hand, the service provider must tighten up their security measures in other to prevent fraud, since as much of the users are of the opinion that securing the mobile money service is the sole responsibility of the service provider.

4.3 Potential sources of fraud:

As was discovered in the discussion (section 5. 2)' of the respondents are likely to give their PINs if asked to do so. This can be argued to mean that a user's personal security practices to secure their mobile money, such as keeping their PINs safe and not sharing it , could be ignored.

By identifying these potential sources of the mobile money fraud, gives the service provider the chance to know the necessary measures to put in place, to enhance the mobile money security, and thereby help reduce the occurrence of fraud.

4.4 Unauthorized transaction:

From the Table (4-6), mean (1.78) of respondents experienced mobile money transfer from their wallet without their permission.

It can be deduced that, even though the respondents who shared their PINs did so with close relatives and could have done this based on trust, however unauthorized transactions have been performed on

these users' accounts. This percentage of unauthorized transactions gives cause to worry about the potential fraud cases because most users shared their PINs with their close relations.

4.5 Security practices of the users:

From Table (4-27) (P-value ≈ 0.000 ≤ 0.05 = a), I shall reject the null hypothesis and Accepted an 'alternative hypothesis':

There is a statistically significant relationship between improving the security activities of the users and reducing risk of fraud.

As already concluded, it can be deduced that the majority of the mobile money users, understand that it is not a good practice to share their PINs with other people and hence do not do it.

This can be seen in Table (4-7), which shows that mean (3.50) of users will go for the fashion of the day of the phone as a priority, whilst mean (3.84) will consider the security the phone provides. This research also reveals that materials stored on the phone are the major concern to the respondents. Table (4.7) shows several concerns for mobile phone users regarding their mobile device security. It shows that a majority of participants agreed about the importance of the information that they have in their mobile devices. The level „ High importance ‟ was chosen most frequently. The level „ Moderate importance ‟ was chosen most frequently and mean (4.8) as an important level of the information stored in the participants‟ mobile devices, Next was „ High importance ‟ at mean (3.98) and the lowest was „Low importance‟ at mean (2.36).

the result of this research indicated that Mean (4.18) of users prefer locking mechanisms in the form of using passwords, PINs and pattern to prevent unauthorized access to their mobile phones.

It was identified that mean (4.12) of the users will have their mobile phone blocked. However, before this is done, it means the individual must either have their phone registered with the service provider or install third party software on the phone to lock it. Mean (3.72) on the other hand indicated that they would also use GPS tracker to try locating the phone. Finally, mean (3.90) of the respondents will use the service provider's software to block the mobile phone.

This may imply that the user is avoiding the disclosure of the content stored in their phone which could also lead to their privacy being exposed or the one who steals the phone using privileged services on the phone, such as mobile money at the discomfort of the original owner.

From these discussions, it can be identified that the security practices of the mobile money users includes not sharing their mobile money PINs. The security that the mobile phone provides is not their priority when they want to buy a mobile phone, and also they believe that the security of t heir mobile money is not the sole responsibility of the MNO, but it is mainly the joint responsibility of the user and the service provider. This shows that the users see themselves and their personal efforts as important in securing the mobile money.

It can also be further argued that users do not consider the security features the phone provides as important as their personal security posture.

This is so because to the users, in buying a mobile phone, the security the phone provides is not very important to them but rather the fashion of the day the phone provides. It can be argued from this finding that in order to enable proper security of the mobile money to reduce fraud, the service provider must include enhancing the security awareness of the users and not only on technological security measures.

It is obvious that improving the security activities of the users can be more rewarding in reducing fraud and not only technological security measures.

4.6 Relationship between mobile phone and mobile money protection:

From Table (4-31) (P-value ≈ 0.000 ≤ 0.05 = a), I shall reject the null hypothesis and Accepted an 'alternative hypothesis':

There is a statistically significant relationship between mobile money protection and responsibility to ensure mobile money secured.

As users take precautions to protect their mobile phones, and their mobile money service using authentication method The Personal Identification Number (PIN) is a secret-knowledge authentication method and consequently relies upon knowledge that only the authorized user has. Although the PIN and password are the most commonly used methods for authentication in information systems, such secret-knowledge approaches unfortunately have long-established problems, with weaknesses often being introduced by the authorized users themselves.

From the Table (4-10) gives the opinion of respondents on another question in the survey investigated the most preferred authentication method by mobile phone users for the information security of their mobile device. The PIN or password method means (4.40) was the preferred authentication method, followed by the pattern mean (3.78), while mean (3.64) of the participants agreed that biometric authentication. However, a majority of the participants agreed that PIN or password method authentication will meet their need to protect sensitive information on their mobile device.

However, a majority of the participants agreed that PIN or password method authentication will meet their need to protect sensitive information on their mobile device.

The reason including user's password and PINs However, if anyone happens to steal the phone, successfully logs on to the phone, and tries through brute force or guess the PIN to the mobile money, the person may or may not be successful, since the mobile money service gets locked after 3 failed PIN entries.

The researcher further asked the respondents' view on whether having a secure phone makes their mobile money service secured. The table (4-14) shows that mean (4.14) of the respondents agree that having a secure mobile phone definitely ensures the safety of their mobile money.

4.7 Security countermeasures implemented by the service provider:

The following are some of the measures put in place by the service provider to reduce the occurrence of fraud. The first measure put in place was to set a maximum password or PIN attempt threshold to three in order to prevent brute force attacks on mobile money account by locking the account after three continued failed logon attempts.

This helps to protect users whose mobile phone have been misplaced or stolen from attempts made by the thief to access the mobile money service of the original owner.

Furthermore, as it was noted that mobile money users sometimes give their PIN to service centre agents to do transactions on their accounts, these agents have been advised not to accept such offers from customers any longer, which is in line with the operational management guide of the service provider.

4.8 Summary Analysis

4.8.1 Measures to improve security and to prevent fraud:

Considering the earlier discussions, the researcher conclude that, in spite of the several security measures carried out by both the service provider and the customers, the security of the mobile money service could further be enhanced to prevent fraud by employing the following:

- Set PIN Age or dynamic PIN: as one of the major causes of customer driven fraud is PIN sharing, it is recommended that the service provider must set a PIN age parameter to prompt users to change

their PINs at every quarter. Answering some personal identification questions about the registered user should be performed in order for the PIN change to be completed. Researcher suggest that even if the users share their PINs with close relations and any of those close relations have access to the phone at the time such a PIN change request comes; the person cannot easily change the PIN, since the person will not easily know the answers to the personal identification questions of the original user.

- Security awareness: furthermore, the service provider must at the point of registration communicate the user's responsibility of protecting the mobile money wallet. This can be complimented with the service provider giving at least twice in a year mobile money security tips to the users through SMS to alert them about their security obligations that can help to enhance the security of the service.

From this research, it had also been established that both MNO and majority of subscribers know their security obligations and have taken some steps to protect the mobile money service and their interests respectively. This assertion is elaborated by reviewing the security controls put in place by the MNO in relation to the security practices of the users as shown below:

- **Controls put in place by the MNO:**
  - Proper account management – handling of dormant accounts
  - Daily and periodic reconciliation
  - Enabling transactional auditing

- Risk management
- Change management
- Security awareness

- **End user security activities:**
  - Avery high percentages agree of mobile money users does not share their password.
  - Majority of mobile money subscribers surveyed agree the security of the mobile money service is a shared responsibility between MNO and themselves.
  - Majority of users agree a secured phone means a secured mobile money wallet.
  - Majority of subscribers agree mobile money will buy a secure phone purposely for the mobile money service on the phone. This implies that the security of the mobile phone is also important to the users.

CHAPTER FIVE CONCLOUSION AND FUTUER IMPLICATION

5. Conclusion And Future Implication

This chapter, therefore, presents the conclusions; recommendations, as well as limitations and directions for further studies.

5.1 Conclusions:

This research has revealed that the major uses of mobile money service is for purchasing and for local money transfer, as is generally believed to be the uses of mobile money in most African countries. The researchers are of the opinion that as more people have access to mobile phones as compared to bank accounts, and money transfer can be easily done on their mobile phones made this usage very popular.

More so, it is cumbersome for one to open a bank account, as several materials are required, such as government issued identity cards, references from an existing customer, as well as a form of confirmation of users' location. Meanwhile, as compared to having a mobile money account, the process is not as complicated as opening a bank account. It can further be speculated that people are looking for easier and faster ways of sending and receiving money. It can also be argued that, as mobile money transfers are done mostly from the cities to the countryside, where most people do not have a bank account but a mobile phone is easily accessible, this could be a contributing factor for the major use of mobile money for transfer purposes.

As one of the major causes of consumer driven fraud is PIN sharing, it can be seen from this research that this is not a very common practice. However, the 8.3% that shared their PINs did so with their relations and sometimes with customer agents to help them in transacting one service or the other from their mobile money.

It can be seen from this that, PIN sharing could be done based on trust, and if any fraud should be perpetuated through acquiring of the users'

PIN, the person carrying out the fraud must first try to win the trust of the user, either by pretending to be a part of the service provider or a relative

Who is trying to offer a help. To avert this however, the researchers believe that the MNOs must alert users to first verify from them the authenticity of any suspected request before giving out any information that could make them vulnerable to fraud.

Despite users' awareness of their security measures they can take to prevent fraud, the service provider has a major task in securing the mobile money service, since as much as 60.5% believe the security of the service solely depends on the service provider. The researcher believe this category of users will invariably not put any blame on themselves if any fraud happens, since they believe total protection of the service depends on the service provider.

The general perception that there is direct linkage between mobile phone protection and mobile money protection could be attributed to the fact that users believe the service provider has put in place adequate measures to protect the mobile money service.

5.2 Recommendations:

Some of the recommendations made are as follows:

- As PIN sharing was identified as one of the major causes of consumer driven fraud, it is recommended that the service providers must set up password age parameters for the users to change their passwords every quarter. This must further be authenticated through answering personal identification questions.
- It is also suggested that service provider must enhance their awareness creation about the services available on the mobile money service.
- Service provider must also create awareness to mobile money users that the security of the mobile money service does not only depend on the MNOs, but the users also have a role to play.

5.3 Limitations and directions for further studies:

This research was conducted in Sudan, and used one out of the three mobile money service providers, who at the moment has the highest subscriber base compared to the other two companies.

It is possible that at the time a similar research is made, this distribution will not remain the same. It must also be noted that this research findings are limited to only this one company and do not necessarily represent the opinion of all the three mobile money service providers in the country. As the research did not include non-registered users there is the possibility of missing the inputs of

this category of users, and this must be considered in interpreting the findings of this research.

From the questionnaire, there were sent to the service centre managers and were tasked to ensure they get the required number of feedbacks. Also the service centre managers were given enough time (2 weeks) to administer the questionnaire and return them. More so, the service centers have more customers coming in for transactions, among which mobile money is one of the most used.

The questionnaires were administered to mobile money users by the MNO service centre agents. There is the tendency that there may be a response bias based on the fact that, it may occur to users surveyed that, for example sharing of mobile money PINs could lead to fraud when asked the question if they ever shared their mobile money PIN. As a result the response provided may not directly reflect the actual practice by the user. The personal relationship with the agents administering the survey could also indirectly influence the feedback provided by the respondent, providing a feedback they deem right and not what actually happens in practice.

From this study, it is obvious certain parts of the work could have been exhaustively discussed; however, this could not be done due to time limitations.

REFERENCES

[1] T. E. W. 2012, "One business where the poorest continent is miles ahead," *The Economist*, 04 Nov. 2012.

[2] Karnouskos, "Cell Phone Forensic Tools," December 2012.

[3] Herzberg, "An analysis of research methodologies', in The information systems research challenge," 2003.

[4] Githui, "Mobile money transfer in Kenya: an ethical perspective," *Research Journal of Finance and Accounting ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online) Vol 2*, DM 2011.

[5] G. M. M. T. 2012, " "Global Mobile Money Deployment Tracker.","02 February 2013.

[6] Y. K. Au, "The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application' Electronic Commerce Research and Applications," 20 February 2013.

[7] M. Z. Solin, "Mobile money methodology for assessing money laundering and terrorist financing risk," *GSMA Discussion Paper*, 10 January 2013.

[8] H. M. Amrik, "Seeking Fertile Grounds for Mobile Money," 2009.

[9] I. I. F. Corporation), "Mobile Money Study 2011," 12 March 2013.

[10] U. Eze, Gan, GG, Ademu, J & Tella, ""Modelling user trust and mobile payment adoption: A conceptual framework" Communications of the IBIMA," SA 2008.

[11] K. Taga, Karlsson, J & Arthur, "Little Global M-Payment Report," D 2004.

[12] Y. Lee, Kim, E & Jung, "A NFC based Authentication method for defence of the Man in the Middle Attack," *International Conference on Computer Science and Information Technology (ICCSIT'2013)*, January 4-5, 2013.

[13] W. B. 2012, "Information and communications for development 2012: Maximizing Mobile, Washington," March 2013.

[14] S. K. Schwiderski-Grosche, "Secure M-Commerce, Information Security Group, Royal Holloway University of London," 2002.

[15] Mudiri, "Fraud in mobile financial services," Viewed 20 May 2013.

[16] Merritt, "Mobile money transfer services: the next phase in the evolution in person-to-person payments," Viewed 19 April 2013.

[17] Karnouskos, "Mobile Payment: A journey through existing procedures & standardization initiatives " IEEE Communications Surveys & Tutorials, pp. 44-66," 2004.

[18] Mallat, ""Exploring consumer adoption of mobile payments - A qualitative study," Journal of Strategic Information Systems, Vol. 16, pp," 2007.

[19] N. Kreyer, Pousttchi, K &Turowski, "Mobile payment procedures: scope and

characteristics,” *e-Service Journal 2 (2002–2003) 7–22*, (2002–2003).
[20] F. A. Egger, “"Security & Trust: Taking Care of the Human Factor,"

Electronic Payment Systems Observatory Newsletter,” 2001.
[21] W. A. Jansen, “Guidelines on cell phone forensics, NIST Special Publication

800-101,” Viewed 20 May 2013.