# AN INVESTIGATION INTO THE ROLE PLAYED BY PERCEIVED SECURITY CONCERNS IN THE ADOPTION OF MOBILE MONEY SERVICES:

A Zimbabwean Case Study

A thesis submitted in partial fulfillment of the

requirements for the degree of

MASTER OF SCIENCE

of

RHODES UNIVERSITY

**CHARLES MADEBWE**

July 2014

**Abstract**

The ubiquitous nature of mobile phones and their popularity has led to opportunistic value added services (VAS), such as mobile money, riding on this phenomenon to be implemented. Several studies have been done to find factors that influence the adoption of mobile money and other information systems. The thesis looks at factors determining the uptake of mobile money over cellular networks with a special emphasis on aspects relating to perceived security even though other factors namely perceived usefulness, perceived ease of use, perceived trust and perceived cost were also looked at. The research further looks at the security threats introduced to mobile money by virtue of the nature, architecture, standards and protocols of Global System for Mobile Communications (GSM). The model employed for this research was the Technology Acceptance Model (TAM).

Literature review was done on the security of GSM. Data was collected from a sample population around Harare, Zimbabwe using physical questionnaires. Statistical tests were performed on the collected data to find the significance of each construct to mobile money adoption. The research has found positive correlation between perceived security concerns and the adoption of money mobile money services over cellular networks. Perceived usefulness was found to be the most important factor in the adoption of mobile money.

The research also found that customers need to trust the network service provider and the systems in use for them to adopt mobile money. Other factors driving consumer adoption were found to be perceived ease of use and perceived cost. The findings show that players who intend to introduce mobile money should strive to offer secure and useful systems that are trustworthy without making the service expensive or difficult to use. Literature review done showed that there is a possibility of compromising mobile money transactions done over GSM.

**Acknowledgements**

I wish to express my sincere gratitude to my supervisor, Professor Barry Irwin and co-supervisor John Ritcher for their guidance and support. I also wish to thank the participants who completed the circulated questionnaire. I wish to thank my employer NetOne Cellular for affording me time away to conduct my studies. I would like to thank my family for the support and God Almighty for the wisdom, inspiration and good health throughout my studies.

**Table of Contents**

**List of Tables**

**List of Figures**

**List of Abbreviations**

| | |
|---|---|
| A3 | GSM Authentication algorithm A3 |
| A5/A8 | One algorithm performing the functions of A5 and A8 |
| A5/1 | GSM Encryption algorithm A5/1 |
| A5/2 | GSM Encryption algorithm A5/2 |
| A8 | GSM Encryption key generating algorithm A8 |
| ANOVA | Analysis of Variance |
| ARPU | Average Revenue Per User |
| BCCH | Broadcast Control Channel |
| DES | Data Encryption Standard |
| DoI | Diffusion of Innovation Theory |
| FCCH | Frequency Control Channel |
| FDMA | Frequency Division Multiple Access |
| GSM | Global System for Mobile Communications |
| HLR | Home Location Register |
| IMSI | International Mobile Subscriber Identity |
| MFS | Mobile Financial Services |
| MM | Mobile Money |
| MNO | Mobile Network Operator |
| MS | Mobile Station |
| MSC | Mobile Switching Centre |
| NFC | Near Field Communications |
| OTA | Over-The-Air |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |

| | |
|---|---|
| RBTS | Rogue Base Station |
| SCH | Synchronisation Channel |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SMSC | Short Message Service Centre |
| SPSS | Statistical Package for the Social Sciences |
| SRES | Signed Response |
| STK | Subscriber Identity Module Tool Kit (SIM ToolKit) |
| TAM | Technology Acceptance Module |
| TBP | Theory of Planned Behavior |
| TDMA | Time Division Multiple Access |
| TMSI | Temporary Mobile Subscriber Identity |
| USSD | Unstructured Supplementary Services Data |
| UTAUT | Unified Theory of Acceptance and Use of Technology |
| VAS | Value Added Services |
| VLR | Visitor Location Register |
| WAP | Wireless Application Protocol |

# Chapter 1 – Introduction

## 1.1 Introduction

When Global System for Mobile communications (GSM) was developed it was meant for communication and not to be as secure as banking platforms. The security of GSM has been criticized mainly because the GSM consortium chose to develop their security away from the public domain (Van de Merwe, 2003). There exists security concerns with GSM networks and the SMS/GPRS protocol and mobile banking solutions implemented by banks. In a study covering 13 000 consumers by Javelin Strategy and Research, mobile banking was shown to have been less used in developed countries in spite of the explosive growth of smart phone ownership to levels above forty percent (ABA Banking Journal, 2011).

According to ABA Banking Journal (2011), tech-savvy consumers are increasingly using smartphones for almost everything with the exception of mobile banking and purchasing. Between 2010 and 2011 the adoption rate of mobile banking never changed irrespective of the aggressive marketing. Rates of mobile purchasing also remained unchanged. Consumers regard mobile banking as risky such that between 2009 and 2010 there was an increase of 54% in those who formerly rated it as unsafe now classifying it as very unsafe (ABA Banking Journal, 2011).

Sub–Saharan Africa has part of the least developed telecommunication infrastructure in the world (Aker and Mbiti, 2010). There exists fewer than 3 landlines per 100 people in Africa (International Telecommunications Union, 2009). In spite of this, the access and use of mobile telephony has increased significantly such that the number of mobile phones is ten times that of landlines in Sub-Saharan Africa (International Telecommunications Union, 2009). Mobile phone coverage is enjoyed by 60% of the population. Mobile phone subscriptions went up by 49% yearly for the period spanning the years 2002 to 2007 compared to 17% achieved by Europe (Aker and Mbiti, 2010).

This rapid adoption of mobile phones has prompted business to introduce value added services (VAS) to increase revenues. Safaricom of Kenya launched M-Pesa[1], a mobile wallet in the year 2007 that achieved its first year targets in terms of subscribers in two months (Michaels, 2011). It still continues to grow and had 16 million users in 2011 representing 40% of the population (Michaels, 2011). Mobile Money is particularly well embraced by the developing world (Smart City Magazine, 2013).

M-Pesa handles two million transactions daily, US$4.98 billion annually which is equivalent to 17% of Kenya's GDP (Michaels, 2011). Kenya is now the leading country in mobile money market (International Telecommunications Union, 2009). Other telecommunication players in Kenya and other nations like South Africa and Zimbabwe have also taken up mobile money.

In Zimbabwe, NetOne[2], a telecommunications firm, was the first to embark on such a project called OneWallet in 2010, before its rival Econet Wireless[3] introduced EcoCash in 2011. The uptake rate of EcoCash has also been rapid compared to OneWallet (Kabweza, 2012). It now stands at 1.7 million subscribers. NetOne uses a SIM ToolKit (STK) based system while Econet Wireless uses a system based on a technology called Unstructured Supplementary Services Data (USSD). STK based systems are generally considered to be more secure than USSD based systems (Telecom-week, 2012). NetOne took a security based initiative in rolling out its product but the uptake rate of its system has not been as high as that based on USSD technology despite the latter being considered less secure.

The research seeks to find security loopholes in GSM mobile money systems and whether these security concerns are of significance in the adoption of mobile money technologies in Sub-Saharan Africa. It seeks to compare the background in the developed world and Africa to see the factors that affect adoption rate. Is there a correlation between security of mobile money products and usage or is it the availability of service and ease of use that matter?

[1] http://www.merchantpro.co/betterthancash.pdf
[2] http://www.netone.co.zw/
[3] https://www.econet.co.zw/

## 1.2 Research Problem

Mobile money as a VAS service provides convenience to users and increases average revenue per user (ARPU) for mobile network operators (MNOs) as well as reducing customer churn (Aweda, 2010). Customers need to know the risks associated with mobile money. MNOs need to know the behaviour patterns of consumers so that they tailor make their products for the market segment they wish to target (Penicaud, 2012). They do not need to over-commit resources towards unimportant areas whilst neglecting the important aspects of their systems.

There are questions that need to be answered: what are the security risks associated with mobile money? What factors influence the adoption of mobile money by members of the target market? Does security affect the customer's choice of a mobile money service provider?

Research pertaining to this has been done with focus on mobile commerce and mobile banking. There are various studies done on effects of perceived risk concentrating mainly on online banking (Masinge, 2010). Masinge (2010) who focused his mobile money studies in the context of South Africa, argues that perceived risk should not be modelled as a single construct as this will fail to make it highlight the risk factor characteristics. In Zimbabwe studies to do with mobile banking were done by Chitungo and Munong (2013) focusing on the rural population and they found perceived ease of use to have a significant effect on user's attitude thereby influencing intention to adopt.

Other studies done in Sub-Saharan Africa were done in Ghana, Tanzania and Kenya to investigate key factors that influence mobile money adoption using key constructs from the Technology Acceptance Model (TAM) and Diffusion of Innovation (DoI) theory (Tobbin and Kuwornu, 2011). Demographics and socioeconomic factors have an effect on mobile money services uptake while regulation is the only external component that can hinder the progress of a service (Penicaud, 2012).

Penicaud (2012) notes that following best practices is critical for adoption of a service but there is need to adapt services to the local market context. For the service to survive in markets with diverse demographic and socio-economic circumstances operators need to tune the product to meet the specific market requirements.

According to Tobbin and Kuwornu (2011) research done on the adoption determinants of m-commerce and mobile banking can be applied to mobile money since mobile money is an extension of mobile banking. This research seeks to add value to previous studies by narrowing the focus to mobile money only and limiting the scope to Sub-Saharan Africa, Zimbabwe. This will give a better view of factors to consider when implementing mobile money to would be providers and assist in improving mobile money services already being offered in Zimbabwe by Econet wireless and NetOne.

### 1.3 Research Objectives

The following are the goals that this research seeks to achieve.

- To establish whether there exists a correlation between security concerns of GSM mobile money systems and their adoption.
- To find factors that affect uptake rate of GSM mobile money by users in order of precedence.
- To give a guideline of the acceptable tradeoff between security and other system critical factors to be considered by operators on GSM mobile money product implementation.

### 1.4 Research Questions

In order to meet the research goals, the research seeks to answer following questions.

- What are the security risks associated with mobile money over cellular networks?
- Why is mobile money uptake rate higher in Africa compared to the developed world?
- How does the security of USSD and STK based systems compare?
- Do users in Africa value security when adopting a mobile money technology?
- What was the best way for NetOne to follow in rolling out its mobile money project?

### 1.5 Research Scope

This research was conducted in both urban and peri-urban centres of Zimbabwe. The constructs covered by the survey are: perceived security, perceived usefulness, perceived ease of use, perceived cost and perceived trust. The research will also focus on security issues associated

with mobile money systems as posed by the nature of GSM, mobile stations and their operating systems.

The research scope can be described by the definitions that follow:

- Perceived security will cover the following facets: privacy risk, performance risk, financial risk, integrity, reliability.
- Perceived ease of use will encompass registration procedures, ease of product learning, ease of use of the payment procedures, fewer steps required to make a payment, readily available customers services, correct screen size and input capabilities and a readily available agent network.
- Perceived usefulness will mean the extent to which mobile money will dovetail into the daily activities of consumers and enhance their way of transacting.
- Perceived cost refers to tariff charges incurred as transactional cost per mobile money transaction.
- Perceived trust is the customer belief that a third party will not act opportunistically.

### 1.6 Research Model and Hypotheses

This research extends Technology Acceptance Model (TAM) by additionally examining the effects of perceived trust and perceived security/risk.

**TAM based hypotheses**

Perceived usability (PU) and perceived ease of use (PEOU) are determinants of behaviour intention (BI). This means PEOU and PU are two factors that greatly affect adoption of mobile money by a user since BI is analogous to adoption of mobile money (Masinge, 2010). Actual usage of a technology is determined by the intention to adopt the technology (Venkatesh and Davis, 2000). This study looks at people from all categories of life for as long as they are 16 years and above. The following hypotheses are proposed.

H1: Perceived usefulness (PU) influences the adoption of mobile money over cellular networks.

H2: Perceived ease of use (PEOU) influences the adoption of mobile money over cellular networks.

**Perceived cost hypothesis**

Poor people have very little disposable income thus prefer the cheapest prices. We hypothesize that cost of mobile money negatively affects adoption.

H3: Perceived cost influences adoption of mobile money.

**Perceived risk/security hypothesis**

Risk is a notable factor that affects adoption of mobile banking (Masinge, 2010). All risk facets : security, performance, financial, time and social risks also act as deterrents to mobile money adoption. For the study the perceived security hypotheses reads as follows:

H4: The level of security has an impact on the usage of mobile money over cellular networks.

H5: The level of trust a customer has in a mobile money service provider affects the adoption of mobile money .

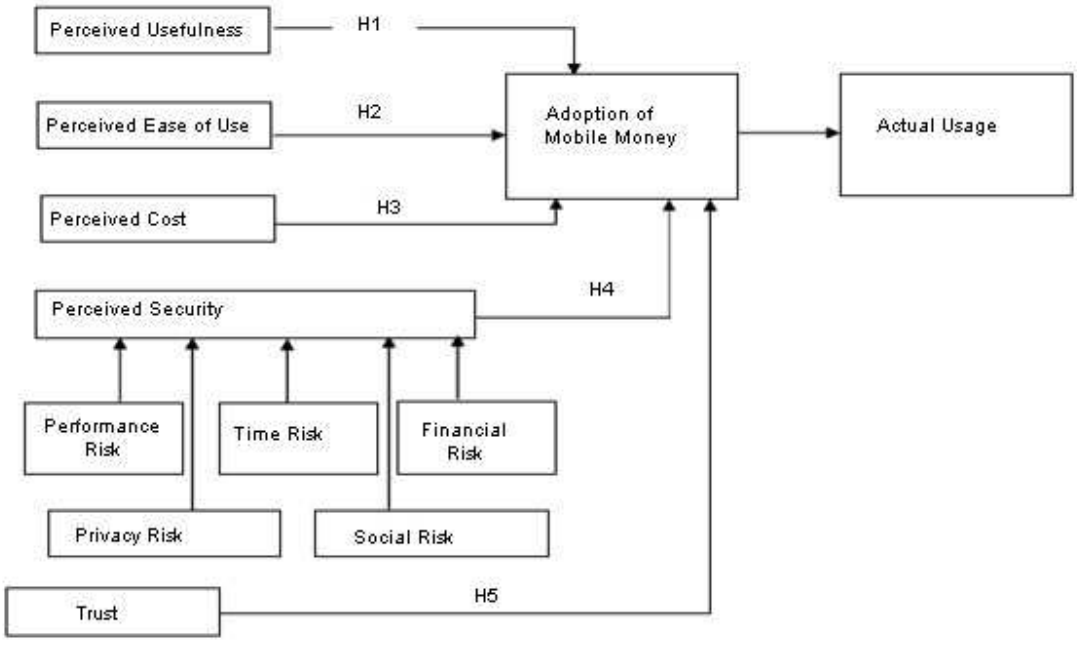


**Figure 1.1: TAM based research model with hypotheses based on perceived security and perceived cost**

## 1.7 Research Aim

The major research target is to find the extent of influence possessed by security issues in the adoption of mobile money over GSM. It also seeks to find other factors that influence adoption of mobile money and the extent to which they do as well as security loopholes that exist in mobile money systems over GSM. Reasons for different mobile money adoption patterns in the developed world and developing world are also investigated.

The research adds to knowledge already present concerning customer behaviour with regards to mobile money services. Since mobile money is an extension of m-commerce, the research will add a dimension of understanding to m-banking as well. It also adds to academic research on general technology adoption drivers. The research gives an insight into security loopholes posed by using mobile money over GSM.

The research objectives were met by conducting both an empirical study using questionnaires and an explorative research through literature review on the adoption of mobile banking as well as mobile money . Since mobile money is an extension of mobile commerce, which in turn is just another information system (Tobbin and Kuwornu, 2011), research previously done on adoption of information systems was also reviewed. The technology acceptance model was adopted. Research was also done on security loopholes presented by mobile money over GSM because of the technologies and equipment used as well as procedures in place.

Mobile money service providers need to understand the security loopholes posed by offering mobile money over GSM. They need to understand the technology adoption behaviour of consumers in their target markets so that they tailor make their products to suit the target market (Penicaud, 2012). They need to know the optimal resources to commit to security aspects of mobile money systems as well as other system critical requirements, like performance speed, so that no resources (financial/computer) are committed superfluously.

The research will equip mobile money service providers with better understanding of patterns and behaviours of Sub-Saharan Africa customers as far as mobile money systems security aspects are concerned to allow them to formulate appropriate marketing and business models (Masinge, 2010).

## 1.8 Structure of the Document

The remaining part of this document is organised as follows.

Chapter 2: This chapter takes the reader through a literature review, provides a background to and current mobile money services in Sub Saharan Africa using Zimbabwe as an example. The chapter gives an insight into other studies done on main conceptual elements in this research like perceived security and perceived cost. An assessment of numerous technology adoption models is done with a view to chose a model that fits this research.

Chapter 3: Methodology details of the research are given in the chapter. Empirical research was used to test the hypotheses.

Chapter 4: Data analysis is done in the chapter.

Chapter 5: This chapter looks at presentation of results.

Chapter 6: Concludes this research and discusses implications of findings to business then closes by giving recommendations for future studies.

# Chapter 2 – Literature Review

## 2.1 Introduction

The chapter gives an insight into related work done with regards to adoption of mobile money over GSM and CDMA in Sub Saharan Africa by other scholars. It also considers work done on mobile banking adoption, m-commerce adoption and adoption of other information systems which fit in the context of the study. Literature review of security risks posed by offering mobile money over GSM is also reviewed. An insight into the factors affecting mobile money adoption in the developed world is also given. A thorough comparison of the security of Unstructured Supplementary Services Data (USSD) protocol versus that of Subscriber Identifier Module ToolKit (SIM Toolkit) is also given.

This chapter starts by looking at the mobile money enabling technologies. It then gives a background of GSM and looks at the architecture of GSM and the algorithms that are used so that the reader can have an appreciation of the effects of the components and algorithms to mobile money security. It then looks at the reasons behind different mobile money adoption patterns in Africa and the developing world as well as the general factors that affect mobile money adoption. The chapter proceeds to look at the security concerns brought about by SIM cards and handsets used by mobile money users and compares USSD and STK based mobile money systems security.

## 2.2 Mobile Money Enabling Technologies

Mobile money is the term used for using a cell phone to make payments to others where value can be stored on a mobile wallet before and after the transaction. A sender can put money into his mobile wallet by going to a registered agent after which they use a secure electronic approach to transfer funds to the mobile wallet of the recipient who can then either keep the funds in his mobile wallet or visit an agent to convert the mobile money to cash (Smart City Magazine, 2013). Mobile financial services (MFS) also referred to as mobile money (MM) is a term used to

refer to provision and availability of banking and financial services with the help of mobile telecommunication devices (Tiwari, Buse, and Herstatt, 2007).

Mobile money can be made available by making use of any of the following technologies.

### 2.2.1 SIM Tool Kit (STK)

This is the way through which mobile money is often delivered. It allows mobile operators to load a set of menus and applications on to the subscriber identity module (SIM) thereby housing the subscriber's mobile money menu within the SIM card. STK works on most devices allowing mobile money accessibility to a wide range of customers, both rich and poor. User input is obtained through a menu presented by a SIM programmed application and transaction data is transmitted through encrypted SMS. The STK option is available for GSM networks and involves swapping of a subscriber SIM in exchange with one that houses the required application.

SIM Tool Kit is a GSM standard which allows the SIM card to initiate actions which can be used for a number of value added services. It consists of commands programmed on to the SIM specifying how the SIM must interact with the external environment. For applications that require a basic, easy to understand user interface, it is the ideal technology. It is secure, usable and portable thus caters for low cost mobile stations.

### 2.2.2 Unstructured Supplementary Services Data (USSD)

This is the technology used by Econet Wireless in Zimbabwe and MPESA-Tanzania. USSD is a communication protocol that works by sending text messages between a mobile phone and applications resident on a network. It is a standard for sending and receiving information over GSM signaling channels and is used mainly for balance querying in prepaid GSM services (Smart City Magazine, 2013). It is faster than SMS by nearly seven times and is very cost effective. Its operations are simple and handset independent allowing accessibility by old cellphones to the latest smartphone (Sanganagouda, 2011).

USSD does not require as a pre-requisite, any application to be installed on the SIM card or handset. USSD requires that a subscriber dial a short code number for the menu to be activated. At each user input data is sent to the server and the new menu screen is sent back which is time

consuming. USSD allows for session based communication between the mobile device and the server unlike SMS which employs a store and forward oriented message transaction therefore is more secure than SMS (Sanganagouda, 2011).

### 2.2.3 Short Message Service (SMS)

This technology involves a direct connection from the SMS gateway to the mobile money platform. It uses standard SMS messages in transmitting transaction data implying that no specific applications are pre-requisites for the SIM or handset (Smart City Magazine, 2013). SMS is less secure compared to other options and has usability difficulties since it does not use menus. SMS allows for 160 alphanumeric characters (Hord, 2005).

### 2.2.4 Web (WAP)

This is a set of protocols used to connect mobile phones and radio devices to the internet. The technology rewrites existing web pages into a simplified language (Rouse, 2010). Consumers will use these installed web pages for making payments. WAP has cost and speed setbacks. It has the benefit of possible follow-on sales because mobile lead back to visited stores. It also has high consumer satisfaction due to quick payments. WAP is normally used alongside other systems like SMS, USSD, STK and Voice eg YuCash of Kenya (Smart City Magazine, 2013). Lipuka of SubSaharan Africa that had in excess of 60 million subscribers in 2013 use WAP for bill payment.

Mobile money can also be provided through a contactless radio technology that is able to transmit data between devices that are a few centimeters away from each other called Near Field Communication (NFC). The NFC chips can be embedded into mobile phone SIM cards paving way for a whole range of digital services like e-ticketing and payments (Kessler, 2011). Quick Response codes which are square bar codes read by an imaging device and decoded by a specific software are also a possible technology through which mobile money can be provided. The technology allows customers to purchase goods through their mobile phone (Korhan, 2011). They are originally from Japan were they are very common. They enable a piece of information from a transitory media to be put in a cellphone (Lyne, 2009).

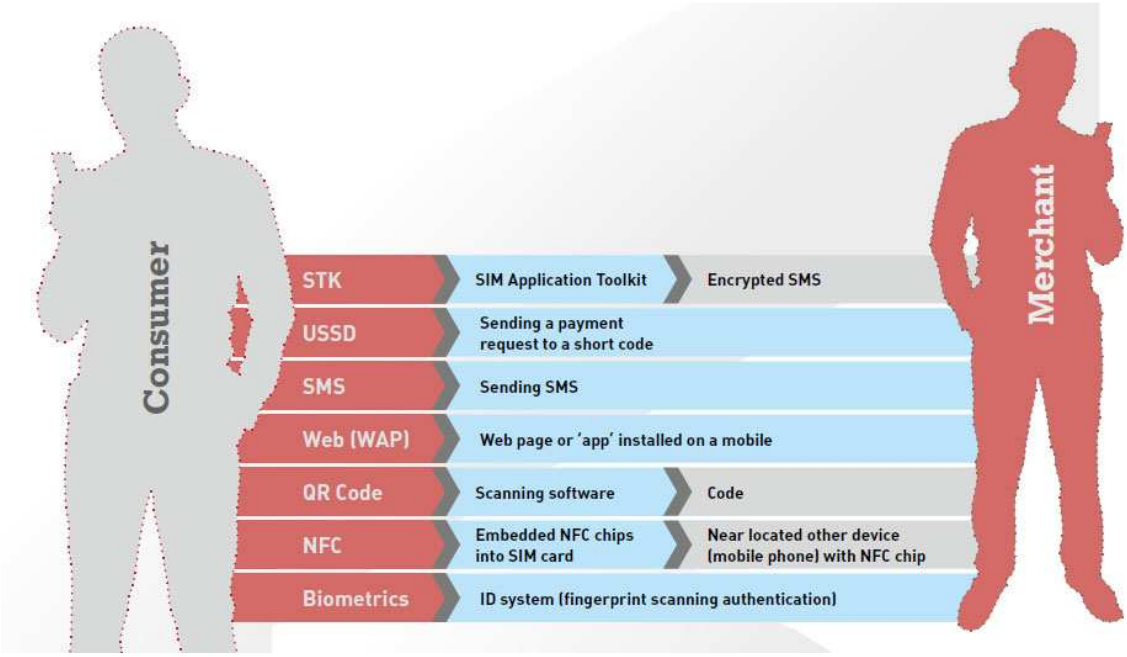


**Figure 2.1: Mobile money enabling technologies overview. Adapted from** (Smart City Magazine, 2013)

Figure 2.1 shows a visual summary of the technologies that enable mobile money. It shows how the interaction between a merchant and a customer is enabled by each of the technologies.

## 2.3 GSM Architecture

To offer a complete mobile money service there is need for a partnership between a mobile network operator (MNO) and a financial institution. A financial institution is not mandatory though. A GSM network is mandatory. Figure 2.2 represents a traditional GSM architecture. Lines show communication between components in operation.

A Mobile Station (MS) which can be a cell phone initiates a session and signals come from it to the Base Transceiver Station (BTS). The BTS serves the purpose of routing signals to and from the MS and translates to digital format the received radio signals then forwards them to the Base Station Controller (BSC). The BSC transmits the received signals to the Mobile Switching Centre (MSC) which then queries Home Location Registers (HLR) and Visitor Location Register (VLR) which are databases that keep information about the destination MS (Nokia, 2002). The HLR keeps data about all customers who belong to an area serviced by a MSC. Such data include the International Mobile Subscriber Identity (IMSI), services subscribed by a user,

authentication data (Ki) and some other temporary data (SANS Institute, 2001). The VLR contains relevant data for all subscribers a MSC is currently serving.

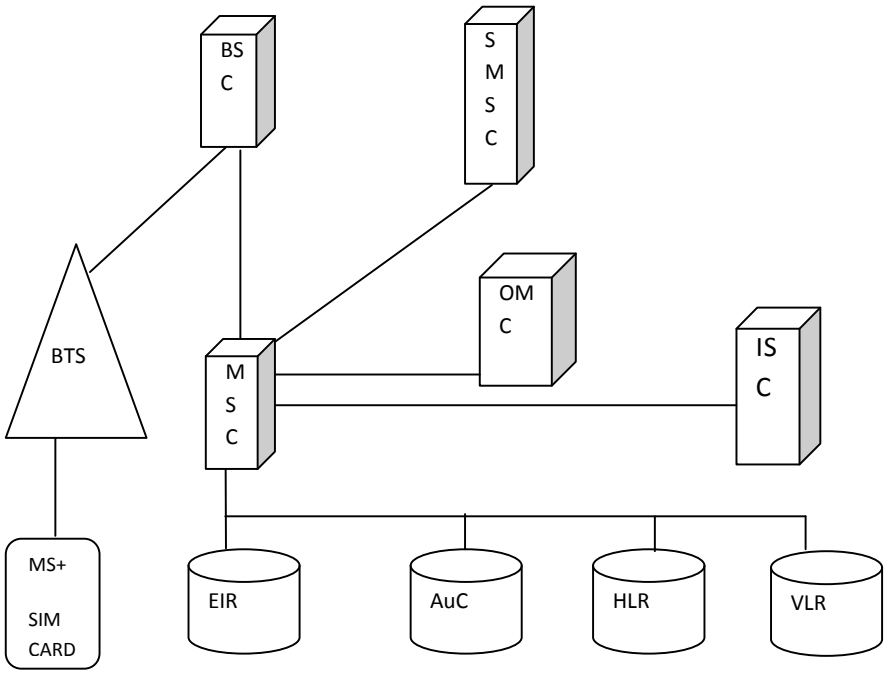


**Figure 2.2: A Traditional GSM architecture**

If the signal that is received is an SMS message it is forwarded to the Short Message Service Centre (SMSC) for delivery with a copy remaining in the SMSC. The International Switching Centre (ISC) is used for international connections.

Equipment verification and user authentication are tasks performed by the Equipment Identity Register (EIR) and Authentications Register (AR) databases respectively. Maintenance operations are controlled by the Operation and Management Centre (OMC). The Authentication Centre (AuC) is a database that keeps the Ki, the A3 authentication algorithm, the A5 ciphering algorithm and the A8 algorithm that generates ciphering keys. It creates the sets of random numbers (RAND), Signed Response (SRES) and the Cipher Key (Kc) and the sets are then stored in the HLR and VLR (Rhee, 2009).

### 2.3.1 Control Channels in GSM

GSM uses a variety of channels in which data is carried namely *traffic channels*, which are reserved for user data and *control channels* which are used for network management messages

and channel housekeeping tasks (Singh, Kumar, & Liu, 2011). Control channels are categorized into four namely

- broadcast channels
- common control channels
- dedicated channels
- associated control channels

For the purposes of this research we look at the broadcast channels whose function and components will be referred to later in the document. Table 2.1 lists the broadcast channels and explains their use.

**Table 2.1: Broadcast channels (BCH ) in GSM**.

| Control Channels | Usage |
|---|---|
| Broadcast Control Channel (BCCH) | Broadcasts continually on the downlink information like on which frequencies the neighboring cells may be found, different cell options and access parameters. |
| Frequency Correction Channel (FCCH) | Synchronises the mobile to time slot structure of a cell by defining the boundaries of burst periods and the time slot numbering. Every cell in a GSM network broadcasts exactly one FCCH and one SCH which are by definition on time slot number 0 within a TDMA frame. |
| Synchronisation Channel (SCH) | |

**Source** (Yousef, 2004)

### 2.4 GSM security

Cellular communications are sent over the air thus are less secure than wired networks as this introduces the possibility of eavesdropping with appropriate receivers (SANS Institute, 2001). GSM has built-in security functions meant to guide against subscriber privacy which include

- Securely stored authentication keys ($K_{Is}$)
- Rejection of duplicate SIMs on the network

- Authentication allowed for registered subscribers only.
- Data transfer security through encryption
- Subscriber identity protection
- Mobile phones rendered inoperable without a SIM card.

The security services provided by GSM are:

- ***Authentication*** - to allow the operator to know who is using the system for billing purposes
- ***Anonymity*** - To make it difficult to identify a system user.
- ***User data protection*** – to protect user data passing over the radio path
- ***Signaling protection*** – To protect sensitive information like telephone numbers on the signaling channel

### 2.4.1 GSM Algorithms

GSM makes use of security algorithms to enhance security. The strength of these algorithms is directly related to the suitability of GSM in delivering security sensitive services like mobile money. In order to understand security issues brought about by using mobile money over GSM it is necessary to have some basic knowledge about the algorithms in use. There are three algorithms in use namely:

- ***Authentication algorithm A3*** - which is one way function, implying that computing the signed response (SRES) using A3 is very easy but its complex to retrieve the input parameters, random number (RAND) and authentication key ($K_{I)}$ from SRES. This ensures $K_I$ remains secret. The algorithm is operator-dependent.
- ***Ciphering Algorithm A5*** – there exists several implementations of this algorithm due to export restrictions on encryption technologies. Three variants of the algorithm are used A5/0, A5/1 and A5/2. The strongest is A5/1 and is used in America and Europe with A5/2 being used in Asia. Poor countries and those under UN sanctions use the A5/0 with no encryption.

- ***Ciphering Key Generating Algorithm A8*** – this is operator dependent and is mostly combined with the A3 to form a single hash function called the COMP128 which creates Kc and SRES on the fly.

### 2.4.2 Authentication

When authenticating a subscriber the validity of the subscriber's SIM card is checked then a check on whether the mobile station is allowed on a particular network is performed as shown on Figure 2.3. The network performs this authentication through a challenge response method whereby a 128 bit random number (RAND) is sent over the air to the mobile station. The RAND is then sent to the SIM card where it is processed using the A3 authentication algorithm and the Ki.

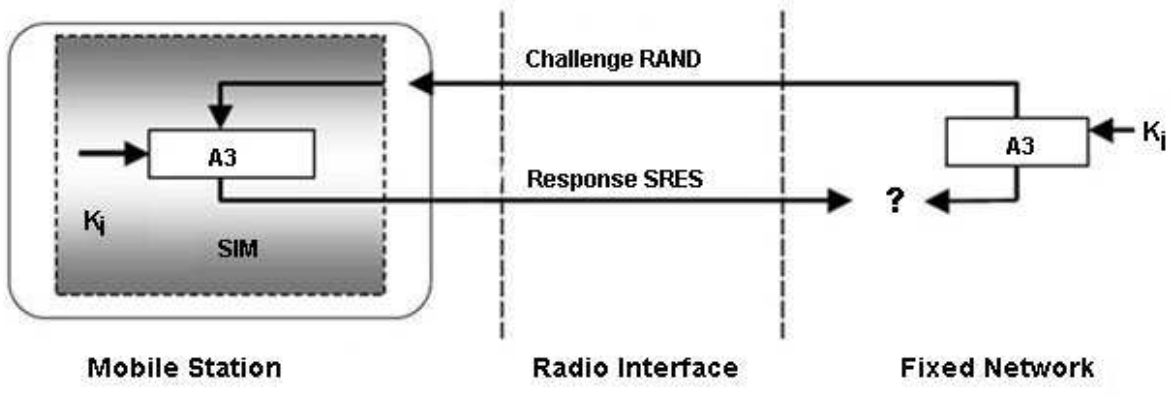


**Figure 2.3: GSM Authentication (Brookson, 1994)**

The output of this A3 algorithm is the signed response (SRES) which is transmitted back to the network via over-the-air interface back to the network. The network uses the AuC to compare its SRES (stored in the HLR or VLR) with the received SRES where a match results in the subscriber being allowed on to the network (SANS Institute, 2001).

### 2.4.3 Anonymity

Anonymity is achieved by using temporary identifiers called the Temporary Mobile Subscriber Identity (TMSI). The TMSI is issued the first time a subscriber switches on the mobile phone and the IMSI reaches AuC to prevent the use of the IMSI. Unless if it is really necessary, the IMSI is never transmitted beyond this point. This makes it difficult for a potential eavesdropper

to track the GSM subscriber using the IMSI. All further communication between the network and mobile subscriber will be done using the TMSI as the unique identifier of the subscriber. The TMSI is only changed during a location update of which a new TMSI is immediately allocated by the VLR which manages TMSI assignment. Should the mobile station be switched off the SIM card stores the TMSI for the next time (Golde, 2012).

### 2.4.4 Encryption and Decryption of Data

A ciphering key is used by GSM to protect both signaling and user data on the susceptible air interface. After authenticating a user on the network the RAND originally from the network together with the SIM's Ki are sent through the A8 ciphering key generating algorithm producing a ciphering key (Kc). The resultant Kc from the A8 algorithm is used with the A5 ciphering algorithm to encipher or decipher data. The SIM card has stored on it the A8 algorithm while A5 algorithm is resident on the hardware of the mobile phone to allow it to encrypt and decrypt data on the fly.

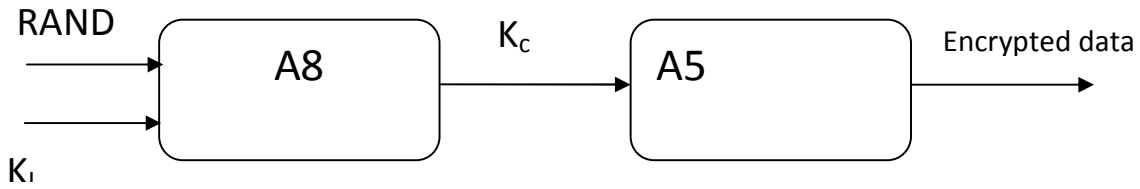


**Figure 2.4: GSM data encryption using a ciphering key**

### 2.4.5 GSM Architecture Security Weaknesses

GSM has got limitations in security issues such as lack of data integrity and cryptographic issues with regard to authentication and encryption algorithms (Abunyang, 2007). The A5 encryption algorithm commonly used has been reverse engineered. The A3/A8 authentication algorithm have been proven to be vulnerable after flaws were indentified (Abunyang, 2007; Rao, Rothagi, & Scherzer, 2002; Van de Merwe, 2003). The security of mobile money is dependent on the security of the backbone GSM components it rides on. If the GSM security is compromised this has an effect of affecting mobile money transactions.

A survey has revealed that more than two thirds of smart phone owners are yet to adopt mobile banking applications because of security issues (Ashford, 2012). The survey further states that only fourteen percent of PC-based online bankers confessed security based hindrance (Metaforic, 2012). The GSM standard was created in secrecy hiding all the used algorithms from the public domain. This implies they can be attacked and compromised easily if they lose this obscurity (Chemwe, 2010). Analysts argue that a system not exposed to scrutiny by the world's most able minds can not be referred to as very secure (SANS Institute, 2001). Mobile money cash transfer and banking application security ride on GSM security thus is also affected.

Many of the valuable aspects of GSM can be attacked. GSM's privacy, authentication and confidentiality mechanisms can be compromised by an attacker with the correct tools. To break protection an attacker needs to use active attacks, which is base station functionality. If the attacker can decrypt GSM traffic i.e A5/1 and A5/2, passive attacks are enough (Yousef, 2004).

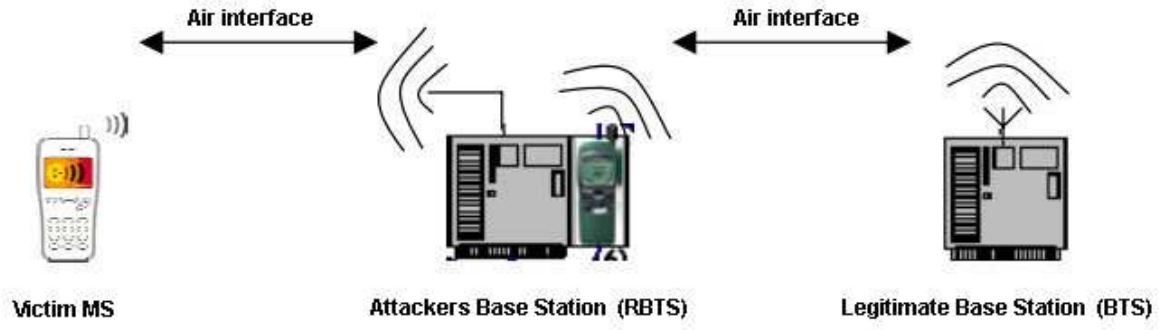


**Figure 2.5: Mounting a man in the middle attack (Yousef, 2004)**

The cryptographic algorithms used to encrypt GSM traffic are cryptographically weak and can be cryptanalysed in real time affecting confidentiality (Matuszewski, 2012). Though cryptanalysis of A5 algorithm is difficult and requires huge amounts of computational power, GSM does not provide satisfactory security for users with valuable information to communicate (Yousef, 2004). GSM security functions are adequate for normal cellular communication but are however not suitable for mobile commerce applications traversing these networks (Van de Merwe, 2003). Mobile money falls in this category. An additional layer of security would be advisable for such users.

GSM has one way authentication which allows false base stations to be setup as shown in Figure 2.5. It is only the network that authenticates a subscriber who attempts to log on to it but the subscriber has no way of checking the legitimacy of the network they are connecting to (Toorani and Beheshti, 2008). The presence of communication in GSM does not identify the originators uniquely (Gold, 2011). The wireless infrastructure that terminals use to access the network makes these technologies vulnerable to attack (Rizzo and Brookson, 2014). The ubiquitous nature of wireless networks make GSM very susceptible.

It is technically feasible to perform man in the middle attack by creating a rogue base station (RBTS) to fool a mobile station as shown in Figure 2.5. When a mobile station is turned on it orients itself with the network by synchronizing itself in frequency and time then reading system cell data from the BCCH (Yousef, 2004). The mobile station finds the frequency where the FCCH, SCH and BCCH are being transmitted.

GSM requires that a base station transmit something in every time slot of the base channel which is the broadcast carrier. Base channel is the network beacon that contains the FCCH, SCH and BCCH. If a base station tasked with broadcasting the base channel fill its time slots the power density for its frequency becomes higher than any of the other channels which may utilize only a few of the allocated eight. This uniqueness of the base channel makes it simple for an attacker to pick the right frequency (Yousef, 2004).

Since a mobile station looks for physical channels with the highest power levels, an outsider who can transmit dummy outbursts more frequently can fool a mobile station. The attacker will then manage to control traffic between the mobile station and the real network as well as messages in the other direction.

The attack described above is called man-in-the-middle attack. It allows the attacker to eavesdrop, modify, delete, re-order, replay, signaling and user data messages exchanged between the mobile station and the legitimate network (Gadaix, 2001). Mobile money users who use GSM to transmit alerts for financial transactions can fall prey to this kind of attack.

GSM does not use public key encryption citing speed issues but public key cryptographic approach is the best way of authentication and securing the communication used on financial transactions (Khan and Ullah, 2010). Today there is an increase in computing power accessible

at lower cost meaning cryptosystems must be able to resist brute force attacks which were thought unthinkable in the past. The algorithms should be the source of strength not the keys. GSM takes ciphering of information sent over the air as one of its security aspects but the ciphering algorithms for data encryption are weak (Matuszewski, 2012). To enable trust of terminal identity in MFS public key encryption as shown in Figure 2.6 is essential.

Mobile money systems require special security where terminals can trust each other. The public key cryptography authentication shown in Figure 2.6 enables terminals to trust each other therefore making mobile money transactions secure.

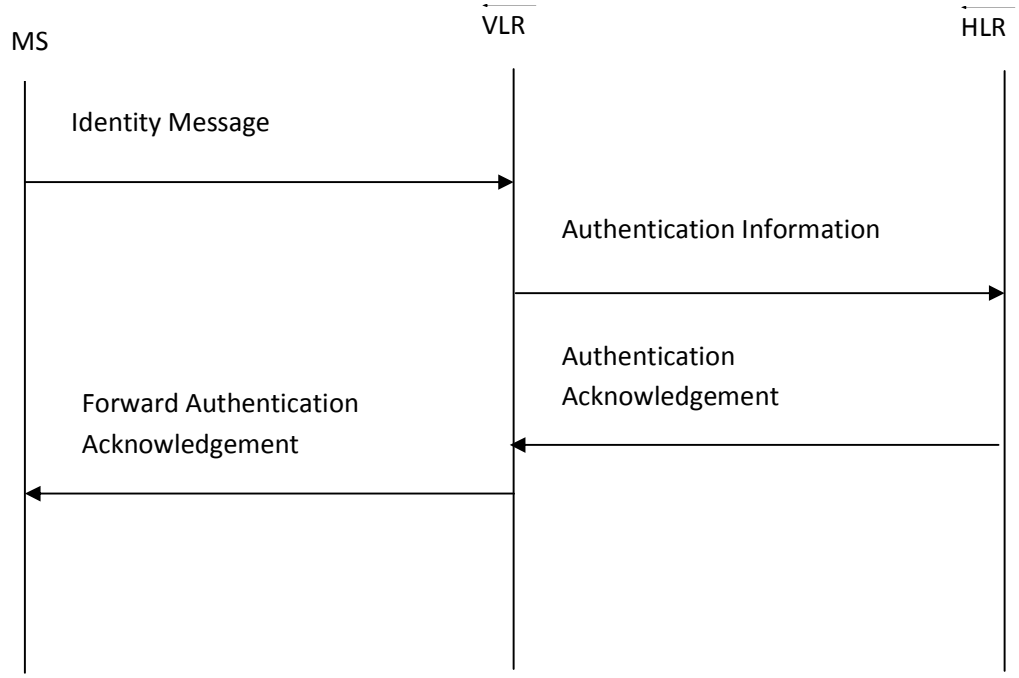


**Figure 2.6 : Public key cryptography authentication (Khan and Ullah, 2010).**

Even though it is possible to implement the end-to-end encryption of mobile communication using Public Key Infrastructure (PKI) the prohibitive factor is the complexity of setting up the infrastructure and the fact that most users of mobile phones are not well versed in cryptographic procedures. Users may become overwhelmed when faced with public and private keys, certificates, signatures and revocation lists (Smith, Schridde, & Freisleben, 2008) .

Cryptanalysis take advantage of the fact that traces of the structure pattern may ‘survive encryption’ and be readable in ciphertext. This loophole will make it possible to deduce the

plaintext or the key especially in COMP128. This will enable an attacker to get the secret key of a GSM subscriber (Barkan, Biham, and Keller, 2003). A3 and A8 use COMP128 algorithm and are used exclusively the world over. COMP128 was cracked in April 1998 and another named COMP128-2 was developed in mitigation. However due to the costs involved coupled with ignorance most mobile operators are still using the flawed algorithm.

To monitor the movement and call patterns of a subscriber an attacker needs to know the IMSI and TMSI of the mobile station. A mobile station performs an IMSI attach each time it is powered on to indicate the IMSI as active on the network (Dammann, 2011). A network has the capability to request for identification information from a mobile station by making use of the identification procedure whenever it fails to identify a mobile station using the TMSI. The network transfers the IDENTITY REQUEST message to the mobile station asking it to transmit a specific identification parameter using the IDENTITY TYPE information element (Yousef, 2004).

GSM does not use message authentication to check the origin of a message on the radio link (Gadaix, 2001). Attackers can use a device known as an IMSI-Catcher which masquerades as a base station to collect the IMSI of users in a target area by advising the holder of an unknown TMSI that the TMSI is invalid thereby triggering the mobile phone user to send the IMSI again. The IMSI-Catcher can be used to track or even locate a specific user using the signal strength and propagation delay (Dammann, 2011).

With this IMSI the attacker can get the TMSI which will enable the attacker to pair the IMSI and TMSI for unique identification of subscriber thus be able to track him/her. Since TMSI is offered encrypted the attacker can suppress the encryption by fooling the mobile station and the real network to believe that they are using incompatible encryption capabilities therefore A5/0 which means no encryption (Yousef, 2004). In mobile money this can be used to target a prolific customer by possibly monitoring their movements to find a time they are offline then replace their SIM card so as to perform transactions using their account. The card can even be cloned and anytime the legitimate subscriber goes offline the cloned one is switched on so as to avoid duplication detection by the network.

An attacker who captures a mobile station can send classmark information on behalf of the captured mobile station informing the network about its ciphering capabilities. The attacker sends a message to the network indicating that it can only use A5/2 or A5/0 (no encryption). Later on when calls are made by the specific captured mobile station, the network will cipher using the earlier specified methods preferably A5/0. The attacker does this to suppress encryption between the target user and the true network (Gadaix, 2001).

An attacker who has captured a mobile station will ask the mobile station to inform about its ciphering capabilities by sending it a CLASMARK ENQUIRY message. The mobile station then responds with a CALSSMARK CHANGE message that contains a mobile station classmark 2 information element. On receiving the CALSSMARK CHANGE message the attacker edits the parts that have to do with encryption capabilities to fool the network into believing that A5/1 and A5/2 are not available to the mobile station. This is done by altering the bits used to indicate encryption algorithm availability for A5/1, A5/2 and A5/3 to 0 as 1 indicates availability.

The attacker then passes the edited classmark information to the unsuspecting network. The network may decide to establish an un-ciphered connection, after which decision the attacker relinquishes connection with the true network and impersonates the network to the target user. From this point onwards all the messages transferred between the mobile station and the legitimate base station will not be encrypted allowing the attacker to eavesdrop.

A subscriber roaming in a foreign land will request a call establishment process when they wish to make a call. The serving VLR of the foreign network does not have the Ki of the subscriber hence request for authentication information from the home network of the subscriber (HLR). Five triplets of RAND, SRES, Kc are then sent to the hosting network's VLR and it authenticates the visitor. Only one set of the triplets is used with four being retained for future use to avoid querying the HLR so often. There is no guarantee however that the hosting network or personnel administering the databases containing such information will be wholly ethical and not think of making financial gain using unorthodox means like selling the data.

All networks based on 3rd Generation Partnership Project (3GPP) standards like Universal Mobile Telecommunications System (UMTS), General packet radio service (GPRS), Enhanced Data for Global Evolution (EDGE) and Long Term Evolution (LTE) resort back to a basic 2G

(Global Systems for Mobile Communications, GSM) connection when connection on 3G and beyond can not be achieved (Jover and Giura, 2013). Reasons for this fallback are usually an attempt to balance traffic or because reception on the desired radio band is impossible.

It is known that 2G networks provide weak encryption and are not secure (Al-Muhtadi, Mickunas, & Campbell, 2002) . The lack of dual authentication in GSM creates potential security breaches. The fall back to 2G networks introduces potential security breaches like the jamming attack (Jover & Giura, 2013). This is achieved by deliberately transmitting radio signals to disrupt communications to make a cell phone fail to detect any 3rd Generation (3G) base station forcing a fall back to GSM for network access.

Another way to break the security of GSM just like many other systems is through social engineering. Foolish as it may sound, an attacker can pretend to be a repair man and enter a suitable building then install a wire tap. It is also very possible that the attacker can bribe an engineer to do it for him or give him all the $Ki_s$ for all subscribers of the network.

### 2.5 SIM Card Security

SIM cards are the de facto trust anchor for mobile devices worldwide but are vulnerable to SIM cloning[4] which is a great threat (Matuszewski, 2012; Vincent, 2013). These SIM cards associate mobile devices with phone numbers, protect the mobile identity of subscribers and store payment information in NFC-enabled phones and mobile wallets (Vincent, 2013). A subscription can be cloned by having access to the physical card or over the air interface (Brookson, 2005). Cloning a subscription over the air requires base station functionality (Yousef, 2004).

In the case of GSM mobile money that make use of SIM Toolkit one of the security strengths lie in having the physical SIM in person. Once the SIM card is cloned it will appear as if it has been replaced hence the MFS platform will allow the new card holder an opportunity to key in a new personal identification number (PIN). This will allow the attacker to freely perform transactions as if they were the legitimate owner of the account. SIM cloning is thus a great danger to mobile money over GSM.

[4] http://www.wisegeek.org/what-is-a-sim-clone.htm

There are over 7 billion active SIM cards in use worldwide making the SIM a widely used security token whose security is based on nothing else other than what the manufacturers claim (Nohl, 2013). SIM cards are extensible through custom Java software administered using over-the-air (OTA) updates deployed via SMS. Though this extensibility is rarely used currently its existence poses a critical hacking risk (Srlabs, 2013). Extensibility is the ability to add new software functionality to the SIM cards.

The OTA commands like those used for software updates are cryptographically secured SMS messages delivered directly to the SIM. Whilst there exists state-of-the-art Advanced Encryption Standard (AES) or the outdated 3DES algorithm for OTA many SIM cards use the 70s- era Data Encryption Standard (DES) cipher (Srlabs, 2013). DES keys have long been considered to be insecure with Nohl's method managing to compromise the encryption within two minutes on a standard computer (Vincent, 2013).

An attacker starts by sending a binary SMS to a target device in order to derive a DES OTA key. A SIM card does not execute an improperly signed OTA command but responds to the attacker with an error code carrying a cryptographic signature that is also sent over binary SMS. This plaintext signature tuple can be resolved using a rainbow table[5] to a 56-bit DES key within two minutes on a standard computer (Nohl, 2013).

The DES key obtained enables an attacker to send correctly signed binary SMS which can download java applets on to the SIM card. Java applets on a SIM card are amongst other things, allowed to send SMS, query telephone location and change voice mail numbers. These capabilities can be exploited if availed to a malicious user. Nohl in his research also noted that the Java sandbox of at least two major SIM card vendors are not secure (Srlabs, 2013). A Java applet can break out of its realm to access the rest of the card which allows for remote cloning of millions of SIM cards including their International Mobile Subscriber Identity (IMSI) and authentication key (Ki) together with payment information stored on card. Over 750 million users around the world are affected by SIM cloning (Kumar, 2013).

In the telecommunication business subscribers often lose their SIM cards for different reasons prompting mobile network operators to offer replacement SIM cards. Depending on how

[5] http://www.project-rainbowcrack.com/

rigorous the SIM replacement processes are in checking the authenticity of credentials presented by the SIM replacing subscriber, chances are an attacker can replace a SIM that belongs to a target. Until such a time as and when the legitimate subscriber raises alarm, the attacker can access the MFS account of the victim. This is especially true for SIM Toolkit based MFS services like NetOne's OneWallet because they offer new PIN prompts for every SIM swap.

### 2.6 Handset Security

In addition to the security concerns posed by GSM, the mobile stations used by subscribers have their own security concerns. This broadens the attack surface (Metaforic, 2012). Threats targeting smart phones and tablets have reached levels where they pose meaningful challenges to users and service providers (Juniper Networks, 2012). Malware threats to mobile phones is anticipated to grow as functionality of mobile phones is enhanced (Yan, Li, Li, & Deng, 2009).

All popular mobile operating systems are similar in that they support some kind of mobile device management (MDM). The devices only differ in the way they support MDM. Some mobile operating systems have device-native capabilities while others require third party MDM agents. For users of smartphones and tablets manageability depended on the mobile operating system capabilities. Ultimately, security depends on device make and model and the mobile operating system and version (Phifer, 2013). Mobile device used and mobile operating system used is of importance to mobile money users.

There are numerous factors on which resistance of mobile operating systems to malware depend. Users should be concerned about the history of an app store (app store provenance) and should not install applications sideloaded[6] from less trustworthy sites. Preventing installation of public applications from sources that are not trusted has proven to be an effective malware deterrent measure basing on results from Apple that exerts tight control over the iTunes App Store in comparison to the more relaxed Google Play Store oversight that caused an increase in Android malware (Phifer, 2013).

Mobile devices and applications have become critical to the lives of people. They are now ubiquitous and produced in volumes such that in 2011 alone mobile handsets shipped were 1.6

[6] http://searchconsumerization.techtarget.com/definition/sideloading

billion with 66.9 million tablets (Juniper Networks, 2012). This high volume of devices gave rise to a wide range of possibilities for users to interact and manage personal data while mobile. Smartphones are becoming the major means for people to access information or share it. These opportunities however open avenues for hackers (Jorja, Dawson, & Omar, 2012). Malware is increasing at an exponential rate.

Mobile malware has become smarter and new technology on mobile phones has brought new breed of attack. Google Android platform is the hardest hit because of its dominant share in the market and lack of control over applications in the Android application store (FBI and Department of Homeland Security, 2013). Most users of mobile money over GSM in sub Saharan Africa have handsets that use this mobile operating system therefore would be vulnerable to attacks on Android.

Malicious actors continue to find new ways to exploit vulnerabilities and human behavior. Application stores are becoming the delivery point of infected applications as more and more users are downloading applications. The number of application developers has surged and so has that of attackers. Juniper MTC reports an evolution from ‘more sophisticated, complex and deep attacks to attacks that are light weight, fast and application based (Juniper Networks, 2012).

In the PC world malware consists to a greater extend of spyware, Trojans, worms and viruses while for mobile devices most of the malware is spyware and Trojans which come as applications or functionality hidden in applications. There are more malware samples for PC as compared to mobile malware for the sole reason that PC malware needs to evolve to remain potent against anti-malware capabilities available on PCs (Yan et al., 2009). PC security vendors add identifying signatures to pick malware they would have discovered, thus an attacker needs to modify their malware to circumvent detection thereby creating more malware sample.

However mobile malware is a cause for serious public concern since the population of mobile phones is greater than that of PCs and a greater number of these mobile devices lack end-point anti-malware solutions as yet. There were 96% of smartphones without pre-installed security software in 2012 (Jorja et al., 2012). Malware writers simply create malicious applications which they post to application stores waiting for a user to unwittingly download and install.

Even though operating system developers like Apple and Google now have the capacity to remotely remove malware from devices that downloaded it from official application stores, a workaround has been found by malware developers that modifies versions of common types of malware to escape removal. Moreover downloads from the web and other third party sources are not mitigated by this remediation from Google and Apple (Juniper Networks, 2012). Most users use these third party application stores.

Prior to 2011, the majority of malware targeted Nokia Symbian and Java ME devices but now there is a great shift towards Android. The statistics are as shown in the Figure 2.7 and Figure 2.8

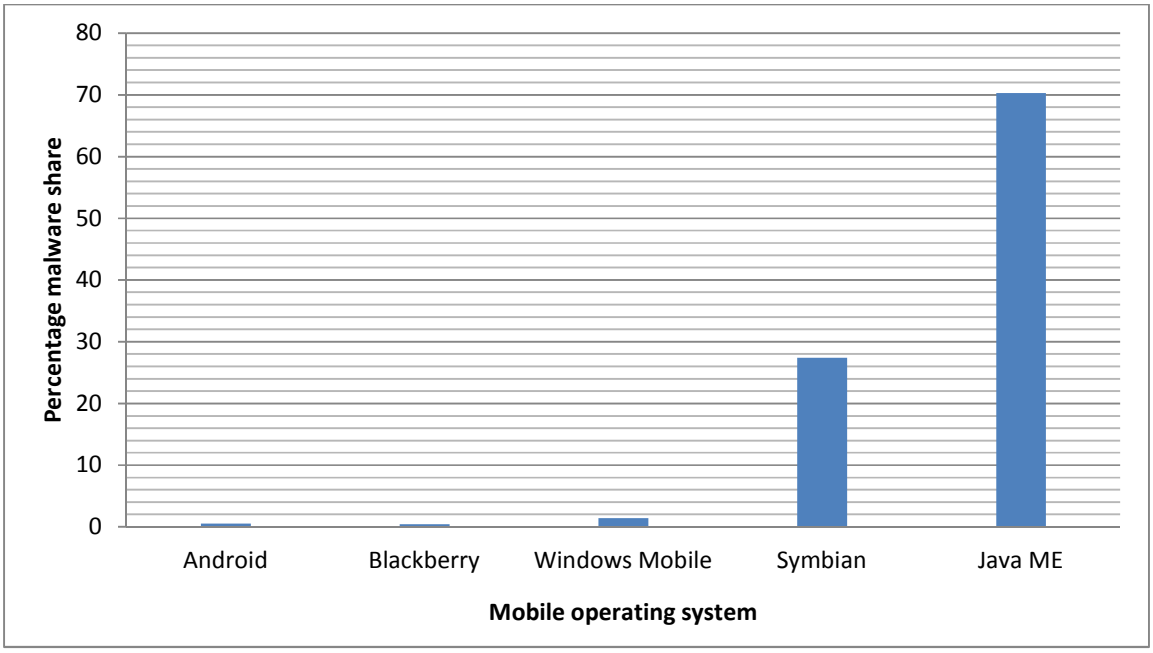


**Figure 2.7: Percentage malware by mobile operating system in 2010** (Juniper Networks, 2012)

Android began to attract a huge share of the malware after 2011. The malware patterns changed to proportions shown by Figure 2.8.

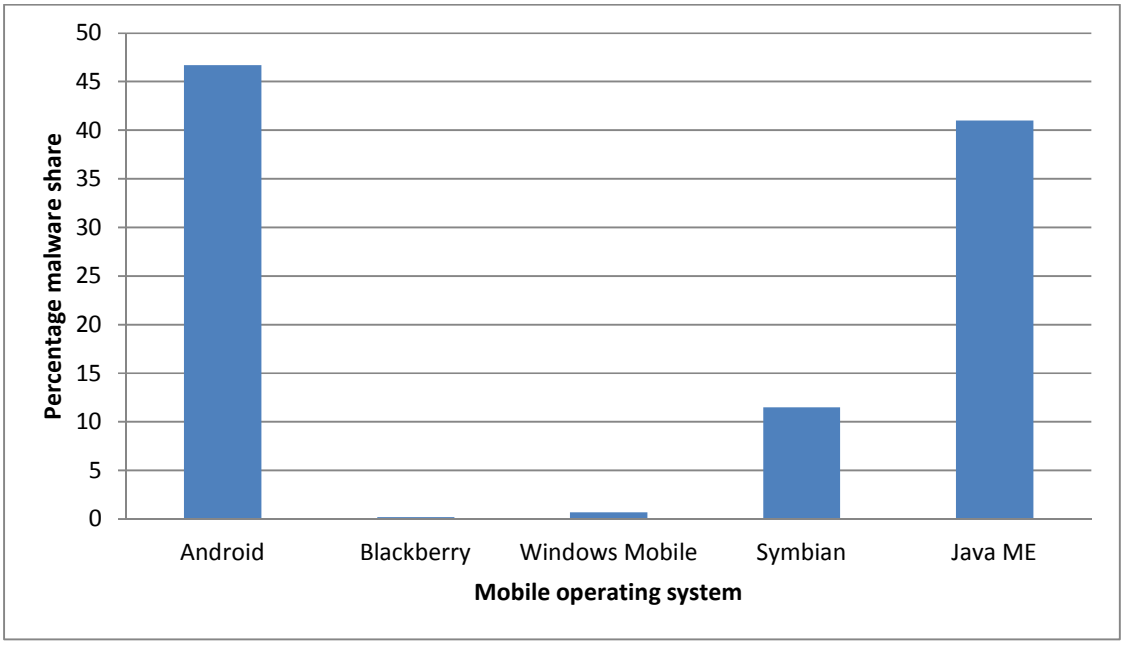


**Figure 2.8: Percentage malware by mobile operating system after 2011** (Juniper Networks, 2012)

A study found that from 2009 to 2010 the vulnerabilities in mobile operating systems rose by 42% (Ruggiero & Foote, 2011). The Juniper MTC identified that there was a 155% increase in mobile malware across all platforms in 2011 as compared to 2010 showing a high level of maturity for the emerging threat. Android was mostly affected by a form of malware called spyware in 2011. Spyware has the ability to capture and transfer data such as GPS coordinates, text records or browser history without providing an explicit means for the user to identify the application's actions (Dimov, 2013).

Another form of malware that affects mobile devices is SMS Trojans and accounts for 36% of mobile malware. These run quietly in the background clandestinely sending SMS messages to premium rate numbers owned by attackers. In addition to outright malicious applications meant to steal information or money from user, there are also many suspicious applications that compromise privacy by sharing information with a third party (Wright, 2012).

Juniper MTC noted that, 30.0% of applications can obtain device location without user's permission, 14.7 % of applications request permissions that can allow them to initiate phone calls with the user not knowing, 6.0 % of applications request ability to scan accounts on the device

including email and social networking sites, and 4.8 % of the applications were able to send SMS messages without user consent.

The ability of malicious applications to perform clandestine actions on a users' handset presents a huge security challenge to mobile money applications. In addition to challenges presented by the GSM network the handset the subscriber uses presents an extra attack surface.

### 2.6.1 Google Android: The Advantages and Risks of Popularity

To get a general idea of the extent of the threat to mobile money brought about by the mobile handset the subscriber uses, the most popular mobile operating system, Google Android, was used.

The rapid rise of Google Android operating system adoption made it so popular overtaking strong incumbents like RIMs BlackBerry and Apple's iOS. Since its release in 2007 until the end of 2011 its market share grew to 46.9% with the nearest competitor, the iOS platform coming distant second on 28.7%. The open nature of the Android platform and the Android market simplified it for developers to bring applications to the market quickly, such that there was half a million published Android applications and 10 billion application downloads in 2011 (Juniper Networks, 2012).

The majority of malware programs have Google Android as their main target because Android is the most popular mobile operating system and developers can easily distribute applications through the Google Play application store (Jorja et al., 2012). The same traits that make it succeed have created new risks. Juniper MTC found that malware targeting the Android platform rose by 3.325% to 13,302 samples in seven consecutive months of the year 2011 (Juniper Networks, 2012). Potential attackers look for high return on investment and naturally target the largest audience in the same manner Microsoft Windows is targeted in the computing world.

Android's open application market place simplifies the way attackers reach victims. The official Android Market allows developers to post applications and have them available immediately without vetting to block unwanted applications (Ruggiero & Foote, 2011). Though Google has been quick in removing malicious applications from the official market place, the detection and

deletion process takes days by which time a successful attack would have occurred (Juniper Networks, 2012).

The ability of Android devices to download content from anywhere is a huge security negative. This has seen the sprouting of unofficial third party application stores that make no effort to rid themselves of malicious applications.

Android has challenges when it comes to updating its operating system. Its open source model relies on mobile device manufacturers to push security patches through the devices. Controlling the operations of device manufacturers is not feasible. Some device manufacturers build customized versions of the Android operating system, thus certain devices either fail to receive or have to wait to get security updates. This implies that even patched security vulnerabilities or new security features may not get to all devices rendering them less secure (Juniper Networks, 2012).

### 2.6.2 RIM's BlackBerry and Other Platforms

Malware targeting RIM's BlackBerry and Nokia's Symbian and other major operating systems continue to grow albeit at a slower rate than prior. BlackBerry devices were found to be infected by Zeus Trojan. Devices affected by this malware enabled criminals to obtain user credentials to initiate online banking sessions. Mobile devices running Symbian Series 60 platform are affected by a Bluetooth worm called Cabir if they are left in discoverable mode (US-CERT, 2010).

Other major mobile platforms still have the threat of malware though the threat is growing at a rate less than that of Android. There were 3851 new malicious Java ME samples collected in 2011 showing that even though Symbian and Windows mobile devices dwindled in the market compared to Android and iOS, there exists enough users to attract the attention of Java ME malware developers (Juniper Networks, 2012). Users of GSM mobile money use mobile stations that make use of these mobile platforms thus are prone to threats that target these platforms.

GSM mobile money makes use of SMS platforms. The idea that most of the mobile platforms in use by a majority of mobile stations have a chance of having malware sending SMS text messages originating from them without the user's consent means the inclusion of an SMS component in GSM mobile money transaction flows can be exploited (Juniper Networks, 2012).

SMS was meant for users to transmit non sensitive information over GSM without special emphasis on issues like data confidentiality, mutual authentication, end to end security and non repudiation (Abunyang, 2007). There are SMS simulators that can send an SMS text message on behalf of a user, for example those developed using SMS gateway software like OzekiNG. This is referred to as message spoofing. To accomplish it an attacker sends messages that appear to be from a legitimate user by simply editing the originator address in the field in the SMS message header (Abunyang, 2007). The originator field can be changed to another alphanumeric string thereby enabling masquerading attacks.

The SMS centre servers hosted by mobile network operators store copies of SMS messages (Abunyang, 2007). This property coupled with the default plaintext data format of SMS implies that any person with access to the SMS centre server can easily see sensitive information. Encryption in the GSM system exists only between the mobile phone and the base transmission station with end to end protection being currently unavailable.

### 2.7 Mobile Money Uptake Rate in Africa and the Developed World

Demographics and socioeconomic forces have an impact on mobile money services uptake (Penicaud, 2012). Regulation is the only external factor that can hinder the progress of the service. Penicaud (2012) notes that following best practices is critical for service adoption but there is need to adapt services to the local market context. For the service to survive in markets with diverse demographic and socio-economic circumstances operators need to design the product to fit the specific market needs.

The uptake rate of mobile money has been skewed globally in favour of the developing world. Six of the eight fastest growing mobile money providers are in East Africa (Smart City Magazine, 2013). Developed nations have more subscribers with smartphones which demands a more sophisticated service such as can be attained using technologies like NFC and QR codes (Smart City Magazine, 2013).

In the United Kingdom 23% of consumers are willing to use mobile wallet instead of cash for purchases (Moran, 2011). This figure rises to two thirds if the survey is conducted amongst smartphone owners only (Boden, 2014). Above half of those interviewed would use a mobile wallet if their security concerns were addressed (Smart City Magazine, 2013). Only 15% of

consumers would use it for larger payments with the remainder wary about security. These findings indicate that security and the enabling technology are key factors which need to be addressed if mobile money uptake is to improve in the developed world.

The mobile money ideology has been around in developed nations for some time but the demand for adoption has been absent. People can easily access banks, ATMs, online banking and other financial services thus mobile money has been less appealing and not a necessity. Rich nations have cash machines, credit cards, internet banking therefore do not see the need for mobile banking (The Economist, 2012). Developing nations like Kenya have populations with less access to traditional banks and infrastructure is underdeveloped. This has driven the massive embrace of mobile money (Cheney, 2008). In developing nations mobile money adoption has more to do with convenience than need for the service (Cheney, 2008).

A tenth of the population say they may use the service in the future while 36% of those interviewed were ignorant of the cashless payment capabilities available on their mobile stations which make use of the near field communication technology (Moran, 2011). The anticipated benefits cited by most of those intending to use NFC enabled mobile wallet in future was convenience to pay, speed in paying and the advantage of not carrying cash and credit cards. Reasons cited for unwillingness to use mobile payment were satisfaction with current payment methods and fraud and security concerns (Moran, 2011).

The major reason why subscribers are not anticipating using mobile payment options in future is that they are content with the way they transact now. Sixty seven percent of the population has no plans to use mobile money in the future. Any new technology will always face consumer concerns ranging from data security, changing of mobile provider and the reversal of mistaken payments which are genuine worries that must be eliminated first for consumers to adopt mobile money (Smart City Magazine, 2013).

There are bankers who feel that mobile money and branchless banking is a direct challenge to basic norms of banking and they are against this idea. They feel that they have to be selective of their customers so as to serve higher value customers instead of the general masses. They find retail payments and money transfers as uninteresting issues. Mobile money will reduce the profitability of these bankers therefore they are against it (Mas, 2013).

Mas (2013) noted that if mobile money in its electronic form does not connect with the way people use their money it will not be accepted as a primary mechanism for holding value by most people. He also notes that as long as people continue to be in possession of cash rather than the electronic money retailers will be unwilling to take payments in electronic money. If the general populace learns to hold electronic money then shops will also use it.

There are a range of mobile wallet products that are being introduced to the market with the sole aim of persuading the developed world to use mobile money. Such products include Google Wallet, Apple's PassBook and Visa. They are all trying harder to get a satisfactory share of the mobile money market. Sayid (2012) notes that there need to make the service secure, accessible and less difficult to operate to increase the uptake rate.

The explosive growth of mobile payments has been noticed in the developing world mainly because of the fewer options to cash available in these markets (Jimenez and Vanguri, 2010). A large number of trials lack the size and connections to the financial ecosystem needed to succeed in areas where there is no banking or telecommunications presence.

### 2.7.1 General Factors Affecting Uptake of Mobile Money

Accessibility is a key factor in the choice of a way to send and receive money (Tobbin and Kuwornu, 2011). Perceived usefulness and ease of use are also very important factors of system adoption and use (Tobbin and Kuwornu, 2011). Research done on the adoption of mobile money can be seen as the same when compared to research previously done for mobile banking and mobile payments. This makes it possible to argue that m-banking and m-payment adoption determinants can be applied to mobile money (Tobbin and Kuwornu, 2011). There are a number of models that have been used by scholars in the last twenty years to come up with determinants of technology adoption which also apply to mobile money (Nzoutchoum, 2012).

There is the diffusion of innovation theory (DoI), the technology acceptance model (TAM), theory of planned behavior (TPB), the extended technology acceptance model and the unified theory of acceptance and use of technology (UTAUT). The premises under which the models are established are key to the adoption of any technology (Nzoutchoum, 2012; Tobbin and Kuwornu, 2011). Mobile money services studies have shown that the application of these information

systems theories and models have included value added mobile services (Tobbin and Kuwornu, 2011).

Perceived usefulness and ease of use are the premises under which TAM is established (Barati and Mohammad, 2011). Perceived ease of use is defined as the degree of effortlessness in using a certain system. TAM has proven to be a useful theoretical tool and has received extensive empirical support through validations, applications and replications (Tobbin and Kuwornu, 2011).

Diffusion of innovation theory (DoI) is another that can best explain consumer behavior towards a new technology. Innovation is an idea, object or practice which an individual or adoption unit considers new, while diffusion is the process of communicating and spreading the innovation among members of the adopting set. Basing on these definitions innovation diffusion is attained by how a social system accepts and uses a technology.

Innovation according to Rogers (1995) has the following characteristics, relative advantage, compatibility, complexity, trialability, observability. Relative advantage is the extent to which an innovation is better than the predecessor practice. Compatibility is how in line the innovation is with what people do.

Complexity is how difficult or easy it is to use the system. Trialability is the degree to which one can experiment with the innovation before making a decision to adopt or discard. Observability is how the innovation results are noticed by others.

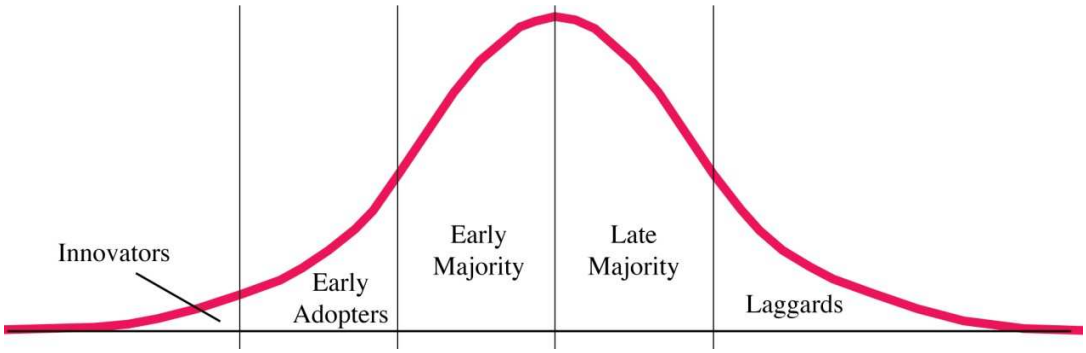


**Figure 2.9: Multi-Step Flow Theory Diffusion of Innovations Theory** (Rogers, 1995)

Rogers explains the dynamics that occur whenever people adopt a new technology using the innovation adoption curve (Sahin, 2006). He further notes that there are *innovators*, *early adopters*, *early majority*, *late majority* and *laggards* in the adoption curve model.

Innovators are the brave people who pull the change, while the early adopters are those respectable people, opinion leaders who try out new ideas in a careful way. The early majority comprises of the thoughtful people who are careful but still accept change more quickly than others. The late majority is the group of skeptical people who use new ideas and products after seeing the majority using them. The last group of laggards is that group of traditional people who care about the old ways and are very critical of new ideas such that they will only embrace them when they become widely used or mainstream (Sahin, 2006). Mobile money services adoption may also follow the pattern described by the innovations adoption curve.

Adoption of mobile money is slowed down by insufficient understanding of the services (InterMedia, 2013). Amongst the top three reasons cited by respondents for not using mobile money in Tanzania, 13% cite lack of awareness about the service while 12% cited insufficient understanding of mobile money (InterMedia, 2013). Usage barriers may also be noticed when innovation is not dovetailing with existing workflows, practices or habits. This is the most common cause of consumer resistance to innovation (Nzoutchoum, 2012).

The constructs that support TMA and DoI are similar and the models are considered complementary. Relative advantage and perceived usefulness from DoI and TMA models are examples. If mobile money can positively follow constructs that support these models it will be adopted (Tobbin and Kuwornu, 2011).

There are also other constructs that are considered important for the adoption of any system, mobile money included. These are perceived trust (PT), perceived risk (PR), perceived privacy, and transactional cost (TC) (Tobbin and Kuwornu, 2011). Mobile money products should possess these qualities if they are to be adopted. These constructs have got a security inclination meaning security is also an important aspect considered when choosing a mobile money service for adoption (GaneshSankar, 2011).

Higher perceived usefulness leads to a higher behavioural intention to use mobile money (Tobbin and Kuwornu, 2011). Perceived ease of use in mobile money encompasses registration

procedures, ease of use of the payment procedures, fewer steps required to make a payment, readily available customer services, correct screen size and input capabilities and a readily available agent network. The product must be available or compatible with phones with basic features and software.

According to Tobbin and Kuwornu (2011), studies done before concluded that perceived ease of use is the main factor that determines consumer behavioural intentions. If mobile money is easy to learn and use it will be adopted. Another empirical study by (Yu, 2012) found intention to adopt mobile money to be significantly influenced by social influence, perceived financial cost, performance expectancy and perceived credibility in that order of influencing strength.

Conversely, Tan and Teo (2000) argue that attitudinal and perceived behavioural control factors, rather than social influence play a huge role in influencing internet banking. Other factors they found include compatibility, trialability, risk, customer confidence in service usage and government support for electronic commerce.

The adoption of mobile money requires a certain level of financial understanding for customers to be able to compare and evaluate the financial products on offer, such as saving products, bank accounts and payment instruments (Nzoutchoum, 2012). This means dealing with mobile money needs a basic level of financial literacy from poor low income end users. (Nzoutchoum, 2012), in a study conducted in Uganda, noted that the main issues considered by respondents in using mobile money are speed, safety, cost-effectiveness and accessibility of the service whenever making a saving or transferring money.

David and Penicaud (2011) noted that around 15% of mobile money projects lead to successful service usage. The frequency of use of mobile money is only 3% to 4.5% (Cobert, Helms, and Parker, 2012). The issues that dissuade users from adopting mobile money as noted by the Ugandan populace are unstable mobile money network or platform from the provider, liquidity constraints on the part of agents, poor customer care and inefficient registration in that order of relevance (Nzoutchoum, 2012).

The customer's intention to use a mobile technology is dependent on the mobile experience the customer possesses and the technical support the customer receives when using the mobile technology (Chung & Kwon, 2009). The customer's mobile banking experience and the

technical assistance rendered by the provider are associated with perceived ease of use and perceived usefulness (Chung & Kwon, 2009). Mobile money systems need to be easy to use and useful to the subscriber for them to be adopted.

Mobile experience according to Chung and Kwon (2009) is defined as a customer's general experience with services found on the mobile phone such as short messaging service (SMS) and gaming. Experience is deemed to boost a user's confidence in their ability to use technology gadgets in supporting their task performance. A customer's experience is vital in understanding their perceptions, attitudes as well as behaviour in technological surroundings. A user who uses mobile internet and views it as dovetailing with his her lifestyle is more likely to adopt mobile banking and thus mobile money (Chung & Kwon, 2009).

The Rasch model that looks at the probability of an individual facing challenges on performing a particular mobile banking task with respect to the individual's ability to generally adopt mobile banking assumes that individuals with lower ability are more likely to experience difficulties than individuals of higher ability (Pallant & Tennant, 2007) . This is in agreement with Chung and Kwon (2009) who view experience with technological gadgets as having a role to play in the adoption of mobile money. Technological awareness is thus a significant factor in mobile money adoption.

Dube et al (2011) in a study looking at the challenges faced by banks in Zimbabwe in promoting the adoption of SMS banking noted that the main drivers on adoption of banking technological services is mainly to do with accessibility and affordability in developing countries. The study noted the need for increased awareness campaigns to ensure customers know about the existence of SMS banking services. Mobile money services need to follow suit to lure subscribers (Dube et al., 2011). There is need to make the service affordable and accessible as well as make customers aware of the existence of the services. Uptake of financial intermediation technology is affected by cognitive and unfavorable economic issues (Carlsson, Walden, & Bouwman, 2006).

Numerous scholars and researchers agree that compatibility, where a product dovetails with the lifestyle of a user, perceived usefulness, and risk are significant indicators of mobile banking adoption. Compatibility has a strong direct effect to mobile banking adoption and is the biggest antecedent for perceived ease of use, usefulness and perceived credibility (Koenig-Lewis,

Palmer, & Moll, 2010). Perceived trust and credibility are important aspects in diminishing the perceived risk of mobile banking. Mobile money services should also manage their perceived trust aspects and credibility to have a reduced perceived risk score so as to be adopted.

The uptake of mobile banking and consequently mobile money is affected by perceived credibility which is defined as the belief that a partner is trustworthy and has the required expertise to carry out transactions (Erdem & Swait, 2004). Perceived credibility is the degree to which a would be user is convinced the service will be free of security and privacy threats (Wang, Wang, Lin, & Tang, 2003). Reduced perceived credibility makes users fear that money or personal information may be made available to third parties without their consent or knowledge in the process of using mobile banking (Luarn & Lin, 2005). Perceived credibility and consequently perceived security has a significant positive effect on the adoption of mobile money services (Wang et al., 2003).

Saleem and Rashid (2011) agree that the concerns of customers on security and technology reliability issues are hugely significant when it comes to service adoption. Security issues are important to potential users if they are to adopt a mobile money service (Yang, 2009). System configuration security and basic fees for mobile banking web connections were found to be the primary factors causing resistance to mobile banking adoption (Yang, 2009). Concerns around risk and security issues do stall adoption of mobile banking and related systems like mobile money (Brown, Cajee, Davies, & Stroebel, 2003).

A subscriber who wishes to adopt mobile banking is forced to think about issues relating to privacy, password integrity, encryption of data, hacking and the protection of individual information (Benamati & Serva, 2007). Customers will also consider information loss during mobile banking transactions done using mobile phones (Laforet & Li, 2005). Most scholars whose work has been reviewed to this end are in agreement that perceived security plays a significant role in the adoption of mobile banking and consequently mobile money.

The main consideration made by customers to switch their financial activities to the virtual channels is security (Martin, 1998). The key determinant in a consumer's decision to adopt online banking products and consequently mobile money is perceived security (Roboff & Charles, 1998; Sathye, 1999). Service versatility is also important in attracting customers to

mobile money (Saleem & Rashid, 2011). Service versatility is related to service usefulness. Saleem & Rashid (2011) thus agree that service usefulness is important to mobile banking systems.

Lee (2013) showed trust and perceived risk to be direct antecedents of intention to use a new technology service. Research work done around the world has shown that trust and perceived risk are critical factors in understanding the consumer's acceptance of information communications technologies (ICTs) in the e-business environment (Featherman & Pavlou, 2003). Trust and risk are issues related to security aspects of a system. Mobile money, as a subset of the ICT systems, needs to copy the attributes that make other ICT systems adoptable to the users. This implies mobile money services should be trustworthy and attempt to minimize the perceived risk aspect.

Scholars and researchers whose work has been reviewed to this end have pointed out the importance of perceived security, perceived usefulness, perceived cost and perceived ease of use in affecting the behavioural intention to use new technologies and thus mobile money. Users do not want to use systems that expose their personal data or money to risk. Users want affordable mobile money systems that are easy to use and make their tasks easy to accomplish.

### 2.8 Comparison of the USSD and STK Mobile Payment Technologies

Giving subscribers an STK application is like giving them a dedicated terminal looking at this from a security perspective (Kabweza, 2012; Mikesell, 2012). USSD is less secure than STK, for instance it displays customer personal identification number (PIN) in the clear whereas STK encrypts data using the triple Data Encryption Standard algorithm ( Lee, 2008).

**Table 2.2 Comparison of USSD and STK Mobile Payment Technologies**

| Technology | Secure | Universally compatible | Ergonomic (Easy to use) | No telecommunications cost imposed | No software download required | User privacy |
|---|---|---|---|---|---|---|
| SMS/USSD | ✘ | ✓ | ✘ | ✘ | ✓ | ✘ |
| STK and Java | ✓ | ✘ | ✓ | ✓ | ✘ | ✘ |

STK is ideal for financial or mobile commerce deployments. In terms of compatibility USSD is accessible from virtually every mobile phone whilst STK, though it may theoretically be said to be compatible with most phones it may practically face challenges[7].

In terms of ease of use STK does not require the subscriber to remember the exact string to dial as it is menu driven. This makes it easy for customers to use. Its drawback is that it requires the MNO to offer a new SIM card. This has an negative economic impact on the mobile network operator as the subscriber would have to obtain a new SIM card to utilize the application (Krugel, 2007). USSD does not require any specific software to be downloaded to a subscriber's SIM card or handset. STK based applications may require that the operator re-load the application over-the-air to all active SIM cards in the market every time changes are made to the application (Krugel, 2007).

### 2.9 Summary

This chapter has looked at the GSM architecture and the way GSM works. It identified the security concerns brought about by the nature of GSM, the handsets (operating system/hardware) used and the SIM cards (algorithms-A3/A5/A8). It pointed out the factors that affect mobile money in the developed world and the developing world. It looked at prior work done in Africa on adoption drivers of mobile money and mobile banking or m-commerce with a view to make this research add to that knowledge. The next chapter will outline the methodology followed to obtain the results that were achieved.

[7] http://www.advocotek.com/white-papers/TagPay%20Unique.pdf

# Chapter 3 – Methodology

## 3.1 Introduction

This chapter describes how the research data was collected. It seeks to take the reader through the processes that were involved to collect the data and the processes that will be applied to the resultant data to yield the conclusions reached at. It is the research methodology of the study that deals with research design, setting, population, sample and data collection instrument.

## 3.2 Research Design

The research was carried out using a quantitative research methodology. Questionnaires were used in the survey. The research aimed to find the statistical importance of factors in the adoption of mobile money over cellular networks. The effect of independent variables on the dependent variable (mobile money uptake) was established. The study was done using a questionnaire because of the distinct advantages of using a questionnaire. Questionnaires are cheaper as compared to methods like personal interviews. They allow confidentiality to be maintained.

### 3.2.1 Population

A population is an accessible group of people who a meet well-defined set of eligibility criteria. For the purposes of this study, the population was the whole Zimbabwean populace aged 16 years and above whether they use mobile money or not. The idea was to capture views of those who use the product to pick the traits they considered in choosing their provider as well as get the reasons why those who shun or do not use the technology do so to allow for corrections in future deployments. For this reason the eligible population was huge.

According to Zimbabwe National Statistical Agency, Zimbabwe has a population of 12 973 808 people with over 42% of them aged 15 years and below (ZimStat, 2012). About 55% of the

population, which translates to 7,1 million is 16 years and above. This is the population that is eligible to respond to the circulated questionnaires.

### 3.2.2 Sampling and Size of Sample

A sample is a subset of the population that is selected for a study. Sampling is done by choosing some of the members of a population, in order to reach a conclusion about the population as a whole (Masinge, 2010).

The sample size was determined using the Assumption(s) of Normality (Mordkoff, 2011). According to the normality assumption, all data follow a normal distribution as **n** tends to infinity or to **N** or as **N** tends to infinity or when **n** is large where **n** = sample size, **N** is population size and a large **n** was statistically proven to be **n** $\geq$30 (Mordkoff, 2011). As **n** increases the dataset becomes more representative (Rhiel & Chaffin, 1996).

For academic purposes as well as taking time, resource constraints and the lengthy of the questionnaire into consideration, 250 copies of the questionnaire were printed and distributed. Of these there were 179 that were responded to and were received. Thirty seven (37) questionnaires were discarded because of incomplete data entry or invalid responses using listwise deletion which states that if a record is missing on any one variable it should be thrown out. The analysis was done on 142 remaining questionnaires.

Convenience or non probability sampling was employed as the questionnaires were circulated to eligible people. Not every eligible person had a chance of making part of the sample since there was no prior database of all eligible respondents. The researcher thus used convenience sampling which is the rationale choice in cases were identifying all members of a population is impossible.

### 3.2.3 Data Collection

To conduct the survey physical copies of the printed questionnaire were circulated in urban and rural communities of Zimbabwe. The respondents were mainly from Harare and Midlands provinces. Harare was chosen mainly because it is a place where people with different socio-economic circumstances, from diverse cultural backgrounds from almost all towns and cities of Zimbabwe converge. From it you can find responses that are far reaching without travelling

much. Permission to conduct the survey was given with clearance from the ethics approval from Rhodes University.

Sixty percent of the respondents were from Harare. They include people from EyreCourt township (15%), Chitugwiza city (20%), Mbare Msika bus terminus (12%), the Central Business District (7%), some college students from the University of Zimbabwe (6%). The remaining 40% was derived from the Midlands province.

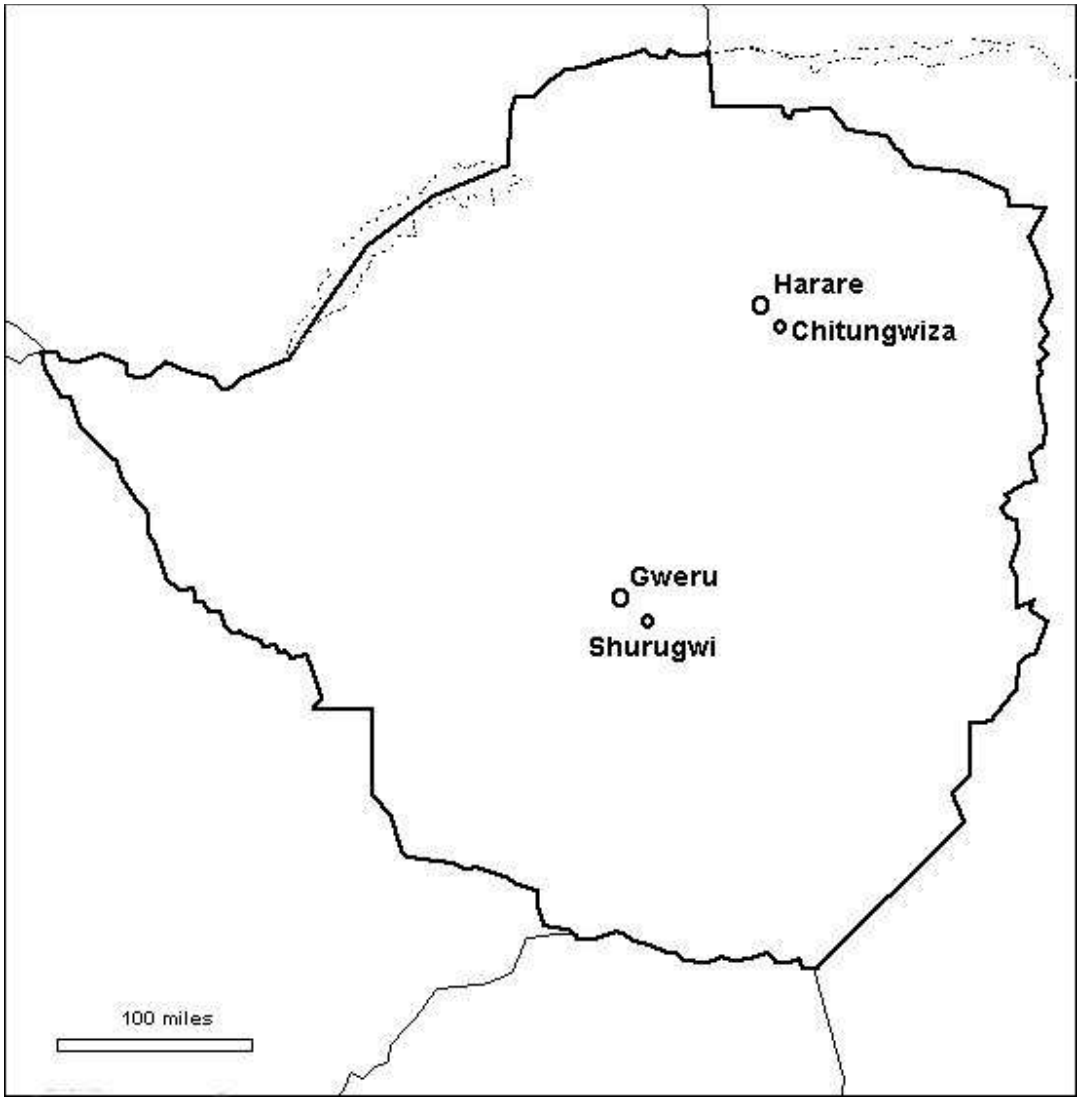


**Figure 3.1: Map of Zimbabwe**

Areas deemed representative of the rural, urban and farm setup of the Zimbabwean society were picked to ensure research data remains credible while containing the costs of the research. It consisted of respondents from Shurugwi town (23%) and the central city of Gweru (17%).

The questionnaire makes use of the five point Likert scale. Respondents can indicate their attitudes by checking how strongly they agree or disagree with statements constructed (Masinge, 2010). The questionnaire offered five alternatives: strongly agree, agree, undecided, disagree and strongly disagree. Respondents would choose from these when responding to posed questions to indicate their feelings or attitudes.

### 3.3 Pre-Test

Prior to conducting the survey a pilot study was initiated for purposes of validating the instrument. This was meant to give the researcher a clear position on whether or not the respondents were facing challenges in understanding the questionnaire. It worked as a tool to discard and iron out ambiguous or biased questions. The pre-test was sent to ten respondents in two batches of five. The first five participants were requested to provide feedback pertaining to format, length, understanding of wording and the scales used on the questionnaire. Adjustments were made and the questionnaire was printed and sent to the last five pre-test respondents. The responses were used to judge how the respondents interacted with the questionnaire. After the pre-test the survey questionnaire was circulated to the whole identified sample population.

### 3.4 Survey Distribution

Harare and Midlands provinces were the provinces in which the survey was conducted by the researcher (see map on Figure 3.1). The researcher informed the community authorities about the survey before going on the ground. The researcher assisted some respondents especially those who were illiterate on how to complete the survey since the questionnaire was written in English. English language was chosen because it is the widely used official language in Zimbabwe. The researcher explained the mobile money concept and translated some sentences into vernacular for the illiterate respondents and those who did not understand. Anyone who was 16 years and above was eligible to participate in the survey. The questionnaire was distributed in person by the researcher with respondents given time to complete the questionnaire. Some questionnaires

were collected as soon as respondents completed while some were collected from a day to a month later.

### 3.5 The Questionnaire

The questionnaire used in the survey had three parts, part A, B and C. The first part, part A, was concerned with gathering data from users of mobile money. The second part, part B, was a section for those who do not use mobile money. It meant to gather data on why they do not use the technology and what improvements could make them use it in future. The third section, part C, was a section for all respondents. It meant to gather demographic variables like gender, age, work status, education level and income level.

The questionnaire sought to ascertain whether the variables deemed independent had any statistically significance or correlation with adoption of mobile money. The dependent variable identified in the study is *adoption of money* while the independent variables identified in Chapter 2 were perceived ease of use, perceive usefulness, perceived cost, perceived security and perceived trust.

### 3.6 Data Analysis

Data from returning questionnaires was captured on to SPSS. The questions were grouped according to the applicable constructs being tested and statistical analysis was done on the collected data. The dependent variable in the study is adoption of mobile banking. The variable was grouped into three categories: users, potential users, and non users. The users were those participants who use mobile money, potential users were those respondents who do not use mobile money but intend to do so if certain conditions e.g. security aspects are met. Non users were those respondents who do not use mobile money and have no intention to use it in future.

To determine which of the independent variables had the greatest effect in determining the outcome of the dependent variable discriminant analysis was employed. There are three possible outcomes to the dependent variable which are current use of mobile money, intention to use mobile money in future or no intention to use mobile money in future. The variables analysed were perceived security, perceived ease of use, perceived usefulness, perceived cost and perceived trust.

### 3.7 Limitations

The survey questionnaire was in English language only and could possibly have affected the understanding of questions by the respondents. Even though translations in vernacular were offered some aspects have got no direct translation to local languages hence there exists a possibility that respondents could pretend to understand.

### 3.8 Summary

The chapter explained how data was obtained. It gives an overview of the limitations that exists courtesy of the data gathering instrument properties like language used. It explains how reliability of the data obtained was measured and how prior checks were made to ensure the questionnaire was understandable to the respondents. The next chapter analyses the data gathered using statistical tools. To achieve this, a software package called SPSS was used.

# Chapter 4 – Analysis

### 4.1 Introduction to Results

This chapter presents, analyses and interprets the responses that were obtained on the impacts of perceived security concerns on mobile money systems adoption. The chapter looks at the demographic information of the participants in the study and then concentrates on discussing the relationship that exists between perceived security and mobile money usage. The data for this research will be interpreted by descriptive means. A quantitative means of analyzing the data is employed for the questionnaire responses.

To evaluate the reliability of the questionnaire, we used the Cronbach's alpha. The Cronbach's alpha is a value that should range between 0.6 and 1 for it to be acceptable (Hair, Anderson, Tatham, & Black, 1998). Values above 0.6 show that measures have strong adequate reliability and discriminate validity (Sekeran, 1992). If the range is 0.6 to 0.8 it is considered acceptable, above 0.8 its good (Nunnally & Bernstein, 1994). Reliability and validity are important elements in evaluating a measurement instrument. Validity measures the extent to which an instrument measures what it is required to measure while reliability looks at how consistent the instrument is in measuring the intended aspects and the two are closely associated. Cronbach's alpha is used to measure reliability. It measures internal consistence, which describes the extent to which all the items in a test measure the same concept or construct (Tavakol & Dennick, 2011).

**Table 4.1: Construct Reliability and Validity**

| Construct | Cronbach's Alpha | Specification |
|---|---|---|
| Perceived security | 0.67 | Acceptable >0.6 |
| Perceived usefulness | 0.78 | Acceptable >0.6 |
| Perceived ease of use | 0.61 | Acceptable >0.6 |
| Perceived cost | 0.80 | Good >0.6 |

### 4.2 Demographic Characteristics

The section gives an overview on the demographic characteristics of the sample population. It looks at gender, age, race, level of education, income level, residential location as well as employment status.

#### 4.2.1 Gender of the Participants

In terms of gender 75% of respondents were male while female respondents were 25%.

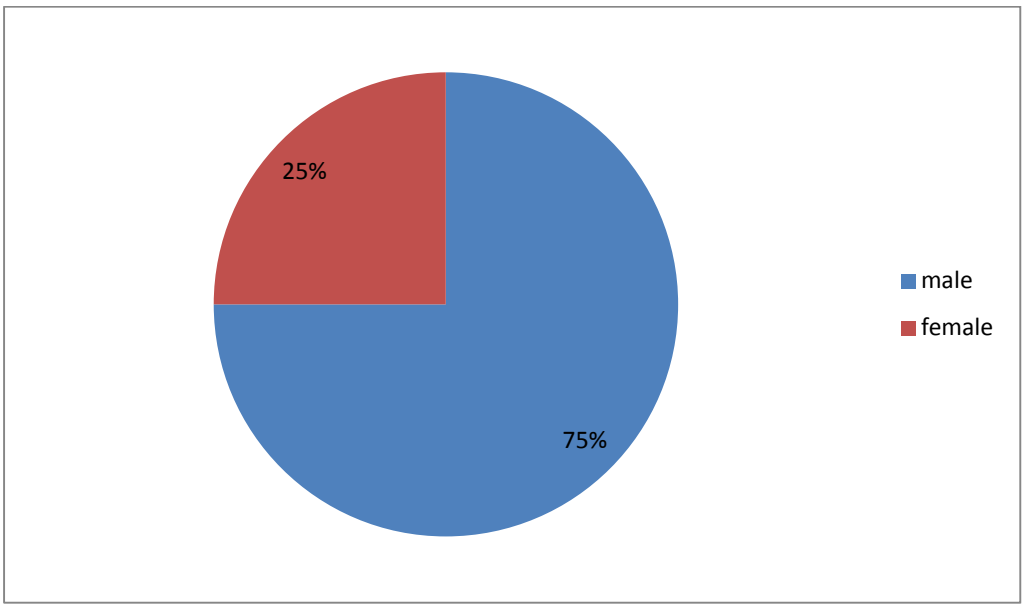


**Figure 4.1 : Gender Representation**

#### 4.2.2 Age of the Participants

The age group with the highest number of respondents was 16 to 25 years (56%), the second largest age group was between 26 and 35 years which constituted 25% of the respondents as shown in Figure 4.2. The third largest age group was 36 to 50 years which had 18% while 1% were over 50 years.

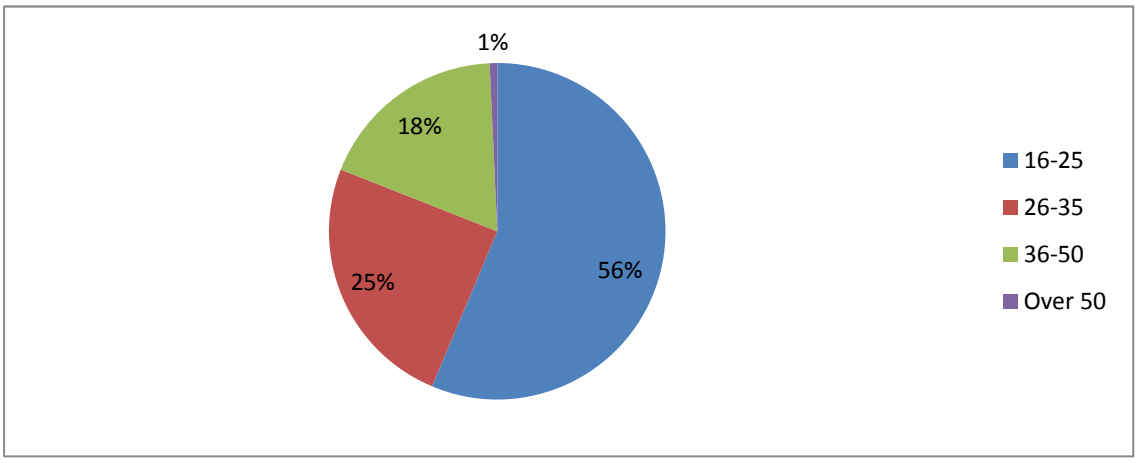


**Figure 4.2 : Gender Representation**

### 4.2.3 Educational Level of the Participants

The level of education of the persons who took part in the research is shown Figure 4.3. Most of the respondents had at least some basic level education (99%). These comprise of 34% who have a bachelors degree, 15% who obtained some formal education, 18% who graduated from high school, 30% who acquired diplomas, while those with a masters degree or higher accounted for 2% with only two (1%) without any form of formal education.

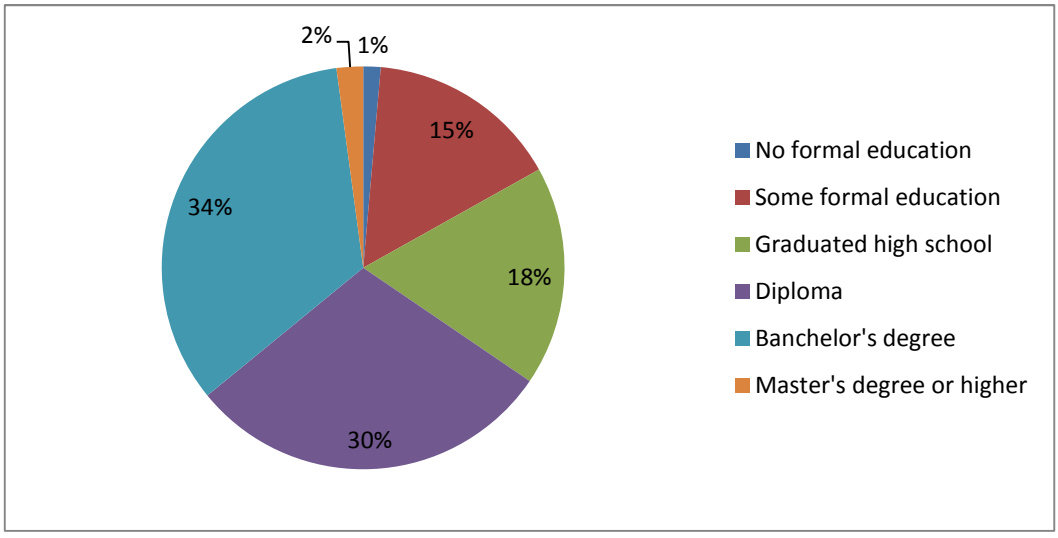


**Figure 4.3 : Educational Level of the Participants**

### 4.2.4 Employment Status of the Participants

Respondents who are in some form of employment accounted for 61%. These were full time employed (38%), part time employed (14%) and self employed (9%). Respondents who were unemployed accounted for 39%. Two respondents were retired accounting for 1% of respondents while 38.0% were unemployed as shown in Figure 4.4.

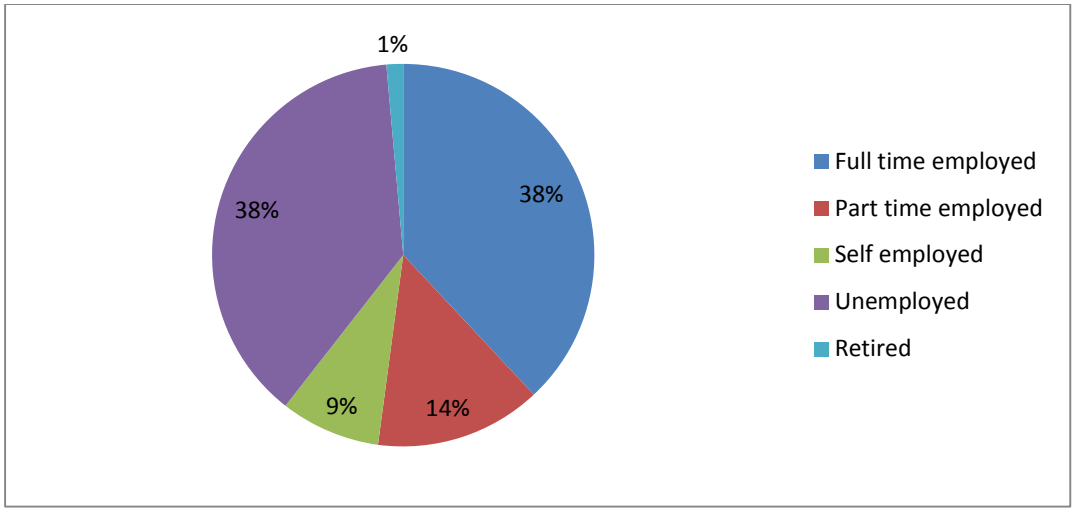


**Figure 4.4 : Employment Status of the Participants**

### 4.2.5 Income Level, Residential Place and Race

The income level of 81.7% of the respondents was below USD500 per month. A paltry 5.6% earned higher than USD1000 while the remainder of 12.7% earned between USD500 and USD1000. Most of the respondents were African (98.6%) with 2.8% being white. Asian and Coloured respondents constituted 0.7% apiece. Over two thirds (68.3%) of the respondents were urban dwellers while there were 31.7% from rural settlements.

## 4.3 Analysis of the Questionnaire

The method of data analysis adopted was one where data obtained from the questionnaire had frequency calculated to find the rate of occurrence. The totality of responses to each individual question was summed to identify the highest count of occurrence for each peculiar response. The quantified responses to each question were made available as a percentage and presented in

tabular form. Depending on the point that the researcher wishes to put across tables containing one or more variables are used. Cross tabulation of variable responses is also used.

The questionnaire was designed with a first section that intended to identify respondents who own cellphones and use mobile money. This made it possible for the researcher to identify responses from respondents who never used mobile money to allow classification when finding reasons why they do not use the service and also find reasons why those who use the service do so. The second last part of the questionnaire was designed to distinguish between those respondents who do not use mobile money, to split them into two categories i.e. those who will use mobile money in future and those who will not use it for life and get the reasons for their decisions too. This allowed the researcher to come up with the three groups of users, potential users and non users.

- ***Mobile Money Use By Participants***

The first part of the questionnaire was used to determine who amongst the respondents are mobile money users and those who are not. Table 4.2 shows the frequencies obtained for each group.

**Table 4.2 : Mobile Money Use by Participants**

| Q2 Do you use mobile money? | | |
|---|---|---|
| **Possible Response** | **Frequency** | **Percentage** |
| Yes | 106 | 74.6 |
| No | 36 | 25.4 |
| **Total** | **142** | **100** |

N=142

Table 4.2 shows that 74.6% of the respondents use mobile money. Just over a quarter (25.4%) of the respondents do not use mobile money. The total number of those who explicitly specified that they use mobile money and those who also explicitly specified that they do not use mobile money was regarded as the totality of the sample size. Judging from the fact that this is based on the responses of the respondents other than speculation the results are reliable. The results show that a high number of respondents use mobile money.

Basing on the data obtained we have 106 mobile users and 36 who do not use. Of these 36 who do not use mobile money 33 indicated that they intend to use mobile money in future while 3 do not intend to do so. These three groups will be referred to as users (106), potential users (33) and non-users (3) respectively. In order to get the reasons behind these actions of respondents with regard to mobile money use and perceived security issues, their responses will be analysed separately and a conclusion will be made on each group.

### 4.4 Perceived Security Construct

The perceived security construct is a construct that is made up of a number of tributary questions. Most of the questions asked in the questionnaire (see Appendix A) were those that relate to the perceived security construct since the key focus of the research was on the impact of perceived security on mobile money systems adoption. The results found on analysis of each of these questions added towards the overall perception about the perceived security construct. Each of these questions was analysed independently and a conclusion about its findings made in relation to the perceived security construct.

The analysis was divided into two parts, one which looked at consumer beliefs with regard to perceived security issues on mobile money. This looked at what respondents thought and believe is right. The next part looked at what the respondents do in practice to show their allegiance to their beliefs. The first section looks at the users, to get to understand why they use mobile money.

#### 4.4.1 Conceptual Beliefs of Respondents - Users

The questionnaire included questions that looked at the ideal mobile money characteristics that users expect and believe should be implemented in order for them to adopt mobile money. This included processes like trainings, awareness adverts and the characteristics of an ideal provider like trustworthiness.

Questions that were thought to represent user beliefs were analyzed in the context of users in the sections that follow to get a firm understanding of why they use mobile money.

- ***Effects of Security Features on System User Friendliness***

Respondents were asked whether they thought security features reduce user friendliness or not on mobile money systems. Of those who use mobile money (106), there were 39.7% who explicitly agreed that security features reduce user friendliness. There were 35.8% who disagreed and 7.5% who strongly disagreed that security reduces user friendliness giving a total of 43.3% explicitly disagreeing that security features reduce user friendliness.

**Table 4.3 : Effects of Security Features on User Friendliness**

| Q5 Do security measures on mobile money systems reduce user friend friendliness? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 13 | 12.3 |
| Agree | 29 | 27.4 |
| Undecided | 18 | 17.0 |
| Disagree | 38 | 35.8 |
| Strongly disagree | 8 | 7.5 |
| **Total** | **106** | **100** |

N=106

According to these results in Table 4.3, of the users that explicitly specified their positions on the effects of security features on user friendliness of mobile money systems, the researcher concluded that users believe that security features are important to mobile money systems since those users who indicated that security features do not affect user friendliness (43.3%) outweighed those who believe so (39.7%). This shows that security features do not deter people from using mobile money systems as the users do not see them as deterrent.

- ***Importance of Mobile Money Security Awareness Prior to Adoption***

The researcher intended to find out whether the users of mobile money systems think it is necessary to go through awareness seminars or trainings on security aspects prior to adopting mobile money. Table 4.4 shows the results obtained from the questionnaire analysis.

**Table 4.4 : Importance of Mobile Money Security Awareness Prior to Adoption**

| Q8 Do you think users should go through security awareness training before adopting mobile money? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 51 | 48.1 |
| Agree | 35 | 33.0 |
| Undecided | 6 | 5.7 |
| Disagree | 10 | 9.4 |
| Strongly disagree | 4 | 3.8 |
| **Total** | **106** | **100** |

N=106

The table shows that 51 users (48.1%) strongly agreed that users should go through security awareness trainings before adopting mobile money. In conjunction with those that agreed (33%) these make a majority of 81.1% explicitly stating that security awareness is important. A minority of 13.2% explicitly disagreed. This clearly shows that users value security consciousness of their mobile money systems.

- ***Safety of Mobile Money Transactions Over the Air***

Users were asked to specify whether they thought mobile money systems can be intercepted or not. Table 4.5 shows the tabulated results from the questionnaire analysis.

**Table 4.5: Safety of Mobile Money Transactions Over the Air**

| Q10 Do you believe mobile money transactions can be intercepted? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 72 | 67.9 |
| No | 34 | 32.1 |
| **Total** | **106** | **100** |

N=106

Table 4.5 shows that the majority of users (67.9%) believe that mobile money transactions can be intercepted even though they use mobile money. The researcher wanted to know the likelihood of interceptions as viewed by those who believe transactions can be intercepted.

**Table 4.6 : Likelihood of Mobile Money Transaction Interceptions**

| Q10a What do you think is the likelihood of that happening? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Highly likely | 8 | 11.1 |
| Likely | 35 | 48.6 |
| Moderate | 24 | 33.3 |
| Unlikely | 0 | 0 |
| Highly unlikely | 5 | 6.9 |
| **Total** | **72** | **100** |

N=72

Table 4.6 shows that of the 72 users who believe mobile money transactions can be intercepted 43 of them representing 59.7% believe that the likelihood of an interception ranges from likely to high likely. Those who think that the likelihood is moderate are 33.3% whilst those who believe it is highly unlikely constitute only 6.9%. From the findings displayed in Table 4.5 where 67.9% of users believe that the transactions they do over the air are susceptible to interceptions, and the results from Table 4.6 which shows that 59.7% of them believe that the likelihood of such is likely to highly likely, the researcher concluded that users use mobile money even though they believe it may not be very safe to do so implying a climb down on their security beliefs.

- ***Role of Users in Safeguarding Mobile Money Transactions***

The researcher intended to find out if users believe or think they have any role to play in ensuring the safety of transactions they perform on mobile money. Table 4.7 tabulates the results obtained from the questionnaire analysis. From the table, it can be seen that a huge total 86.8% of users explicitly agree that they should play a role in ensuring mobile money security.

**Table 4.7 : Role of Users in Safeguarding Mobile Money Transactions**

| Q13 Do you believe users have a role to play in ensuring the security of their mobile money? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 45 | 42.5 |
| Agree | 47 | 44.3 |
| Undecided | 8 | 7.5 |
| Disagree | 3 | 2.8 |
| Strongly disagree | 3 | 2.8 |
| **Total** | **106** | **100** |

N=106

There were 7.5% who were undecided while the remainder of 5.6% think they do not have a role to play in ensuring the security of their mobile money systems. The researcher concluded that users believe that they should exhibit behaviour that adds to a commitment to ensuring mobile money security.

- ***Perceptions of Users on Sensitive Information Security on Mobile Money***

The researcher included questions to find out how secure users feel when they send personal information over the air on mobile money systems in order to find out if there is a correlation with adoption.

**Table 4.8 : Perception of Users on Security of Sensitive Information on Mobile Money**

| Q14 Do you feel secure sending sensitive information over mobile money systems? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 12 | 11.3 |
| Agree | 29 | 27.4 |
| Undecided | 19 | 17.9 |
| Disagree | 36 | 34.0 |
| Strongly disagree | 10 | 9.4 |
| **Total** | **106** | **100** |

N=106

Table 4.8 shows that 38.7% of users explicitly agree that they feel secure to send sensitive information over mobile money systems (see total of those who agree and strongly agree in Table 4.8). Those who do not feel secure to send sensitive information over mobile money systems were 43.4% (see Table 4.8). The fact that the users who do not feel secure sending sensitive information over mobile money systems (43.4%) outweighed those who feel secure (34.0%) got the researcher to conclude that users use mobile money systems irrespective of how secure they feel when using the systems implying that they do not value the perceived security issues.

- ***Perceived Security Against Perceived Usefulness***

To find out how perceived security aspect fares when compared against other factors that also affect the decision of a user in choosing a mobile money service, questions pertaining to that were included in the questionnaire.

**Table 4.9 : Perceived Security Against Perceived Usefulness**

| Q15 Which mobile money product attribute is more important than the other? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Security | 44 | 41.5 |
| Usefulness | 15 | 14.2 |
| Equally important | 47 | 44.3 |
| **Total** | **106** | **100** |

N=106

Table 4.9 shows that 41.5% of users rank mobile money security as more important than its usefulness while only 14.2% think usefulness is more important than security. Those who think the two attributes are equally important account for 44.3%. From these findings the researcher concluded that users believe mobile money security is more important than product usefulness.

- ***Perceived Security Against Affordability***

The research collected responses that looked at how perceived system security fared against affordability in the mind of the users. Table 4.10 contains the tabulated results.

**Table 4.10 : Perceived Security Against Perceived Affordability**

| Q16 Which mobile money product attribute is more important than the other? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Security | 33 | 31.1 |
| Affordability | 26 | 24.5 |
| Equally important | 47 | 44.3 |
| **Total** | **106** | **100** |

N=106

Table 4.10 shows that 31.1 % of users think security attributes of mobile money systems are more important than its affordability, while 24.5% think that affordability is more important. Those who think the two attributes are equally important are 44.3%. From the table it can be seen than more users deem security as more important than affordability.

- ***Perceived Security Against Ease of Use***

The research also gathered the perception of users with regards to the importance of perceived security when compared against mobile money ease of use.

**Table 4.11 : Perceived Security Against Ease of Use**

| Q17 Which mobile money product attribute is more important than the other? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Security | 40 | 37.7 |
| Ease of Use | 22 | 20.8 |
| Equally important | 44 | 41.5 |
| **Total** | **106** | **100** |

N=106

As can be seen from Table 4.11 there are 37.7% of users believe mobile money security is more important than mobile money ease of use while 20.8% think ease of use is more important than security. There are 41.5% users who think these two attributes are equally important. Since the number of users who believe security is more important outweighs the number of those that think

ease of use is more important, without considering the neutral ones, the researcher concluded that users want mobile money product to be secure.

Findings from the three tables Table 4.9, Table 4.10 and Table 4.11 show that users believe security is more important than usefulness, affordability and ease of use since the users who are not neutral about the importance of security with each comparative attribute had a larger group picking security as the most important. This shows that users value security in their minds.

- ***Users View on Importance of Security to Mobile Money Systems***

The researcher asked respondents to rank the importance of security to mobile money systems without comparing it to any other attribute. Table 4.12 shows the tabulated responses as obtained.

**Table 4.12 : Users View on Importance of Security to Mobile Money Systems**

| Q19 On a scale of 1-5, 1 being least important, 5 being very important, how do you rank the importance of security to mobile money systems? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| 1 (Least important) | 0 | 0.0 |
| 2 | 2 | 1.9 |
| 3 | 23 | 21.7 |
| 4 | 20 | 18.9 |
| 5 (Very important) | 61 | 57.5 |
| **Total** | **106** | **100** |

N=106

Table 4.12 shows that users who classified security as the most important are 57.5%. Those who thought it is second most important are 18.9%. These are the users who view security as a priority. Their totality accounted for 76.4% of users. Those who view the importance of security as moderate to least important accounted for 22.6% with no user ranking security as least important. The researcher concluded from this that users perceive security as important to mobile money systems.

### 4.4.2 Summary on Users Conceptual Beliefs on Mobile Money Security

The analysis done to find out the conceptual beliefs of mobile money users on security related issues showed that users do not view security features on mobile money systems as hindering adoption. Users believe they should play a role in ensuring the security of their mobile money accounts. Users of mobile money services believe security of mobile money systems is more important than other attributes namely affordability, ease of use and usefulness. The users viewed security as the most important aspect with no user ranking security as least important amongst the mobile money systems attributes. Users however feel mobile money transactions can be intercepted though they still use mobile money.

### 4.4.3 Conceptual Beliefs of Respondents - Potential Users and Non Users

This section looks at the conceptual beliefs of potential users and non users with regards to perceived security on mobile money and other factors that may affect mobile money uptake. These respondents were asked to complete questions on the questionnaire that intended to find reasons why they do not use mobile money and indicate what can be done for them to come on board. For these respondents the reason why they do not use mobile money and what they expect to change or to be added to mobile money systems in order for them to adopt it was considered all that this group could contribute to the research therefore there is no analysis of their behaviour with regards to mobile money transactions as they do not use the service.

- ***Reasons For Not Using Mobile Money***

The researcher gathered information from respondents who do not use mobile money on the different reasons why they do not use the service. The findings were tabulated in Table 4.13.

Table 4.13 shows that the largest group of potential and non users shun mobile money because of lack of usefulness to them. The second most recurring reason amongst the group is poor ease of use attributes. The third most recurring reason was security and affordability. There are 5.6% of non users who do not use mobile money because they do not know that it exists. It is evident from this analysis that the main reason why non users shun mobile money is because they do not see its usefulness. The second reason is because of ease of use concerns, where 22.2% of non

**Table 4.13 : Reasons For Not Using Mobile Money**

| Q42 What is the primary reason why you do not use mobile money (tick one)? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| I do not know it exists | 2 | 5.6 |
| I do not think it is safe/secure to use it | 7 | 19.4 |
| The service is not very useful to me, it does not change the way I transact. | 12 | 33.3 |
| It is difficult to use (i.e learn, enrol into, use and/or access) | 8 | 22.2 |
| It is expensive to use it i.e. higher tariff charges. | 7 | 19.4 |
| Other reason | 0 | 0.0 |
| **Total** | **36** | **100** |

N=36

users cited difficulties in using the product. Perceived security features and cost are deterrent factors but they are not the main ones.

- ***Most Important Characteristics of Mobile Money to Potential and Non Users***

The researcher intended to find out reasons that would lure non users to the product. The non users were asked which feature on mobile money they would consider as most important if they were to use it in future. Table 4.14 shows the results obtained.

The trait most cited by the non users and potential users groups as most important was security. The second most important trait to lure non users to mobile money was jointly cited as ease of use and affordability. Product usefulness came last amongst the other traits (see Table 4.14). From the findings in Table 4.14 the researcher concluded that non users would adopt mobile money if it became secure in their view. Perceived cost and ease of use are also the joint next important.

**Table 4.14 : Most Important Characteristics of Mobile Money to Potential and Non Users**

| Q43 If you decided to adopt mobile money, what factors would you consider most when choosing a mobile money provider (tick one)? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| The product should be secure, risk free, trustworthy and reliable | 13 | 36.1 |
| It must have useful services, be innovative and improve the way I transact | 5 | 13.9 |
| It must be easy to learn, enroll and use, and should have readily available agent outlets. | 9 | 25.0 |
| It must be cheap to use | 9 | 25.0 |
| Other reason | 0 | 0.0 |
| **Total** | **36** | **100** |

N=36

### 4.4.4 Summary of Conceptual Beliefs of Potential and Non Users

The researcher noted that most of the non users cited security related issues as the main characteristic that would not lure them to use mobile money systems. On reasons why they do not use mobile money most cited non usefulness of the service and mentioned security as the third most popular reason why they do not use mobile money. The results showed that the users believe security is important to mobile money systems.

### 4.4.5 Actual Behaviour of Respondents - Users

The questionnaire that was circulated to respondents had questions that were meant to gather information on what the respondent thought in terms of characteristics that are ideal for mobile money systems (conceptual). It also contained questions that checked how in practice those users behave, to see if the conceptual and the observed trends match. An evaluation of the practiced and the conceptualized was then made to give a conclusion to the research.

- ***Awareness of Security Features on Adopted Mobile Money System***

The research sought to find out if users are aware of security features available on their mobile money systems.

Table 4.15 shows that 66.0% of respondents who are mobile money users are aware of security features present on the mobile money service they use. The remainder of 34.0% are not aware. Table 4.15 also shows that 59.4% of these users check on the security of the mobile money product they use, whilst 40.6% do not.

**Table 4.15 : Awareness of Security Features on Adopted Mobile Money System**

| Q4 Are you aware of any security feature(s) available on your mobile money service? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 70 | 66.0 |
| No | 36 | 34.0 |
| **Total** | **106** | **100** |
| Q40 Do you check on the security of the mobile money product you use ? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 63 | 59.4 |
| No | 43 | 40.6 |
| **Total** | **106** | **100** |

N=106

From Table 4.15 it can be observed that the number of users who are aware of security features available on their mobile money service outweighs that of unaware users. This shows that users are security conscious when choosing a mobile money service.

- ***Customer Reaction To Enhanced Security Features on Mobile Money***

Table 4.16 shows that 97.9% of the users who are aware of security features available on their mobile money would continue to use the service even if the security features were enhanced. Only 2.1% would not. This is in agreement with the earlier observation (see Table 4.3) were users agreed that they do not see security features as deterrent to the use of mobile money

**Table 4.16 : Customer Reaction To Enhanced Security Features on Mobile Money**

| Q4a Would you continue using the mobile money service if these security features were increased/enhanced? (For those who are aware of security features.) | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 68 | 97.9 |
| No | 2 | 2.1 |
| **Total** | **70** | **100** |

N=70

systems. From this analysis it can be said that perceived security has a positive correlation with mobile money adoption.

- ***Mobile Money Security Awareness Campaigns***

Respondents were asked about their knowledge of security features available on the mobile money systems they use and also if they think users should go through security awareness trainings before adopting mobile money. To validate this, respondents were also asked if their mobile money service provider airs adverts on the security features available on their service. Table 4.17 shows the responses.

**Table 4.17: Mobile Money Security Awareness Campaigns**

| Q6 Does your mobile money service provider air adverts on the security features available on their service? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 58 | 54.7 |
| No | 48 | 45.3 |
| **Total** | **70** | **100** |

N=70

Table 4.17 shows that there are 54.7% of respondents from the users group whose mobile money service provider airs adverts on the security features available on the mobile money service. The remainder of 45.3%, use a mobile service provider who do not do that. From the above findings

it can be seen that there are more users of mobile money services who are aware of security features on their mobile money service than those who are not.

- ***Attendance of Mobile Money Security Awareness Campaigns***

The researcher intended to find out if users of mobile money systems actually went through mobile money security awareness prior to adopting their current services. Table 4.18 shows the responses obtained.

**Table 4.18: Attendance of Mobile Money Security Awareness Campaigns**

| Q7 Did you go through a mobile money security awareness training before using mobile money? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 15 | 14.2 |
| No | 91 | 85.8 |
| **Total** | **106** | **100** |

N=106

Findings displayed on Table 4.18 show that 85.8% of the users did not attend a mobile money security awareness campaign. Only 14.2% did attend. This shows that users did not attach much importance to security or did not get access to such trainings. However they still went on to use the service without such trainings hence they did not see the trainings as important.

- ***Customer Awareness of Official Mobile Money SMS Notification Shortcodes***

The researcher wanted to know whether customers would survive phishing attacks through the use of bogus SMS shortcodes when transactions occur. Customers were asked about their knowledge of the official shortcodes used by their mobile money service providers. Table 4.19 shows the responses obtained.

The results from the table show that 56.6% of the users are aware of the SMS shortcodes used by their mobile money service provider for alerts relating to mobile money transactions. There are 43.4% of users who are not aware of their official mobile money service alert SMS notification shortcodes. These are the ones susceptible to bogus messages.

**Table 4.19: Customer Awareness of Official Mobile Money SMS Notification Shortcodes**

| Q11 Are you aware of the SMS shortcodes used by your mobile money service provider for alerts relating to mobile money transactions? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 60 | 56.6 |
| No | 46 | 43.4 |
| **Total** | **106** | **100** |

N=106

The fact that more users are aware of the official SMS shortcodes used for transactional alerts means that users reduce vulnerability to bogus SMS messages. This is a user behaviour that adds towards a commitment to improving security.

- ***Origin Verification of Mobile Money SMS Messages By Users***

Table 4.20 compliments findings from Table 4.19. There are 60.4% of users who verify the origins of mobile money SMS messages. These users have less chance of falling prey to bogus messages. There are 39.6% of users who do not verify the origins of transactional alerts. The fact

**Table 4.20: Origin Verification of Mobile Money SMS Messages By Users**

| Q12 When you receive mobile money SMS messages do you verify their origin? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 64 | 60.4 |
| No | 42 | 39.6 |
| **Total** | **106** | **100** |

N=106

that there are more users who verify the transactional SMS origins compared to those who do not shows a behaviour that is pro security being exhibited by users.

- ***Most Important Mobile Money Factor for Users***

To find out the main reason considered by those who use mobile money for them to use it, the researcher included a question on that aspect. Table 4.21 shows the results of the findings tabulated.

The largest group of users chose their mobile money basing on its usefulness (see Table 4.21). The second most recurring attribute used for choosing a mobile money service was security related. Affordability was the third most cited reason to lure customers to use a service while ease of use attribute anchored the list of reasons in terms of recurrence (see Table 4.21).

**Table 4.21: Most Important Characteristics of Mobile Money to Non Users**

| Q18 What was the most important factor you that considered when you chose your current mobile money service (tick one)? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| It enables me to accomplish my tasks easier due to useful, innovative services | 52 | 49.1 |
| Using the mobile wallet does not require a lot of mental effort | 9 | 8.5 |
| The service is secure, risk free, trustworthy and reliable | 25 | 23.6 |
| The service is affordable to use | 17 | 16.0 |
| Other reason | 3 | 2.8 |
| **Total** | **106** | **100** |

N=106

The remaining users (2.8%) chose theirs for other reasons which they unfortunately did not specify even though they had an option to do so. This shows that mobile money service usefulness is the most important factor for adoption. Security comes second followed by cost then ease of use amongst the user group.

- ***User Behaviour and Handset Issues***

For the researcher to thoroughly scan the security related behaviour exhibited by the respondents who use mobile money, there was need for a background check on the handsets they use the operating system used, the behaviour the users constantly exhibit when using their mobile handsets which they in turn use for mobile money so that this behaviour can be evaluated in relation to the security issues it poses to mobile money transactions.

Information about the mobile operating systems used by users was gathered and tabulated in Table 4.22.

**Table 4.22: Mobile Operating System of User Handsets**

| Q23 Which mobile operating system software is used by your mobile phone? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Android | 46 | 43.4 |
| Symbian | 19 | 17.9 |
| Windows | 16 | 15.1 |
| Blackberry | 10 | 9.4 |
| Java ME | 10 | 9.4 |
| Other | 5 | 4.7 |
| **Total** | **106** | **100** |

N=106

The most used mobile operating system amongst mobile money adopters is Android which commands 43.4% of the users as shown on Table 4.22. The most used mobile operating system amongst adopters, Android, is the most affected by malware (Juniper Networks, 2012). This implies that mobile money users are vulnerable to the threats caused by this malware. Irrespective of this the users still use mobile money on these gadgets.

The researcher uses Table 4.23 to highlight the characteristics of mobile money users with respect to security concerns. Table 4.23 shows that 92.5% of mobile money users did not have their handsets scanned for virus prior to adopting mobile money. Only a paltry 7.5% users did scan their handsets prior to adoption. Table 4.23 also shows that less than a quarter (20.8%) of

mobile money users use antivirus software on their mobile phones. The majority (79.2%) of users do not use antivirus software on mobile phones which they use for mobile money irrespective of the fact that 43.4% of them use the Android platform which is the most targeted by malware (Juniper Networks, 2012).

**Table 4.23 : Mobile Money User Behaviour Summary- Antivirus**

| Q9 Did you have your mobile handset scanned for viruses before using mobile money? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 8 | 7.5 |
| No | 98 | 92.5 |
| **Total** | **106** | **100** |
| Q20 Do you use antivirus software for your mobile phone? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 22 | 20.8 |
| No | 84 | 79.2 |
| **Total** | **106** | **100** |
| Q20a How often do you update the antivirus software? (For those who do update) | | |
| **Possible response** | **Frequency** | **Percentage** |
| Daily | 5 | 22.7 |
| Twice a week | 2 | 9.1 |
| Weekly | 3 | 13.6 |
| Monthly | 6 | 27.3 |
| Less frequently than monthly | 3 | 13.6 |
| Never | 3 | 13.6 |
| **Total** | **22** | **100** |
| | | |

Of the 20.8% of users who use antivirus, the researcher wanted to get their virus updating behaviour to inquire more about their security consciousness. Table 4.23 shows that 72.8% of

these users update it at least once monthly. There are 27.2% of them who never update their antivirus or update it less frequently than monthly. The number of users who update antivirus out of those who use antivirus is encouraging but the fact that they are a majority (72.8%) of a minority group (22) still means in terms of antivirus usage on their mobile phones, the mobile money users have a behaviour that is not pro security. They however are comfortably using mobile money.

**Table 4.24 : Customers Mobile Phone Usage Behaviour**

| Q21 Have you verified that your mobile phone is from the displayed brand (e.g. if branded Nokia have you verified that it is from Nokia)? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 78 | 73.6 |
| No | 28 | 26.4 |
| **Total** | **106** | **100** |
| Q22 Do you download software applications to your mobile phone ? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 75 | 70.8 |
| No | 31 | 29.2 |
| **Total** | **103** | **100** |
| Q22a Do you download from official sites only? (For those who download) | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 32 | 42.7 |
| No | 43 | 57.3 |
| **Total** | **75** | **100** |

Table 4.24 continues to look at the security related behaviour from mobile money users. The results show that 73.6% of users verify the authenticity of the mobile handset brands they use. Only 26.4% do not verify authenticity of the mobile handsets. This is a good thing from a security perspective as it allows users to know which site is official for them to get software updates for their handsets as well as other support features. Table 4.24 further shows that the

majority of these users (70.8%) download software applications to their handsets while the remaining minority (29.2%) do not. It is critical to look at the behaviour of interaction of these users who download applications with the download sites.

Table 4.24 shows that most of these users (57.3%) with a habit of downloading applications download them from third part websites which are unofficial. A lesser number (42.7%) of them do download from official websites. According literature review done in the second chapter of this document, unofficial websites have applications that can contain viruses as no one bothers to monitor such sites (Juniper Networks, 2012). This behaviour by the users is not good for their security given the malicious abilities of malware once it becomes resident on their gadgets. It can be concluded from this reckless behaviour that users are not very serious about their mobile handset security, which can affect their mobile money transaction security.

**Table 4.25 : Customers Mobile Phone Usage Behaviour - Bluetooth**

| Q24 Does your phone have Bluetooth capabilities? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 96 | 90.6 |
| No | 10 | 9.4 |
| **Total** | **106** | **100** |
| Q24a Do you always switch it off after use? (For those who have Bluetooth) | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 78 | 81.3 |
| No | 18 | 18.7 |
| **Total** | **96** | **100** |

Table 4.25 shows that a majority of mobile money users use handsets that have Bluetooth capabilities. Only a minority of 9.4% of users have mobile handsets without Bluetooth capabilities. Table 4.25 further shows that most of these users with handsets that have Bluetooth capabilities do switch off their Bluetooth after using it. A smaller number of them (18.7%) do not switch it off after use. Bluetooth if not switched off, allows malicious elements to control the handset of a user, allowing them to clandestinely send SMS messages or even make phone calls

without the consent of the owner (US-CERT, 2010). From a mobile money perspective this poses threats as the users may have confidential information sent to attacker defined destinations for improper use. The fact that most of the users with Bluetooth enabled handsets switch it off after use shows that users are security conscious and are therefore less vulnerable to such attacks.

**Table 4.26: Customers Mobile Phone Usage Behaviour - Handset**

| Q25 Do you share your mobile phone with others? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 27 | 25.2 |
| No | 80 | 74.8 |
| **Total** | **107** | **100** |
| Q29 Do you use the security lock on your mobile phone? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 65 | 63.1 |
| No | 38 | 36.9 |
| **Total** | **103** | **100** |

A majority of mobile money users do not share their mobile handsets with anyone whilst a minority do share theirs with others (see Table 4.26). Sharing handsets increases vulnerability of the mobile money related data contained in these handsets. Since most of the mobile money users (74.8%) do not share their handsets with others it implies their mobile money related information resident on these handsets is less vulnerable to eavesdropping. This behaviour of most users of not sharing their handsets, coupled with the fact that most of them (63.1%) use security lock on their phones shows a security conscious mobile money user population.

Table 4.27 contains information about the way users manage their personal identification credentials on mobile money systems. A large number (73.6%) of the users do not share their mobile money usage credentials with others whereas the remaining 26.4% do share. Sharing of mobile money usage credentials is risky as accountability becomes difficult. However the majority of users (see Table 4.27) do not share their mobile money usage credential. This observation shows a user population with mobile money security awareness.

**Table 4.27: Customers Mobile Money Usage Behaviour -PINs**

| Q26 Do you share your mobile wallet usage credentials with others (spouse, friends or relative)? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 28 | 26.4 |
| No | 78 | 73.6 |
| **Total** | **106** | **100** |
| Q30 Do you renew/change the password/personal identification number (PIN) of your mobile money account? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 47 | 44.3 |
| No | 59 | 55.7 |
| **Total** | **106** | **100** |
| 30a How often do you change it? (For those who change) | | |
| **Possible response** | **Frequency** | **Percentage** |
| Daily | 4 | 8.5 |
| Twice a week | 3 | 6.4 |
| Weekly | 8 | 17.0 |
| Monthly | 13 | 27.7 |
| Less frequently than monthly | 17 | 36.2 |
| Never | 2 | 4.3 |
| **Total** | **47** | **100** |

Below half of users change their PINs whilst 55.7% do not change their PINs ( see Table 4.27). Although most of the mobile money users do not share their PINs most of them (55.7%) do not change their PINs. This increases the chances of ill meaning elements with access to mobile money accessing gadgets to guess these credentials ending up abusing funds stored in a mobile money account belonging to a user. The fact that most users do not change their PINs shows a user population not very concerned about the security of their mobile money accounts.

Table 4.27 reveals that only 44.3% of mobile money users do change their PINs on their mobile money systems. Of these 8.5% change it daily, another 6.4% twice a week and another 17.0% weekly. There are 27.2% who change monthly. The component of these users adds up to 59.6% who change mobile money system PINs at least once a month. Those users who change it less frequently than monthly make up the rest (40.5%). Changing PINs on mobile money systems reduces the chances of having accounts accessed by malicious elements without the consent of the legitimate owner. The fact that more users (59.6%) of those who change their mobile money PINs change it at least once a month is a positive security related behaviour.

- ***Mobile Money User Experiences***

To further analyse the behaviour of mobile money users the researcher looked further at user experiences concerning mobile money with a view to find out why they exhibit the tendencies they have shown in the prior findings revealed. Table 4.28 shows the results tabulated from the findings.

A huge number of users use subscriptions registered in their own names to perform mobile money transactions whilst 9.4% of them do not (see Table 4.28). Using subscriptions registered in names of other users to perform mobile money transactions has got risks such as the rejection of erroneous transaction reversals presented by the user who is not registered as the official user of the transacting account. The fact that most of the users (90.6%) use subscriptions registered in their own names shows that the user population is conscious of the security issues surrounding borrowing a mobile money account.

A majority of users are not aware of someone they know who have suffered from a security breach or theft as a result of a mobile device being hacked and they themselves have also not become victims (see Table 4.28). Only a paltry 9.4% of users have experienced that. This may be the reason for the behaviour that shows lack of security consciousness exhibited by some mobile money users as revealed by some sections in the prior analysis done.

**Table 4.28: Mobile Money User Experiences**

| Q31 Is the subscription (mobile number) you use for performing transactions registered in your name? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 96 | 90.6 |
| No | 10 | 9.4 |
| **Total** | **106** | **100** |
| Q32 Have you or someone you know suffered from a security breach or theft as a result of your mobile device being hacked? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 10 | 9.4 |
| No | 96 | 90.6 |
| **Total** | **106** | **100** |
| Q33 When you lose your SIM card, are you satisfied with the security checks taken by your provider to ensure only the legitimate owner replaces a SIM card ? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Yes | 89 | 84.0 |
| No | 17 | 16.0 |
| **Total** | **106** | **100** |
| Q34 Do mobile money banking services sometimes fail to perform well due to network problems? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 51 | 48.1 |
| Agree | 41 | 38.7 |
| Undecided | 5 | 4.7 |
| Disagree | 3 | 2.8 |
| Strongly Disagree | 6 | 5.7 |
| **Total** | **106** | **100** |

Mobile money users are satisfied with the security checks taken by their mobile money provider to ensure that only the legitimate owner replaces a missing SIM card (see Table 4.28) whilst 16.0% do not. In STK based systems like OneWallet the physical SIM card plays a major role in safeguarding the mobile money account of a subscriber. If a SIM card is cloned or replaced, the mobile money system automatically overrides the existing access credentials and gives the new SIM card owner the chance to key in new credentials (PIN). This may result in cloned or wrongly replaced SIM cards accessing the wrong accounts. Malicious elements can exploit this. The fact that more users (84.0%) are satisfied that the SIM replacement procedures uniquely identify the legitimate owner shows that they are conscious of this security issue.

The researcher needed to get an insight into the mobile users experience with regard to mobile money systems availability. Just like confidentiality and integrity, availability is a key issue of system security. Table 4.28 shows that 86.8% of users explicitly agree that mobile money banking services sometimes fail to perform well due to network problems. The fact that the majority of users (86.8%) are in agreement that network challenges have a negative effect on system availability but still use the mobile money systems shows that they do not really see occasional system unavailability as an impediment to usage.

### 4.4.6 Summary on Actual Behaviour of Mobile Money Users

The researcher noted that most of the mobile money users claim to be aware of security features available on their mobile money systems and they do check on the security features available on their services (see Table 4.15). They also use services from service providers who make them aware of security features available on their mobile money services through adverts (see Table 4.17). Most of the mobile money users are aware of transactional alert shortcodes from their providers and would verify the origins of mobile money transactional alert messages.

The users of mobile money ranked security as the second most important reason why they chose their mobile money service after usefulness. Users check the authenticity of the handsets they use for mobile money so as to get software updates from official websites. Most users have Bluetooth enabled handsets but switch the service off immediately after use. Users of mobile money do not share their phones with others and use security lock features present on the gadgets. They do not share mobile money account usage credentials and those who change these

credentials change them at least once a month. They do not borrow mobile money accounts but use their own. The surveyed users are satisfied with the security related conduct exhibited by their mobile money service providers. The users have not fallen prey or had anyone who has fallen prey to malicious elements on mobile money systems.

Users however exhibit behaviour that makes them vulnerable to attacks on mobile money systems. Most of them did not attend awareness trainings prior to adopting mobile money. A large group of the users use the Android operating system on their handsets which is prime target of most malware developers (FBI and Department of Homeland Security, 2013). Most of them do not use antivirus software on their phones and those who use antivirus do not update it or take longer to update it exposing themselves to malware threats. The majority of these users download applications from unofficial sites further increasing the risk they expose themselves to. A large group of users do not change their mobile money account access credentials thereby increasing the risk of having the credentials guessed by malicious elements. Most of these users are aware that network issues may affect system availability but still use the services.

### 4.4.7 Summary

The chapter looked at the demographic aspects of the respondents. It looked at the perceived security construct of the research by looking at the conceptual elements of users, potential users and non users of mobile money. It then looked at the actual behaviour of users to get a good understanding of the value they attach to perceived security as an aspect of mobile money. The next chapter continues to look at perceived trust, ease of use, affordability and perceived usefulness to see how they affect mobile money adoption then gives a conclusion to the findings.

# Chapter 5 – Presentation of Results

## 5.1 Introduction

This chapter continues to analyse the research results and interprets them in the context of the research objectives. It looks at the relationship between mobile money adoption and the other constructs not looked at in the previous chapter. The constructs are perceived trust, perceived usefulness, perceived cost and perceived ease of use.

## 5.2 Perceived Trust

The questionnaire (complete copy is contained in Appendix) included questions that sought to find out whether users trust the mobile money systems they use or not. This section analyses the questions that pertain to the perceived security construct.

### 5.2.1 Users Trust of Mobile Money Systems

The researcher wanted to find out if users trust the mobile money systems they use. The circulated questionnaires contained questions pertaining to that. Table 5.1 shows the frequencies of the responses tabulated.

Results show that 68.9% of mobile money users believe that mobile banking service providers are fair in their conduct of customer transactions (see Table 5.1). There are 18.7% of users who do not believe that mobile banking service providers are fair in their conduct of customer transactions. Table 5.1 also shows that 65.1% of users believe that network providers are trustworthy. There are 17.0% who disagree that mobile network providers are trustworthy. Since most of the users agree that mobile network operators fairly conduct transactions and are trustworthy the findings show that mobile money users trust their mobile money service providers. This is in agreement with finding by Erdem and Swait (2004) and Yu (2012).

**Table 5.1: Users Trust of Mobile Money Systems**

| Q35 Do you believe mobile banking service providers are fair in their conduct of customer transactions? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 23 | 21.7 |
| Agree | 50 | 47.2 |
| Undecided | 13 | 12.3 |
| Disagree | 14 | 13.2 |
| Strongly Disagree | 6 | 5.7 |
| **Total** | **106** | **100** |
| Q36 Do you believe that mobile network providers are trustworthy? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 19 | 17.9 |
| Agree | 50 | 47.2 |
| Undecided | 19 | 17.9 |
| Disagree | 13 | 12.3 |
| Strongly Disagree | 5 | 4.7 |
| **Total** | **106** | **100** |
| Q37 Do you believe wireless infrastructure can be trusted? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 18 | 17.0 |
| Agree | 50 | 47.2 |
| Undecided | 11 | 10.4 |
| Disagree | 20 | 18.9 |
| Strongly Disagree | 7 | 6.6 |
| **Total** | **106** | **100** |

Table 5.1 further shows that 64.2% of users believe mobile wireless infrastructure can be trusted. The remaining 25.5% do not believe mobile wireless infrastructure can be trusted. The fact that

the number of users who trust wireless infrastructure (64.2%) outweighs that of users who do not trust wireless infrastructure shows that mobile money users trust wireless infrastructure.

### 5.2.2 Users Operational Concerns on Mobile Money Systems

There are 56.6% of users believe that mobile banking services may not perform well or may incorrectly process payments (see Table 5.2). There are 27.3% who do not believe that mobile

**Table 5.2: Users Operational Concerns on Mobile Money Systems**

| Q38 Do you believe that mobile banking services may not perform well or may incorrectly process payments? | | |
|---|---|---|
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 16 | 15.1 |
| Agree | 44 | 41.5 |
| Undecided | 17 | 16.0 |
| Disagree | 26 | 24.5 |
| Strongly Disagree | 3 | 2.8 |
| **Total** | **106** | **100** |
| Q39 When transferring money through mobile banking, do you fear that you will lose money due to careless mistakes such as wrong input of account number or wrong input of amount of money? | | |
| **Possible response** | **Frequency** | **Percentage** |
| Strongly Agree | 35 | 33.0 |
| Agree | 41 | 38.7 |
| Undecided | 11 | 10.4 |
| Disagree | 18 | 17.0 |
| Strongly Disagree | 1 | 0.9 |
| **Total** | **106** | **100** |

banking services may not perform well or may incorrectly process payments. The fact that more users (56.6%) believe that mobile banking services may not perform well or may incorrectly

process payments shows that customers have less trust in mobile money systems. They however use these services.

Table 5.2 shows further that 71.7% of users fear to lose money when transferring money through mobile banking due to careless mistakes such as wrong input of account number or wrong input of amount of money. There are 17.9% who do not fear that they will lose money through such mistakes (see Table 5.2). The fact that the majority (71.7%) of users fear to lose money through carelessness means they do not trust mobile money systems.

### 5.2.3 Summary on Perceived Trust

The researcher noted that most of the mobile money users trust that their service providers are fair in their conduct of transactions done by customers. Most of these customers have trust in the mobile network providers. The users also trust the wireless infrastructure used by the network providers. They however believe that mobile money systems may incorrectly process transactions. They fear also that careless mistakes can make them lose money whilst transacting on these mobile money systems. Generally though users of mobile money systems trust the mobile money service they use.

## 5.3 Most Important Characteristic for Mobile Money Adoption

The researcher wanted to find the most important characteristic of mobile money. Table 5.3 shows the results obtained from the analysis of data obtained from non users, potential users and users. The most important factor that affects mobile money adoption is reached at through the amalgamation of the reasons for not using mobile money of non users and potential users, the reasons that would make them use mobile money and the reasons that made users to adopt mobile money. The most important factor as can be seen from the frequency column in Table 5.3 is perceived usefulness, followed by perceived security. Perceived cost is the third most important with perceived ease of use being the least important as shown in Table 5.3.

**Table 5.3: Most Important Construct on Mobile Money Adoption**

| **Perceived Construct** | **Non Users (Shun Reason)** | **Non Users (Expected Attribute)** | **Calculated Average** | **Users (Usage Reason)** | **Frequency** | **%** |
|---|---|---|---|---|---|---|
| Usefulness | 12 | 5 | 8.5 | 52 | 60.5 | 42.6 |
| Security | 7 | 13 | 10 | 25 | 35.0 | 24.6 |
| Cost | 7 | 9 | 8.0 | 17 | 25 | 17.6 |
| Ease of Use | 8 | 9 | 8.5 | 9 | 17.5 | 12.3 |
| Other | 2 | 0 | 1 | 3 | 4 | 2.8 |

N=142

## 5.4 Hypothesis Analysis of All Constructs

Table 5.4 shows the calculated P values for each construct to ascertain whether there exists a correlation between adoption of mobile money and the construct. The constructs looked at are perceived usefulness, perceived security, perceived cost, perceived ease of use and perceived trust.

**Table 5.4 : Computed Coefficients**

| **Perceived Construct** | Unstandardized Coefficients | | Standardized Coefficients | **t** | **Sig (P-Value)** |
|---|---|---|---|---|---|
| | **B** | **Std. Error** | **Beta** | | |
| Usefulness | .221 | .333 | .445 | 6.129 | .000 |
| Security | .242 | .046 | .465 | 3.312 | .002 |
| Cost | .112 | .036 | .484 | 7.144 | .002 |
| Ease of Use | .231 | .031 | .458 | 3.937 | .001 |
| Trust | .165 | .047 | .309 | 3.375 | .004 |

**Dependent variable : Mobile Money Adoption.**

Table 5.4 shows that all five of the null hypotheses have been rejected. This confirms a significant relationship between adoption of mobile money and perceived usefulness, security, cost, trust and ease of use. The values obtained for each construct are as follows, Usefulness ($P<0.05$), Security ($P<0.05$), Trust ($P<0.05$), Cost ($P<0.05$) and Ease of Use ($P<0.05$) thus there is adequate evidence to suggest a correlation between all constructs and adoption of mobile money systems.

The findings are in agreement with Masinge (2010) who noted that customers at the Bottom of the Pyramid (BOP) will consider adopting mobile banking as long as it is perceived to be useful, easy to use and not expensive. The research is also in agreement with Tobbin and Kuwornu (2011) who noted that perceived usefulness and perceived ease of use are important factors in the adoption of mobile money in the study done in Ghana. Luarn and Lin (2005), Wang et al (2003), Saleem and Rashid (2011), Brown et al (2003), Benamati and Serva (2007) also found perceived trust and perceived risk to significantly affect behavioural intention to adopt mobile money. This research is in agreement with these findings. The study by Chitungo and Munongo (2013) reported that cost, perceived usefulness and ease of use positively contribute towards mobile banking adoption which is in agreement with this research and other studies looked at this far.

### 5.5 Mobile Money Usage Against Demographic Characteristics

The researcher looked at the relationship between mobile money usage and demographic characteristics of the respondents like age, education levels and income level. These were discussed individually in sections 5.5.1, 5.5.2, 5.5.3 and 5.5.4. Table 5.5 shows The P values obtained at 5% significance level for testing of the independence of association between demographic characteristics and mobile money usage.

**Table 5.5: Chi-Square Mobile Money Usage Versus Demographic Characteristics**

| Demographic Variable | Computed Pearson Chi-Square P Value |
|---|---|
| Residential area | 0.057 |
| Employment status | 0.004 |
| Age | 0.055 |
| Earnings | 0.105 |

A chi-square hypothesis testing was carried out at 5% significance level where Ho is rejected if P>0.05

The following hypotheses were tested.

### 5.5.1 Relationship Between Mobile Money Usage and Respondent Residential Area

Ho: There is no association between mobile money service use and the residential area of a respondent

**Decision**

The P value of 0.057 for residential area obtained from SPSS shown in Table 5.5 shows that the test is insignificant and thus we fail to reject Ho and conclude that there no association between mobile money service use and the residential area of a respondent.

### 5.5.2 Relationship Between Mobile Money Usage and Employment Status

Ho: There is no association between mobile money service use and the employment status of a respondent.

**Decision**

The P value of 0.004 for employment status obtained from the SPSS shown in Table 5.5 shows that the test is significant and thus we reject Ho and conclude that there is adequate evidence to suggest an association between mobile money service use and employment status of a respondent.

### 5.5.3 Relationship Between Mobile Money Usage and Age

Ho: There is no association between mobile money service use and the age of a respondent

**Decision**

The P value of 0.055 for age obtained from the SPSS shown in Table 5.5 shows that the test is insignificant and thus we fail to reject Ho and conclude that there no association between mobile money service use and the age of a respondent.

### 5.5.4 Relationship Between Mobile Money Usage and Earnings

Ho: There is no association between mobile money service use and earnings

**Decision**

The P value of 0.105 for earnings obtained from the SPSS shown in Table 5.5 shows that the test is insignificant and thus fail to reject Ho and conclude that there no association between mobile money service use and the earnings of a respondent.

### 5.5.5 Summary on Adoption Versus Demographic Characteristics

The findings in Section 5.5 shows that there is no evidence to suggest a correlation between mobile money adoption and three of the demographic characteristics namely, residential area, age and monthly earnings. There however is a correlation between mobile money adoption and employment status. These may be due to the fact that people who are in some form of employment are usually the breadwinners hence need to send money to their dependencies.

## 5.6 Analysis of Perceived Security Construct

The results of the questionnaire analysis resulted in the following observations being drawn. The analysis done to find out the conceptual beliefs of mobile money users on security related issues showed that users do not view security features on mobile money systems as hindering adoption. Users believe they should play a role in ensuring the security of their mobile money accounts. Users of mobile money services believe security of mobile money systems is more important than other attributes namely affordability, ease of use and usefulness. The users viewed security as the most important aspect with no user ranking security as least important amongst the mobile money systems attributes This is in agreement with findings by Brown et al (2003, Featherman and Pavlou (2003), GaneshSankar (2011), Koenig-Lewis et al (2010) and Martin (1998). Users however feel mobile money transactions can be intercepted though they still use mobile money.

The researcher noted that most of the non users cited security related issues as the main characteristic that would lure them to use mobile money systems. On reasons why they do not use mobile money most cited non usefulness of the service and mentioned security as the third

most popular reason why they do not use mobile money. The results showed that the users believe security is important to mobile money systems.

The researcher noted that most of the mobile money users are aware of security features available on their mobile money systems and they do check on the security features available on their services. They also use services from service providers who make them aware of security features available on their mobile money services through adverts. Most of the mobile money users are aware of transactional alert shortcodes from their providers and would verify the origins of mobile money transactional alert messages.

The users of mobile money ranked security as the second most important reason why they chose their mobile money service after usefulness. Users check the authenticity of the handsets they use for mobile money so as to get software updates from official websites. Most users have Bluetooth enabled handsets but switch the service off immediately after use. Users of mobile money do not share their phones with others and use security lock features present on the gadgets. They do not share mobile money account usage credentials and most of those who change these access credentials change them at least once a month. They do not borrow mobile money accounts but use their own. The users are satisfied with the security related conduct exhibited by their mobile money service providers. The users have not fallen prey or had anyone who has fallen prey to malicious elements on mobile money systems.

Users however exhibit behaviour that makes them vulnerable to attacks on mobile money systems. Most of them did not attend awareness trainings prior to adopting mobile money. A large group of the users use the Android operating system on their handsets which is prime target of most malware developers (Phifer, 2013). Most of them do not use antivirus software on their phones and those who have it do not update it or take longer to update it exposing themselves to malware threats. The majority of these users download applications from unofficial sites further increasing the risk they expose themselves to. A large group of users do not change their mobile money account access credentials thereby increasing the risk of having the credentials guessed by malicious elements. Most of these users are aware that network issues may affect system availability but still use the services.

The researcher noted that most of the mobile money users trust that their service providers are fair in their conduct of transactions done by customers. Most of these customers have trust in the mobile network providers. The users also trust the wireless infrastructure used by the network providers. They however believe that mobile money systems may incorrectly process transactions. They also fear that careless mistakes can make them lose money whilst transacting on these mobile money systems. Generally though users of mobile money systems trust the mobile money service they use.

From the analysis the researcher concluded that users conceptually value security. They also exhibit traits that reveal the wish to have a secure mobile money account. They however show characteristics that expose them to risks as they transact on the mobile money systems like downloading applications from third part sites. However for them to adopt a mobile money package it is what they think more than what they will do when they are now using the service that matters. Basing on this, the researcher concluded that the conceptual points raised coupled with a number of positive security related behaviour exhibited by users, perceived security has got an impact on the adoption of mobile money. Users expect mobile money systems to be secure for them to use them.

## 5.7 Research Objectives

This section looks at how research questions were answered and how research objectives were met. It also looks at the outcome of the hypothesis testing done in order to assist in answering the research questions and meet the objectives. This section ties back the results to the research objectives and give the extent to which each of the objectives was met. The objectives are listed and a brief of how each was met or not met is given below each objective.

### 5.7.1 To establish whether there exists a correlation between security concerns of GSM mobile money systems and their adoption.

The research results in Section 5.4 showed that there exists adequate evidence to suggest a correlation between perceived security and mobile money adoption ($P<0.05$ see Table 5.4). Section 5.6 further shows that users value mobile money security. In Section 5.3 mobile money

perceived security was seen to be the second most important aspect considered by consumers when they chose a mobile money service. These findings show that there is a correlation between security concerns of GSM mobile money systems and their adoption agreeing with earlier research by Laforet and Li (2005), Luarn and Lin (2005), Yang (2009).

### 5.7.2 To find factors that affect uptake rate of GSM mobile money by users in order of precedence

The results in Section 5.3 (see Table 5.3) showed perceived usefulness to have a significant influence on the adoption of mobile money over cellular networks. It is the most important aspect of mobile money systems agreeing with Mas (2013), Koenig-Lewis et al (2010) and Nzoutchoum (2012). People adopt mobile money when they deem that the product is of value and will benefit them. Respondents who are currently using mobile money thought of it as useful. The second most important attribute is perceived security, followed by perceived cost then lastly perceived ease of use (see Table5.3).

### 5.7.3 To give a guideline of the acceptable tradeoff between security and other system critical factors to be considered by operators on GSM mobile money product implementation

Results in Section 5.3 show that perceived usefulness is the most important aspect of mobile money considered by users. Security is the second most important (see Table 5.3). All other perceived constructs (trust, cost, ease of use) have a correlation with mobile money adoption as well as shown in Section 5.4 even though they may not be as influential as perceived usefulness and perceived security. It is critical for mobile money service providers to know how to fuse the attributes together in their product to come up with the optimum product for their market. This research shows that perceived security and perceived usefulness require bigger attention than other attributes in designing the mobile money package.

## 5.8 Research Questions

This section seeks to show how research questions were answered and give the extent to which this was so. The questions are listed and a brief of how each was answered or not answered is given below each question.

### 5.8.1 What are the security risks associated with mobile money over cellular networks?

Section 2.4 looked at the security risks posed by the GSM architecture like man in the middle attacks caused by one way authentication and IMSI theft. Section 2.5 then looked at SIM card security, explaining the risks posed by the use of SIM cards in mobile money like SIM cloning. Section 2.6 then looked at handset security, giving an insight into some of the security issues that could arise because of the mobile operating systems used by the mobile money gadgets like malware infections. The combination of these sections shows that mobile money over GSM is not without its worries in terms of security.

### 5.8.2 Why is mobile money uptake rate higher in Africa compared to the developed world?

The biggest reason why there is a higher uptake of mobile money in Africa compared to the developed world is the lack of financial inclusion options for the majority. Traditional banks are scarce and their requirements are not within reach for the majority as seen in Section 2.7. In Europe and the developed world people can choose such that mobile money is not a necessity.

### 5.8.3 How does the security of USSD and STK based systems compare?

STK systems are more secure than USSD systems. STK does not display customer personal identification numbers, it encrypts. STK is like a dedicated channel from a security perspective. The advantages of USSD are that it is cheaper to implement and is universally accessible to every phone (see Section 2.8).

### 5.8.4 Do users in Africa value security when adopting a mobile money technology?

The research was done in parts of Zimbabwe an African country. Section 5.4 showed that there is enough evidence to suggest a correlation between perceived security and mobile money adoption in the study population. Section 5.6 also showed that users value security of their mobile money systems. Since Zimbabwe is an African country, it can be taken as a representative sample of the African continent population. The researcher thus concluded that African users value mobile money security.

### 5.8.5 What was the best way for NetOne to follow in rolling out its mobile money project?

Results in Section 5.3 show that perceived usefulness is the most important aspect of mobile money considered by users. Security is the second most important (see Table 5.3). All other perceived constructs (trust, cost, ease of use) have a correlation with mobile money adoption as well as shown in Section 5.4 even though they may not be as influential as perceived usefulness and perceived security. It is critical for mobile money service providers like NetOne to know how to fuse the attributes together in their product to come up with the optimum product for their market. This research shows that perceived security and perceived usefulness require bigger attention than other attributes in designing the mobile money package.

Results indicate that users will adopt mobile money if they regard it as easy to use (see Table 5.4). It is thus of high importance to develop mobile money systems that are easier to use. Factors that make a product qualify as easier to use include wide screens on mobile devices, easy to understand terminology on product menus, portability of product on all gadget forms, usable keypads, easier access of agent network and easy registration or enrollment into the mobile money systems as well as flexible working hours for agents.

The obtained results indicate that perceived cost is of significance influence to the adoption of mobile money (see Table 5.4). High tariffs on product usage are thus a deterrent factor to mobile money usage. People tend to shun highly priced products. Zimbabwe as a country is experiencing low employment rates and lower salaries and wages as depicted by the demographic results (see Section 4.2.5). The setting of the research may thus be a contributing factor. This is an area that may need a relook in a different setting in future for comparison of results.

Results indicate that users will adopt a mobile money product they deem to be secure (see Table 5.4). The users conceptually want mobile money products that address their security concerns. They however may exhibit behaviour that contradicts this characteristic. None of the users indicated knowledge of a relative or friend who has lost money due to hackings or related breaches and practices. Perceived security/risk issues are thus of significance to the adoption of mobile money systems but not the only thrust.

NetOne as a firm invested a huge amount of money in acquiring STK based secure mobile money system whose cost is not justifying the returns. According to the research this was a proper way to do things but the company may need to look at other factors that may be hindering adoption of its product. The company needs to look at other marketing strategies to lure customers to use its product like increasing product usefulness as shown by Table 5.3.

The results obtained point to a trend whereby users of mobile money adopt the product when they regard providers and the enabling technology to be trustworthy. The customer's trust will affect the customer's behavioural intention and loyalty. According to (Masinge, 2010) trust has negative significant correlation with perceived risk/security. It is therefore critical that mobile money providers like NetOne and would be implementers of the mobile money service should maintain high standards of trustworthiness at all levels.

### 5.9 Chapter Conclusion

The chapter analysed the questionnaire data and interpreted results to give meaning to findings. The findings revealed that all the five constructs, perceived usefulness, perceived security, perceived cost, perceived trust and perceived ease of use affect mobile money adoption. The findings also revealed that the most important attribute of mobile money is perceived usefulness followed but perceived security. Users may exhibit behaviour that exposes them to risks as they transact but they expect the systems to be secure before they adopt them. The research also showed that users trust the mobile money systems they use.

# Chapter 6 – Conclusions and Recommendations

## 6.1 Introduction

This chapter reviews the research background and objectives and proceeds to summarise the research findings. It then concludes with recommendations for future work in the related field.

## 6.2 Research Background and Objectives - Review

The study aimed to investigate the effects of security concerns on the adoption of mobile money over cellular networks and find other factors that affect adoption. It sought to find security risks associated with mobile money over cellular networks. The research intended to answer the following:

What are the security risks associated with mobile money over cellular networks? Why is mobile money uptake rate higher in Africa compared to the developed world? Do users in Africa value security when adopting a mobile money technology? What factors do the users consider when adopting mobile money? How does the security of USSD and STK based systems compare? What was the best way for NetOne to follow in rolling out its mobile money project?

The factors that the study focused on were:

- Perceived usefulness of mobile money systems
- Perceived ease of use of mobile money systems
- Perceived cost of mobile money services
- Perceived security/risk of mobile money services (divided into facets, financial risk, performance risk, security privacy risk)
- Perceived trust (from two perspectives: wireless infrastructure and service providers)

### 6.3 Practical Implications for Business

Results obtained indicate that 74.6% of respondents are currently using mobile money while 25.4% do not use. Of those who use 97.2% use the non STK based service while 2.8% use the security focused STK based service. The research revealed that customers are security conscious. The researcher noted that most of the non users cited usefulness and security related issues as the main characteristic that would lure them to use mobile money systems. Mobile money providers should thus concentrate their energies towards product security and product usefulness without ignoring ease of use and cost. Marketing drive should emphasize on those key issues.

Customers need to know that service providers and their service enabling technologies can be trusted. Marketing teams need to always advertise capabilities that are achievable and already implemented on their mobile money systems to avert customer frustration and distrust. Customer trust has an effect on customer loyalty thus trusted mobile money service providers have a better opportunity of gaining market share (Masinge, 2010).

Cost has significant influence on mobile money adoption thus mobile money providers should seriously consider reducing the costs of mobile money to lure more customers. Users will increase due to reduced costs and the provider will benefit from driving volumes. It will be less costly and justifiable to establish new branches in previously un-serviced locations thereby increasing product visibility and accessibility which benefits both the provider and the customer.

Some users showed lack of knowledge about mobile money. Mobile money providers should conduct awareness programs for both enrolled an un-enrolled customers to increase product knowledge. Trainings should cover functionality, benefits and safety of the product to instill a culture of technology usage in the population that will make it easier to introduce new innovative products to an embracing population.

### 6.4 Recommendation for Future Research

The research results indicated that customers consider security when adopting a mobile money service. The role played by demographic variables on mobile money adoption was not explored extensively. Future research may need to explore the effects of demographic variables like age,

gender, race, education level, average income, religion and culture on adoption of mobile money systems.

The study was conducted in an environment that does not offer many options to consumers. It was also done in an environment where MFS is fairly new. It may be necessary to perform the study again in a changed environment when mobile money technology has aged and customers are more informed about mobile money. Adoption of mobile financial services in developed nations may be driven more by convenience than by the need to provide infrastructure for electronic access to financial services and products as in developing nations like Zimbabwe (Cheney, 2008).

The research did not look at the adoption factors that have to do with the marketing strength of the mobile money services provider. Marketing strategies and promotions do persuade users to adopt a service they would otherwise not have used. Users end up adopting and getting used to a service which seemed alien to them in a not so distant past because of good marketing skills. Future research may consider this.

### 6.5 Conclusion

The mobile money market is influenced by many factors which are mutually interconnected. The main aim is to develop working systems in which all stakeholders play their appropriate roles. The only way to achieve the aim is to have the final consumers adopt the end product. The main aim of this research was to point out a whole series of factors which are crucial to the adoption of mobile money with special emphasis on perceived security/risk.

The research successfully identified security loopholes in mobile money as posed by the nature of GSM and the other enabling technologies and customer behaviour. It managed to highlight the reasons for different adoption patterns mobile money in the developed and the developing world. The research contributes to the IT/IS systems acceptance research as it successfully revealed the effects of perceived security concerns on adoption of mobile money over cellular networks

## References


ABA Banking Journal. (2011). Mobile banking security concerns stalling adoption. *ABABankingJournal*. Retrieved November 7, 2012, from http://www.ababj.com/tech-topics-plus/mobile-banking-security-concerns-stalling-adoption-2205.html

Abunyang, E. (2007). *Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services.* Retrieved from http://masalai.files.wordpress.com/2009/03/sms-bank-in-developing-countries.pdf

Aker, J. C., & Mbiti, I. M. (2010). Mobile Phones and Economic Development in Africa. *Journal of Economic Perspectives*, *24*, 207–232.

Al-Muhtadi, J., Mickunas, D., & Campbell, R. (2002). A lightweight reconfigurable security mechanism for 3G/4G mobile devices. *Wireless Communications, IEEE*, *9*(2), 60–65.

Ashford, W. (2012). Security concerns hold back mobile banking adoption. Retrieved March 18, 2013, from http://www.computerweekly.com/news/2240163841/Security-concerns-hold-back-mobile-banking-adoption

Aweda, T. (2010). *The Value in Value Added Services. Ciuci Consulting*. Retrieved from http://www.ciuci.us/newsletter/ValueAdded.pdf

Barati, S., & Mohammad, S. (2009). An efficient Model to Improve Customer Acceptance of Mobile Banking. *In World Congress on Engineering and Computer Science* (Vol. 2, pp. 20–22). San Fransisco , USA.

Barkan, E., Biham, E., & Keller, N. (2003). Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. *In Advances in Cryptology-CRYPTO 2003* (pp. 600–616). Springer Berlin Heidelberg. Retrieved from http://www.ma.huji.ac.il/~nkeller/biham_gsm.pdf

Beheshti, A. A., & Toorani, M. (2008). Solutions to the GSM Security Weaknesses. *2nd International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST'08)* (pp. 576–581). Cardiff: IEEE. doi:DOI 10.1109/NGMAST.2008.88

Benamati, B., & Serva, A. (2007). Trust and distrust in online banking: Their role in developing countries. *Information Technology for Development*, *13*(2), 161–175.

Boden, R. (2014). Two thirds of UK smartphone owners open to the idea of mobile wallets. *NFC World*. Retrieved July 22, 2014, from http://www.nfcworld.com/2014/07/10/330302/two-thirds-uk-smartphone-owners-open-idea-mobile-wallets/

Brookson, C. (1994). *GSM (and PCN ) Security and Encryption.* Retrieved from http://www.brookson.com/gsm/gsmdoc.doc

Brookson, C. (2005). Smart card cloning is easy! (GSM SIMs). Retrieved April 2, 2012, from http://www.brookson.com/gsm/cardclone.pdf

Brown, I., Cajee, Z., Davies, D., & Stroebel, S. (2003). Cell phone banking: predictors of adoption in South Africa -an exploratory study. *International Journal of ¡nformation Management, 23*, 381–394.

Carlsson, C., Walden, P., & Bouwman, H. (2006). Adoption of 3G+ services in Finland. *International Journal Mobile Communications*, *4*(4), 369–385.

Chemwe, G. W. (2010). Security issues faced by mobile cash transfer applications in Kenya on GSM and 3G networks. *JKUAT Scientific ,Technological and Industrialisation Conference* (pp. 330–336). Nairobi. Retrieved from elearning.jkuat.ac.ke/journals/ojs/index.php/jscp/article/view/714/659

Cheney, J. S. (2008). An Examination of Mobile Banking and Mobile Payments: Building Adoption as Experience Goods? Retrieved from http://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2008/D2008MobileBanking.pdf

Chitungo, S. K., & Munongo, S. (2013). Extending the Technology Acceptance Model to Mobile Banking Adoption in Rural Zimbabwe. *Journal of Business Administration and Education*, *3*(1), 51–79.

Chung, N., & Kwon, S. J. (2009). The Effects of Customers' Mobile Experience and Technical Support on the Intention to Use Mobile Banking. *CyberPsychology and Behavior*, *12*(5).

Cobert, B., Helms, B., & Parker, D. (2012). Mobile money: Getting to scale in emerging markets. McKinsley and Company.

Dammann, J. (2011). IMSI-Catcher and Man-in-the-Middle attacks. *Seminar Mobile Security*. Retrieved from http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/10ws/10ws-sem-mobsec/talks/dammann.pdf

David, N., & Penicaud, C. (2011). *State of the Industry: Results from the 2011 Global Mobile Money Adoption Survey*.

Dimov, D. (2013). Mobile Phone Spying Software: Legality, Symptoms, and Removal. *Infosec Institute*. Retrieved March 4, 2014, from http://resources.infosecinstitute.com/mobile-phone-spying-software-legality-symptoms-and-removal/

Dube, T., Njanike, K., Manomano, C., & Chiriseri, L. (2011). Adoption And Use of SMS/Mobile Banking Services in Zimbabwe: An Exploratory Study. *Journal of Internet Banking and Commerce*, *16*(2).

Erdem, T., & Swait, J. (2004). Brand credibility, brand consideration, and choice. *Journal of Consumer Research*, *31*(1), 191–198.

FBI and Department of Homeland Security. (2013). Threats to Mobile Devices Using the Android Operating System. Retrieved November 20, 2013, from http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*, 451–474.

Gadaix, E. (2001). GSM and 3G Security. *Proceedings of Black Hats Conference*. Singapore: eGlobal.

GaneshSankar, B. M. (2011). *Trust and Security Issues in Mobile Banking and its effects on customers*. Blekinge Institute of Technology. Retrieved from http://www.bth.se/fou/cuppsats.nsf/all/d50bc0fa6f021c46c125795900768dd1/$file/BTH2011Bilal.pdf

Gold, S. (2011). Cracking GSM. *Network Security*, *2011*(4), 12–15.

Golde, N. (2012). E-Plus GSM privacy/TMSI allocation leak. Retrieved May 28, 2014, from http://nion.modprobe.de/blog/archives/705-E-Plus-GSM-privacyTMSI-allocation-leak.html

Hair, J. F. J., Anderson, R., Tatham, R., & Black, W. C. (1998). Multivariate Data Analysis (5th ed.). Upper Saddle River, New Jersey: Prentice Hall.

Hord, J. (2005). How SMS Works. *HowStuffWorks.com*. Retrieved May 28, 2014, from http://computer.howstuffworks.com/e-mail-messaging/sms.htm

InterMedia. (2013). *Mobile money in Tanzania Use, Barriers and Opportunities*. Retrieved from http://www.intermedia.org/wp-content/uploads/FITS_Tanzania_FullReport_final.pdf

International Telecommunications Union. (2009). *Information Society Statistical Profiles 2009 Africa*. Retrieved from http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-RPM.AF-2009-PDF-E.pdf

Jimenez, A., & Vanguri, P. (2010). Cash Replacement through Mobile Money in Emerging Markets: The FISA Approach. New York. Retrieved from http://www-05.ibm.com/za/office/pdf/g-cash.pdf

Jorja, W., Dawson, M. E., & Omar, M. (2012). Cyber Security and Mobile Threats: The need for Antivirus Applications for Smart Phones. *Journal of Information Systems and Planning*, *5*(14), 40–50.

Jover, R. P., & Giura, P. (2013). How Vulnerabilities in Wireless Networks Can Enable Advanced Persistent Threats. *International Journal on Information Technology*.

Juniper Networks. (2012). *2011 Mobile Threats Report*. Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

Kabweza, L. S. M. (2012). EcoCash mobile money registered users now over 1.7 million. *TechZim*. Retrieved June 10, 2013, from http://www.techzim.co.zw/2012/10/ecocash-mobile-money-registered-users-now-over-1-7-million/

Kessler, S. (2011). Near Field Communication: A Quick Guide to the Future of Mobile. Retrieved January 26, 2014, from http://mashable.com/2011/08/11/near-field-communication-guide/

Khan, W., & Ullah, H. (2010). Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography. *International Journal of Computer Science Issues*, *7*(3), 10–16. Retrieved from http://ijcsi.org/papers/7-3-9-10-16.pdf

Koenig-Lewis, N., Palmer, A., & Moll, A. (2010). Predicting young consumers' take up of mobile banking services. *International Journal of Bank Marketing*, *28*(5), 410–432.

Korhan, J. (2011). How QR Codes Can Grow Your Business. Retrieved January 26, 2014, from http://www.socialmediaexaminer.com/how-qr-codes-can-grow-your-business/

Krugel, G. T. (2007). *An Overview of the different mobile banking technology options, and their impact on the mobile banking market.* Retrieved from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/finmark_mbt_aug_07.pdf

Kumar, M. (2013). Sim Card Cloning Hack affect 750 million users around the world. Retrieved January 26, 2014, from http://thehackernews.com/2013/07/sim-card-cloning-hack-affect-750.html

Laforet, S., & Li, X. (2005). Consumers' attitudes towards online and mobile banking in China. *International Journal of Bank Marketing*, *23*(5), 362–380.

Lee, A. (2008). STK Toolkit up to 36 times faster than hardware encryption. Retrieved August 10, 2014, from http://www.primefactors.com/press-releases/89-alex-lee-inc-solves-pci-performance-problem-with-software-encryption-from-prime-factors

Lee, J.-H. (2013). Effects of Trust and Perceived Risk on User Acceptance of a New Technology Service. *Social Behaviour and Personality*, *41*(4), 578–598.

Luarn, P., & Lin, H.-H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computers in Human Behavior*, *21*(6), 873–891.

Lyne, M. (2009). What Is A QR Code And Why Do You Need One? Retrieved January 26, 2014, from http://searchengineland.com/what-is-a-qr-code-and-why-do-you-need-one-27588

Martin, J. (1998). Say goodbye to bankers' hours. *Management Review*, *87*(1), 33–37.

Mas, I. (2013). Why is the Progress of Mobile Money So Gradual and Patchy. Retrieved April 18, 2014, from http://www.cgap.org/blog/why-progress-mobile-money-so-gradual-and-patchy

Masinge, K. (2010). *Factors influencing the adoption of mobile banking services at the Bottom of the Pyramid in South Africa*. Maters thesis, University of Pretoria , Pretoria, South Africa.

Matuszewski, D. (2012). GSM Security. São Paulo. Retrieved from http://grenoble.ime.usp.br/~gold/cursos/2012/movel/GSM security.pdf

Metaforic. (2012). *Mobile banking, Consumer Security Practices and the growing risk to banks*. Retrieved from http://info.metaforic.com/MobileSecPopup.html?CID=70120000000pGVd&status=Responded&s=Website

Michaels, L. (2011). It's Better Than Cash: Kenya Mobile Money Market Assessment. Retrieved from http://www.merchantpro.co/betterthancash.pdf

Mikesell, A. (2012). 4 main technologies underlying mobile commerce apps. Retrieved January 26, 2014, from http://www.mobilemarketer.com/cms/opinion/columns/13201.html

Moran, A. (2011). Mobile Money. *YouGov*. Retrieved June 20, 2014, from http://yougov.co.uk/news/2011/06/17/mobile-money

Mordkoff, T. J. (2011). *The Assumption(s) of Normality*. Retrieved from http://www2.psychology.uiowa.edu/faculty/mordkoff/GradStats/part 1/I.07 normal.pdf

Nohl, K. (2013). "SIM card exploitation" at OHM, Aug 3 2013. Retrieved January 26, 2014, from https://srlabs.de/sim-card-exploitation-at-ohm-aug-3-2013/

Nokia. (2002). GSM Architecture. Retrieved April 20, 2014, from http://www.roggeweck.net/uploads/media/Student_-_GSM_Architecture.pdf

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric Theory* (3rd ed.). New York: McGraw-Hill.

Nzoutchoum, T. A. L. (2012). *Customer adoption and financial services literacy in mobile financial services Case Study in Uganda*. Master's thesis, Université Libre de Bruxelles. Retrieved from http://www.professionsfinancieres.com/docs/2013140936_201_vn_m_customer_adoption_and_financial_literacy.pdf

Pallant, J. ., & Tennant, A. (2007). An introduction to the Rasch measurement model: An example using the Hospital Anxiety and Depression Scale (HADS). *British Journal of Clinical Psychology*, *46*, 1–18.

Penicaud, C. (2012). *State of the Industry: Results from the 2012 Global Mobile Money Adoption Survey*. Retrieved from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/MMU_State_of_industry.pdf

Phifer, L. (2013). Comparing mobile operating systems' manageability and security. Retrieved January 26, 2014, from http://searchconsumerization.techtarget.com/tip/Comparing-mobile-operating-systems-manageability-and-security

Rao, J., Rothagi, P., & Scherzer, H. (2002). Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards. *IEEE Symposium on Security and Privacy* (pp. 31–41). Oakland: IEEE. doi:dx.doi.org/10.1109/SECPRI.2002.1004360

Rhee, M. Y. (2009). *Mobile Communication Systems* (pp. 10–12). John Wiley and Sons (Asia) Pte Ltd.

Rhiel, S. G., & Chaffin, W. W. (1996). An Investigation of the Large-Sample/Small-Sample Approach to the One-Sample Test for a Mean (Sigma Unknown). *Journal of Statistics Education*, *4*(3). Retrieved from http://www.amstat.org/publications/jse/v4n3/rhiel.html

Rizzo, C., & Brookson, C. (2014). Security for ICT - the Work of ETSI. Retrieved from http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp1_security.pdf

Roboff, G., & Charles, C. (1998). Privacy of financial information in cyberspace: banks addressing what consumers want. *Journal of Retail Banking Services*, *20*(3), 51–56.

Rogers, E. M. (1995). *Diffusion of innovations*. *Diffusion of innovations* (4th ed., p. 518). New York: Free Press.

Rouse, M. (2010). WAP (Wireless Application Protocol). Retrieved January 26, 2014, from http://searchmobilecomputing.techtarget.com/definition/WAP

Ruggiero, P., & Foote, J. (2011). *Cyber Threats to Mobile Phones*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

SANS Institute. (2001). *The GSM Standard (An overview of its security)*. Retrieved from http://www.sans.org/reading-room/whitepapers/telephone/gsm-standard-an-overview-security-317

Sahin, I. (2006). Detailed Review of Rogers' Difussion of Innovations Theory and Educational Technology-Related Studies Based on Roger's Theory. *The Turkish Online Journal of Educational Technology*, *5*(2), 14–23.

Saleem, Z., & Rashid, K. (2011). Mobile Banking Adoption in Banking Sector of Pakistan. *Journal of Yasar University*, *21*(6), 3538–3560.

Sanganagouda, J. (2011). USSD: A Communication technology to potentially oust SMS dependency. Retrieved from http://www.aricent.com/sites/www.aricent.com/files/pdf/Aricent_USSD_WhitePaper.pdf

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing*, *17*(7), 324–334.

Sayid, O. (2012). Investigating Mobile Money Acceptance in Somalia: An Empirical Study. *Pakistan Journal of Commerce and Social Science*, *6*(2), 269–281.

Sekeran, U. (1992). *Research Method for Business A Skill Building Method*. (J. Marshall & P. McFadden, Eds.) (4th ed., p. 326). Illinois: John Wiley and Sons, Inc.

Singh, T., Kumar, A., & Liu, Y. (2011). Channels and Identities in GSM. *International Journal of Electronics and Communication Technology*, *2*(3), 210–214.

Smart City Magazine. (2013). *The rise of mobile money- how a low tech revolution is re-shaping the global economy*. Retrieved from https://s3-eu-west-1.amazonaws.com/smartcity/SCM_The_Rise_of_Mobile_Money_2013-interactive.pdf

Smith, M., Schridde, C., & Freisleben, B. (2008). *An Identity-Based Key Agreement Protocol for the Network Layer*. (R. Ostrovsky, R. De Prisco, & I. Visconti, Eds.)*Security and Cryptography for Networks* (pp. 409–422). Marburg: Springer Berlin Heidelberg. doi:10.1007/978-3-540-85855-3_27

Srlabs. (2013). Rooting SIM cards. Retrieved January 26, 2014, from https://srlabs.de/rooting-sim-cards/

Tan, M., & Teo, T. S. H. (2000). Factors Influencing the Adoption of Internet Banking. *Journal of the Association for Information Systems*, *1*(5), 1–42.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55. doi:10.5116/ijme.4dfb.8dfd

Telecom-week. (2012). Banking on the unbanked in Africa. *AfricaTelecomsNews*. Retrieved November 10, 2012, from http://www.africantelecomsnews.com/resources/Mobile_Money_Africa_background.shtml

The Economist. (2012). Mobile money services Let us in. *The Economist*. Retrieved April 19, 2014, from http://www.economist.com/node/21560878

Tiwari, R., Buse, S., & Herstatt, C. (2007). Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage. *in: Proceedings of the International Research Conference on Quality, Innovation and Knowledge Management* (p. 3). New Delhi.

Tobbin, P., & Kuwornu, J. K. . (2011). Adoption of Mobile Money Transfer Technology: Structural Equation Modeling Approach. *European Journal of Business and Management*, *3*(7), 59–77.

US-CERT. (2010). Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices. *United States Computer Emergency Readiness Team*. Retrieved April 20, 2014, from https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf

Van de Merwe, P. B. (2003). *Mobile Commerce over GSM: A Banking Perspective on Security*. Unpublished Master's thesis, University of Pretoria, Pretoria, South Africa.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204.

Vincent, J. (2013). Sim cards hacked: A single text that unlocks millions of mobiles. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/sim-cards-hacked-a-single-text-that-unlocks-millions-of-mobiles-8726638.html

Wang, Y.-S., Wang, Y.-M., Lin, H.-H., & Tang, T.-I. (2003). Determinants of user acceptance of internet banking: an empirical study. *International Journal of Service Industry Management*, *14*(5), 510–519.

Wright, S. (2012). University researchers document Android adware privacy risks. Retrieved March 4, 2013, from http://searchsecurity.techtarget.com/news/2240147136/University-researchers-document-Android-adware-privacy-risks

Yan, Q., Li, Y., Li, T., & Deng, R. (2009). *Insights into Malware Detection and Prevention on Mobile Phones* (pp. 243–249). Retrieved from http://www.researchgate.net/publication/221318032_Insights_into_Malware_Detection_and_Prevention_on_Mobile_Phones/file/9fcfd510b06cde9307.pdf

Yang, A. S. (2009). Exploring Adoption Difficuities in Mobile Banking Services. *Canadian Journal of Administrative Sciences*, *26*(2).

Yousef, P. (2004). *GSM-Security: A Survey and Evaluation of the Current Situation*. Unpublished Master's thesis, Linköping University, Linköping, Sweden.

Yu, C.-S. (2012). Factors affecting individuals to adopt mobile banking: Empirical evidence from the UTAUT model. *Journal of Electronic Commerce Research, 13*(2), 104–121.

ZimStat. (2012). *Women and Men in Zimbabwe Report 2012*. Retrieved from http://www.zimstat.co.zw/dmdocuments/Gender/Report2012.pdf

**Appendix A: Survey Questionnaire**

**Questionnaire for mobile money users**

I am Masters student studying at Rhodes University, Grahamstown, South Africa, towards an M.Sc. in Computer Science, specialising in Information Security. As part of my research I am carrying out an investigation into the role played by security in the adoption of mobile money services on cellular networks.

Thank you for taking the time to fill in this questionnaire. This questionnaire consists of 53 questions and 9 pages. It should only take 15-20 minutes of your time. Responses are indicated by marking the appropriate box at the far right with an '**X**' or filling in more detailed responses where requested. Responses will be treated with complete confidentiality. All questions are optional, but it would assist in the research if you could complete the form as fully as possible. If you have any questions about this questionnaire, please contact Madebwe Charles (g12m7032@campus.ru.ac.za).

| | **Section A** | |
|---|---|---|
| 1 | Do you own a cell phone? | |
| | Yes | |
| | No | |
| 2 | Do you use mobile money? | |
| | Yes | |
| | No | |
| | *If you DO NOT use mobile money, go to Section B on page 7* | |
| 3 | Which service do you use for mobile money? | |
| | EcoCash | |
| | OneWallet | |
| 4 | Are you aware of any security feature(s) available on your mobile money service? | |
| | Yes | |
| | No | |
| | *If you answered yes for question 4 above, go to 4a otherwise go to question 5.* | |
| 4a | Would you continue using the mobile money service if these security features were increased/enhanced? | |
| | Yes | |
| | No | |
| 5 | Do security measures on mobile money systems reduce user friendliness? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |

| | | |
|---|---|---|
| | Strongly disagree | |
| | | |
| 6 | Does your mobile money service provider air adverts on the security features available on their service? | |
| | Yes | |
| | No | |
| 7 | Did you go through a mobile money security awareness training before using mobile money? | |
| | Yes | |
| | No | |
| 8 | Do you think users should go through security awareness training before adopting mobile money? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |
| 9 | Did you have your mobile handset scanned for viruses before using mobile money? | |
| | Yes | |
| | No | |
| 10 | Do you believe mobile money transactions can be intercepted? | |
| | Yes | |
| | No | |
| | *If you answered yes for question 10 above, go to 10a otherwise go to question 11 .* | |
| 10a | What do you think is the likelihood of that happening ? | |
| | Highly likely | |
| | Likely | |
| | Moderate | |
| | Unlikely | |
| | Highly unlikely | |
| 11 | Are you aware of the SMS shortcodes used by your mobile money service provider for alerts relating to mobile money transactions? | |
| | Yes | |
| | No | |
| | | |
| 12 | When you receive mobile money SMS messages do you verify their origin? | |
| | Yes | |
| | No | |
| 13 | Do you believe users have a role to play in ensuring the security of their mobile money? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |

| | | |
|---|---|---|
| | | |
| 14 | Do you feel secure sending sensitive information over mobile banking? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |
| 15 | Which mobile money product attribute is more important than the other? | |
| | Security | |
| | Usefulness | |
| | Equally important | |
| 16 | Which mobile money product attribute is more important than the other? | |
| | Security | |
| | Affordability | |
| | Equally important | |
| 17 | Which mobile money product attribute is more important than the other? | |
| | Security | |
| | Ease of use | |
| | Equally important | |
| 18 | What was the most important factor that you considered when you chose your current mobile money service (tick one)? | |
| | It enables me to accomplish my tasks easier due to useful, innovative services | |
| | Using the mobile wallet does not require a lot of mental effort | |
| | The service is secure, risk free, trustworthy and reliable | |
| | The service is affordable to use | |
| | Other reason(please specify below) | |
| | | |
| 19 | On a scale of 1-5, 1 being least important, 5 being very important , how do you rank the importance of security to mobile money systems? | |
| | 1 (Least important) | |
| | 2 | |
| | 3 | |
| | 4 | |
| | 5 (Very important) | |
| 20 | Do you use antivirus software for your mobile phone? | |
| | Yes | |
| | No | |
| | *If you answered yes for question 20 above, go to 20a otherwise go to question 21.* | |
| 20a | How often do you update the antivirus software? | |
| | Daily | |
| | Twice a week | |
| | Weekly | |
| | Monthly | |

| | | |
|---|---|---|
| | Less frequently than monthly | |
| | Never | |
| 21 | Have you verified that your mobile phone from the displayed brand (e.g. if branded Nokia, have you verified that it is from Nokia)? | |
| | Yes | |
| | No | |
| 22 | Do you download software applications to your mobile phone? | |
| | Yes | |
| | No | |
| | *If you answered yes for question 22 above, go to 22a otherwise go to question 23.* | |
| 22a | Do you download from official sites only? | |
| | Yes | |
| | No | |
| 23 | Which mobile operating system software is used by your mobile phone? | |
| | Android | |
| | Symbian | |
| | Windows | |
| | Blackberry | |
| | Java ME | |
| | Other(specify below) | |
| | | |
| 24 | Does your phone have Bluetooth capabilities? | |
| | Yes | |
| | No | |
| | *If you answered yes for question 24 above, go to 24a otherwise go to question 25.* | |
| 24a | Do you always switch it off after use? | |
| | Yes | |
| | No | |
| 25 | Do you share your mobile phone with others? | |
| | Yes | |
| | No | |
| 26 | Do you share your mobile wallet usage credentials with others (spouse, friends or relative)? | |
| | Yes | |
| | No | |
| 29 | Do you use the security lock on your mobile phone? | |
| | Yes | |
| | No | |
| 30 | Do you renew/change the password/personal identification number (PIN) of your mobile money account? | |
| | Yes | |
| | No | |
| | *If you answered yes for question 30 above, go to 30a otherwise go to question 31.* | |
| | | |

| | | |
|---|---|---|
| | | |
| 30a | How often do you change it? | |
| | Daily | |
| | Twice a week | |
| | Weekly | |
| | Monthly | |
| | Less frequently than monthly | |
| | Never | |
| 31 | Is the subscription (mobile number) you use for performing transactions registered in your name? | |
| | Yes | |
| | No | |
| 32 | Have you or someone you know suffered from a security breach or theft as a result of your mobile device being hacked? | |
| | Yes | |
| | No | |
| 33 | When you lose your SIM card, are you satisfied with the security checks taken by your provider to ensure only the legitimate owner replaces a SIM card ? | |
| | Yes | |
| | No | |
| 34 | Do mobile money banking services sometimes fail to perform well due to network problems? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |
| 35 | Do you believe mobile banking service providers are fair in their conduct of customer transactions? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |
| 36 | Do you believe that mobile network providers are trustworthy? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |
| 37 | Do you believe wireless infrastructure can be trusted? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |

| | | |
|---|---|---|
| | | |
| 38 | Do you believe that mobile banking services may not perform well or may incorrectly process payments? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |
| 39 | When transferring money through mobile banking, do you fear that you will lose money due to careless mistakes such as wrong input of account number or wrong input of amount of money? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |
| 40 | Do you check on the security of the mobile money product you use ? | |
| | Yes | |
| | No | |
| 41 | Do you believe that the mobile money product you use is the most secure on the market? | |
| | Strongly agree | |
| | Agree | |
| | Undecided | |
| | Disagree | |
| | Strongly disagree | |

| | | |
|---|---|---|
| | **Section B (For those who do not use mobile money**) | |
| 42 | What is the primary reason why you do not use mobile money (tick one)? | |
| | I do not know it exists. | |
| | I do not think it is safe/secure to use it. | |
| | The service is not very useful to me, it does not change the way I transact. | |
| | It is difficult to use (i.e learn, enrol into, use and/or access) | |
| | It is expensive to use it i.e. higher tariff charges. | |
| | Other reason (specify below) | |
| | | |
| 43 | If you decided to adopt mobile money, what factors would you consider most when choosing a mobile money provider (tick one)? | |
| | The product should be secure, risk free, trustworthy and reliable | |
| | It must have useful services, be innovative and improve the way I transact | |
| | It must be easy to learn, enrol and use, and should have readily available agent outlets. | |
| | It must be cheap to use | |
| | Other reason(specify below) | |

| | | |
|---|---|---|
| | | |
| 44 | Do you intend to use mobile money in future? | |
| | Yes | |
| | No | |
| | **Section C (All respondents)** | |
| 45 | Are you a bank account holder? | |
| | Yes | |
| | No | |
| 46 | What is your highest level of education? | |
| | No formal education | |
| | Some formal education | |
| | Graduated high school | |
| | Diploma | |
| | Bachelor's degree | |
| | Master's degree or higher | |
| 47 | How would you classify your residential area? | |
| | Rural | |
| | Urban | |
| 48 | Do you have dependents? | |
| | Yes | |
| | No | |
| 49 | What is your gender? | |
| | Male | |
| | Female | |
| 50 | What is your employment status? | |
| | Full-time employed | |
| | Part-time employed | |
| | Self-employed | |
| | Unemployed | |
| | Retired | |
| 51 | What is your age group? | |
| | Under 16 | |
| | 16-25 | |
| | 26-35 | |
| | 36-50 | |
| | Over 50 | |
| 52 | What is your monthly earnings category in US dollar terms? | |
| | Below 500 | |
| | 500-1000 | |
| | 1001- 2000 | |
| | Over 2000 | |

| | | |
|---|---|---|
| | | |
| 53 | How would you describe your ethnic background? | |
| | White | |
| | African | |
| | Asian | |
| | Coloured | |
| | Other (specify below) | |
| | | |

Thank you very much for taking the time to complete this questionnaire.