

UNIVERSITY OF EDUCATION, WINNEBA

**ASSESSMENT OF MOBILE MONEY SECURITY AWARENESS AMONG
MTN MOBILE MONEY USERS IN GHANA**

ALFRED MANNAH

MASTER OF SCIENCE DISSERTATION

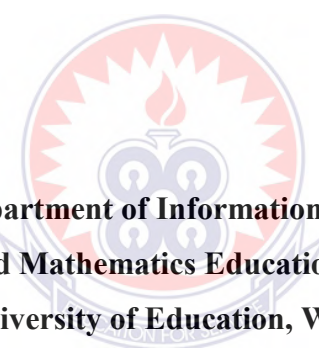


2021

UNIVERSITY OF EDUCATION, WINNEBA

**ASSESSMENT OF MOBILE MONEY SECURITY AWARENESS
AMONG MTN MOBILE MONEY USERS IN GHANA**

ALFRED MANNAH

The logo of the University of Education, Winneba, is a circular emblem. It features a central lamp with a flame, set against a background of a sunburst. The emblem is surrounded by a decorative border.

**A Dissertation in the Department of Information Technology Education, Faculty
of Applied Science and Mathematics Education, submitted to the School of
Graduate Studies, University of Education, Winneba, in partial fulfilment
of the requirements for the award of the degree of
Master of Science
(Information Technology Education)
in the University of Education, Winneba**

MAY, 2021

DECLARATION

STUDENT'S DECLARATION

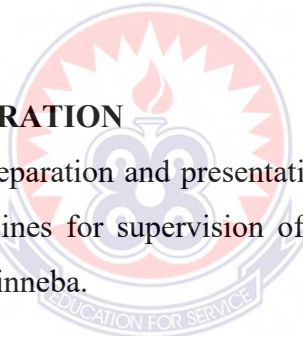
I, ALFRED MANNAH, declare that this thesis, with the exception of quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my own original work, and it has not been submitted, either in part or whole, for another degree elsewhere.

SIGNATURE:

DATE:.....

SUPERVISOR'S DECLARATION

I hereby declare that the preparation and presentation of this work was supervised in accordance with the guidelines for supervision of dissertation as laid down by the University of Education, Winneba.



NAME OF SUPERVISOR: **JOSHUA CALEB DAGADU (PhD.)**

SIGNATURE:

DATE:.....

DEDICATION

This thesis is dedicated to my father, Mr. Gilbert Oppong, my mother, Mrs. Victoria Ebbah, my wife, Rebecca Eduku, and my friend, Jonathan Polley.



ACKNOWLEDGEMENT

My sincere gratitude goes to the Lord for how far He has brought me and for seeing me through the programme successfully. Also, to my supportive supervisor, Dr. Joshua Dagadu I say thank you for your time, valuable suggestions, and constructive criticisms, efforts employed in making this study a successful one. I also express my appreciation to all lecturers and colleagues who have been with me throughout my academics.

Lastly, my appreciation goes to the numerous authors and publishers of the various books from which relevant information was collected to write this thesis.



TABLE OF CONTENTS

DECLARATION	iii
DEDICATION	iv
ACKNOWLEDGEMENT	v
TABLE OF CONTENTS.....	vi
LIST OF TABLES	ix
ABSTRACT.....	x
CHAPTER ONE: INTRODUCTION	1
1.1 Background to the Study.....	1
1.2 Problem Statement	2
1.3 Research Objectives.....	4
1.4 Research Questions.....	4
1.5 Significance of the Study.....	4
1.6 Limitations and Delimitations.....	5
1.7 Organization of the Study	6
CHAPTER TWO: LITERATURE REVIEW.....	7
2.1 Overview.....	7
2.2 Mobile Payments, M-Commerce or E-Commerce	7
2.3 Technology	8
2.4 General Uses of Mobile Money	9
2.4.1 Funds Storage.....	10
2.4.2 Transfer – Domestic and International	10
2.4.3 Payments for Goods and Services.....	11

2.5 Security of Mobile Phones, Mobile Money, M-Payment Services	12
2.5.1 Mobile Money Fraud and Scams	13
2.5.2 M-Payment, E-Commerce and User Perception about Security.....	17
2.5.3 Security dangers to cell phones and mobile money	19
2.6 Empirical Review.....	21
2.6.1 Measure to enhance mobile money security to prevent fraud	21
2.6.2 The link between Mobile Phone Protection and Mobile Money Security.....	23
CHAPTER THREE: METHODOLOGY	26
3.1 Introduction.....	26
3.2 Profile of the Study Area	26
3.3 Research Design.....	26
3.4 Study Population.....	27
3.5 Sample Size and Sampling Technique.....	28
3.6 Data Collection Instrument.....	29
3.7 Pre-Testing.....	29
3.8 Data Collection Technique	29
3.9 Data Analysis Method.....	30
3.10 Ethical Consideration.....	30
CHAPTER FOUR: RESULTS PRESENTATION AND DISCUSSION	31
4.1 Introduction.....	31
4.2 Results.....	31
4.2.1 Demographic characteristics of the respondents.....	31
4.3 Transaction Preference.....	33

4.3.1 Current MTN mobile money security measure	38
4.3.2 Link between mobile device security and MTN mobile money account	
Security	40
4.3.3 View of users about measures that can be put in place to enhance mobile	
money security to prevent fraud	42
4.4 Discussion	43
4.4.1 Demographic Characteristics of the respondents.....	43
4.4.2 Level of preference for MTN Mobile Money as compared to bank	
transactions or other cashless transactions (ATM and e-ZWICH)	44
4.4.3 Measures that respondents have put in place to enhance mobile money	
security to prevent fraud.....	46
4.4.4 Link between mobile device security and MTN mobile money account	
security	48
4.4.5 View of users about measures that can be put in place to enhance mobile	
money security to prevent fraud	50
CHAPTER FIVE: SUMMARY, CONCLUSION, AND	
RECOMMENDATIONS.....	54
5.1 Introduction.....	54
5.2 Summary	54
5.3 Conclusion	55
5.4 Recommendations.....	57
REFERENCES.....	59
APPENDIX.....	65

LIST OF TABLES

TABLE	PAGE
Table 4.1: Age group of respondents	31
Table 4.2: Sex of respondents	32
Table 4.3: Level of education	32
Table 4.4: Occupation	33
Table 4.5: Whether respondents have a bank account	33
Table 4.6: Services operated by the respondents	34
Table 4.7: How long respondents have been using mobile money services.....	34
Table 4.8: Services preferred by the respondents	35
Table 4.9: The services that respondents use for domestic cash transfer	35
Table 4.10: The services that respondents used for international money transfer.....	35
Table 4.11: The service that is easy to use.....	36
Table 4.12: Services that respondents ever used in paying for utilities.....	36
Table 4.13: Whether respondents have ever stopped using the Mobile Money Account	37
Table 4.14: Why respondents stopped using their Mobile Money account.....	37
Table 4.15: Descriptive Statistics on current MTN mobile money security measure	38
Table 4.16: Descriptive Statistics on the link between mobile device security and MTN mobile money account security	40
Table 4.17: Descriptive Statistics on views of respondents.....	42

ABSTRACT

Mobile money is a process by which mobile phone subscribers use telecommunication networks or platforms to perform banking services at any point in time. Mobile money services enable the subscribers to do banking transactions directly from their mobile phones without physically being in the bank to deposit and receive money, pay bills and transact business. The main objective of the study is to assess a holistic approach to Mobile Money security in Ghana. The study was a descriptive exploratory which adopted a quantitative approach and was conducted in Patasi which is a suburb of the Kwadaso Municipality in the Ashanti Region of Ghana. Deliberate convenient sampling was employed by selecting some MTN Mobile Money contact centres in the study area where a sample of 150 respondents was obtained. Data collection was done online using a questionnaire designed in Google form. The link to the questionnaire was sent to respondents via e-mail and on various social media platforms for them to complete it. The study revealed that 98.7% of the people mostly operate MTN mobile money and 98.0% of the respondents preferred MTN mobile money services to ATM and e-ZWICH services. The study also revealed that some of the measures currently put in place to enhance mobile money security include verifying the true identity of the receiver, avoiding sharing of mobile money PINs. Finally, the study revealed that awareness and avoidance of unsolicited messages (scams), checking the authenticity of payment apps before using them, among others can enhance mobile money security. The study, therefore, concludes among others that MTN mobile money service is easy to use and subscribers use the services for both domestic and international money transfers. The study recommends among others that the mobile money service providers, in this case, MTN must set up password expiring time for mobile money subscribers to change their passwords quarterly and authenticate it through answering questions regarding personal identification.

CHAPTER ONE

INTRODUCTION

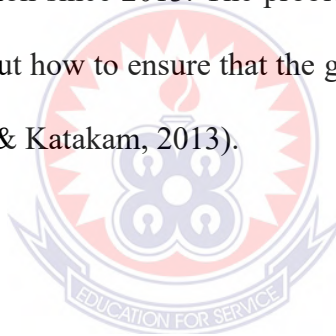
1.1 Background to the Study

Mobile money is a process by which mobile phone subscribers use telecommunication networks or platforms to perform banking services at any point in time. Mobile money services enable the subscribers to do banking transactions directly from their mobile phones without physically being in the bank to receive money, pay bills and transact business all through virtual mobile accounts known as mobile money wallets. The use of mobile money services for transactions has been on a steady growth across Africa and is being positioned as the next service that will revolutionize the economy of Africa dominated by cash. A survey by The Economist webpage (2012) revealed that in 2011, there were about 20 countries globally in which more than 10% of the adult population use mobile money services. Out of these 20 countries, 15 are in Africa and these include Ghana where over 50% of the adult population uses mobile money. From the results of this survey, it was evident that mobile money has become one of the needed financial services for telecom companies across Africa and the world at large. For example, in Ghana, the top-ranked telecommunication companies include Tigo, MTN, and Airtel which all offer their clients mobile money services.

Mobile money services have gradually become part of the day-to-day transactions of people and this is making a transfer of money quite easier and cheaper. In Ghana, people can deposit money into their mobile money wallet and in effect, transfer it to either other mobile money subscribers or those who are not mobile money subscribers. This decreases long-distance travelling time, time spent on queuing in

banks to make a deposit or using methods that are not safe, for example, sending money through bus services for recipients in other towns and villages. –Mobile money transfers can be made by pressing few keys on the mobile phone and recipient receives money almost instantly” (Afanu & Mamattah, 2013, p. 52).

The mobile money industry in Ghana continues to expand and is now in all the regions and even expanding into more rural communities. With over 219 services in about 84 countries at the end of the year 2013, mobile money services are now available in most developing and emerging economies across the globe. While most of the mobile money services remain in Sub-Saharan Africa, it has significantly expanded beyond the region since 2013. The problem is no longer the availability of mobile money services, but how to ensure that the growth of the industry continues to be sustainable (Pénicaud & Katakam, 2013).

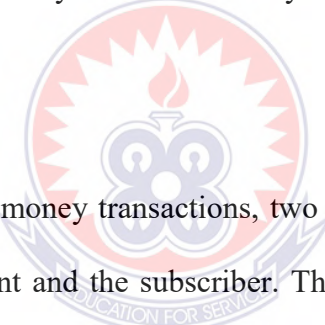


1.2 Problem Statement

With the expanding use of services of mobile money and the new issues arising, it has become very necessary to conduct research into the security practices of the mobile operators and users of the mobile money services to ensure that mobile money services are secured in order to understand the perception of users about the link between mobile phone protection and mobile money security and also to mobile money to prevent fraud. Recently, there has been an increase in fraud cases among some mobile money service providers which led to the loss of money. For example, an online newspaper known as the CIO East Africa (2012) reported a fraud case concerning the mobile money services of MTN Uganda in which the staff of the company stole some millions of dollars from mobile money service users.

Unfortunately, there has been limited research into mobile money fraud in Africa with few undertaken by newspapers, for example, that of the CIO East Africa. Therefore the actual nature and extent of the issues of fraud are yet to be fully classified for the mobile money network operators and users while it is perceived that mobile money service will be more attractive to fraudsters.

It has been predicted that the value of mobile payment transactions worldwide will be worth a market value of about \$617 billion with about 448 million users by 2016 (Gartner, 2012). Based on this estimate, the increase in the use of mobile money services, and the different business-related issues each day, it is prudent to assess a holistic approach to the security of mobile money services that will reduce or prevent fraud.



When it comes to mobile money transactions, two categories of people are involved which include the merchant and the subscriber. The subscriber is the mobile money wallet holder and can use the service without the need for a bank account. All one needs is to obtain an MTN SIM and register it with a valid identity card for a mobile money wallet to be created. The subscriber will need a secret PIN which is a 4-digit number to have access to the mobile money menu on a mobile phone. With the secret PIN, the subscriber can directly deposit money into the mobile money wallet or withdraws money from the wallet (MTN, 2015).

Most of the kinds of literature on mobile money security focuses on fundamental areas such as integrity, availability, confidentiality, authorization, and authentication without clearly linking mobile phone protection and mobile money security.

1.3 Research Objectives

The main objective of the study is to assess a holistic approach to Mobile Money security in Ghana. The specific objectives will include the following:

1. To examine the level of preference for MTN Mobile Money as compared to bank transactions or other cashless transactions (ATM and e-ZWICH).
2. To assess the measures that can be put in place to enhance mobile money security to prevent fraud.
3. To assess how mobile money service subscribers perceive the linkage between mobile phone protection and mobile money security.

1.4 Research Questions

1. What is the level of preference for MTN Mobile Money as compared to bank transactions or other cashless transactions (ATM and e-ZWICH)?
2. What measures can be put in place to enhance mobile money security to prevent fraud?
3. How do mobile money service subscribers perceive the linkage between mobile phone protection and mobile money security?

1.5 Significance of the Study

The use of mobile money as an electronic payment system is increasingly gaining ground in Ghana and most African countries. With MNO reliance on technology (mobile telecommunication and information systems) to deliver the mobile money service comes with some security risks and existing risks inherent in e-payment systems. How these security risks are handled may affect mobile money users' perception of the security of the mobile money service. Also, the mobile money

subscriber's awareness of their responsibility towards the security of the service on their mobile phone could influence some of the actions they take in protecting their mobile money wallet. This research provides some insight into the security controls and practices implemented by the MNO to secure the mobile money service as well as mobile money users' perception about the linkage between mobile money security and the protection of the mobile phone.

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

Many fraud cases regarding loss of Mobile Money in customers' or agents' accounts have been reported to various Mobile Money service providers in the last years. An average of about 365 complaints of fraud monthly from subscribers has been reported to MTN Ghana in the year 2017 (Graphic online, 2017), this figure indicates there is an alarming alert in the security of the Mobile industry. We need to understand the root causes of the fraud to minimize or eliminate this problem in the Mobile Money Market.

1.6 Limitations and Delimitations

There would not be sufficient time to conduct research due to the factor that the researcher is a full-time worker thus hindering him to move out of work to cities to obtain more research details. Also, the research will be conducted on a small size of

the population in the country whereby many mobile money customers and operators are available. Therefore, to generalize the results for larger groups, the study will have to involve more participants in different regions.

Mobile money service encompasses several stakeholders, such as financial institutions, service providers, and trusted third parties (merchants). However, for the purpose of this research, the term mobile money will be limited to a service provided by telecommunication service providers or mobile network operators (MNOs) to their subscribers that enables them to perform mobile money transactions. There are two categories of mobile money users, registered and non-registered. However, this research will focus on only the registered users, who use the service from their mobile phones.

1.7 Organization of the Study

The research has been organized into five chapters:

Chapter One focuses on the background, objectives, research questions, and significance of the study. It also highlights the major problems that the study seeks to address. Chapter Two reviews various literature and other studies that have already been done in the subject area. Chapter Three assesses the methodologies employed to obtain the required data and a profile of the case study organization. Chapter Four presents the results from the data analysis and interpretation of findings. Chapter Five looks at a summary of the findings, conclusion, and recommendations that can be made from the findings that were obtained. It also highlights possible areas that can be used for future research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

This chapter focuses on providing the relevant literature in the scope of this study. It begins with the paradigm shift from the traditional banking system to mobile money services and addresses the importance of deploying e-banking in this 21st century. It also includes the concepts of mobile technology and money, the theoretical backing, and the empirical evidence by other researchers.

2.2 Mobile Payments, M-Commerce or E-Commerce

According to Karnouskos (2004), mobile payment (M-Payment) is any payment where a cell phone is utilised to start, approve and affirm a financial value exchange in return for products and services. Mobile devices which are used for this situation incorporate cell phones, tablets, or whatever other gadgets that can interface with mobile telecommunication networks and empower payment to be made (Herzberg, 2003). Depending on the channels the Mobile Network Operator (MNO) makes accessible for offering this service, a buyer might be restricted to the utilisation of cell phones just or the wide range of various cell phones previously mentioned. M-Payments use what is called e-cash or m-cash to make payments for goods and services.

E-cash has been depicted as a more extensive idea that alludes to payments made utilising the automated teller machines (ATM), near-field communication (NFC) contactless cards, prepaid cards, credit cards, debit cards, just as cell phones. Mobile money is viewed as a subset of e-cash that alludes to monetary services and

exchanges made utilising technologies incorporated into cell phones. These services might be straightforwardly attached to the personal account, prepaid, debit, or credit cards or linked to ATM (IFC, 2011).

The quick development in the utilisation of cell phones and the absence of admittance to formal bank services in most African nations are contributing variables to the fast development and the utilisation of mobile money services in many parts of the continent. More than one billion clients in emerging markets have access to a cell phone however do not have a bank account (GSMA, 2012). Cell phone entrance in Africa gives the required stage to contact the poor and unbanked with financial help.

In Ghana, for instance, mobile-subscriber entrance is just about 80%, yet banking infiltration is 18%. This infers MNOs have an opportunity to fill this hole through creative mobile money services to give financial stages to about 62% of people with cell phones without bank accounts. It is proposed that the utilisation of mobile money in non-industrial nations is to “replace ‘risky’ cash since not all payment alternatives exist”, in this way supporting the attestation that in non-industrial nations, mobile money is here and there the main suitable financial option for an enormous section of the populace (Crowe, 2010).

2.3 Technology

In a study by the World Bank (2012), it was proposed that change in technology in terms of more affordable phones and expanded networks enabled the possibility of mobile money. The most fundamental technology utilised for long-distance transfer of funds is short message service (SMS). The next technology which is easier to

understand is the unstructured supplementary service data (USSD), which gives a few prompts for the transfer of funds. This technology is still being used by some Mobile Network Operators (MNOs), for instance, Tigo (Millicom Ghana) in the service delivery. Another innovative channel utilised for mobile money service is the more advanced SIM Toolkit Application (STK), an application encoded in a Subscriber Identity Module (SIM) Card, a compact memory chip used in some cell phones, which has superior organisation security (IFC, 2011). Some service providers make use of all the innovative channels to convey mobile money services to their subscribers.

The basic technology used to convey the service which is the network and platforms and cell phones have quickly developed its beginning a few years back. Cell phones are quickly spreading over the world at a modest expense, and their improved capacities will transfer mobile money applications past the channels firmly controlled by mobile money operators to the platforms that are more open to rivalry. Despite the pervasiveness of cell phones and the potential for improved transactions, SMS and USSD's usefulness will stay significant for reaching a more extensive base of clients (World Bank, 2012). For quick payment at the point of sales terminals, the NFC, in either cell phones or cards permits the client to pay by just passing the telephone or card over a receiver (IFC, 2011).

2.4 General Uses of Mobile Money

The utilisation of mobile money services is progressively turning out to be essential for the everyday transaction of individuals and is right to state that it is bringing in cash transfer benefits very simpler and at a less expensive expense. In Ghana, for

instance, one can store cash in his/her mobile money wallet and transfer this to either mobile money subscribers or non-mobile money subscribers. This decreases the time spent in long distances travel, queuing at the bank to make a deposit, or using unsafe methods of payments, for example, sending cash through transport services for beneficiaries in different towns. Mobile money transfers can be made by pressing a few keys on the cell phone and the beneficiary gets cash immediately. It very well may be said that most customers like the convenience and usability of the service for transactions and payments from their cell phones; therefore, the market for m-payment is developing quickly (Au & Kauffman, 2007). Mobile money is a promising technology for driving mobile payment and the cashless economy of several African nations, including Ghana.

2.4.1 Funds Storage

Some mobile money services permit their clients to store money either through a bank account held with a bank or an account held with the MNO (Solin & Zerzan, 2010). In Ghana, some mobile money subscribers can transfer cash from their bank account to their wallet and the other way around. This suggests mobile wallets could likewise turn into a mode of holding funds and not just the conventional bank account funds.

2.4.2 Transfer – Domestic and International

Domestic cash transfer refers to money transmitted from one individual to another where the two players are in a similar nation (Solin & Zerzan, 2010). In Ghana, all the mobile money service providers – MTN Ghana, Airtel, and Tigo (Millicom Ghana) offer this cash transfer service to allow individuals to transfer cash to others whenever it might suit them. Mobile money transfers could be completed by either a subscriber

or non-subscriber to either party. A transfer from a subscriber is done by charging their mobile money wallet of money to be transferred to the mobile money beneficiary or creating a token and unique code, which is sent to a non-subscriber to use in withdrawing out the money from a mobile money merchant or the bank. A non-subscriber may complete a mobile money transfer by utilising the services of a vendor or MNOs service centre. In Ghana, recently one can transfer funds across networks; for instance, a client can transfer assets from MTN Ghana mobile money service to Airtel mobile money service referred to as interoperability of MNOs (IFC, 2011), which contending mobile money service providers must perceive as a component of the incentive to customers.

International cash transfer then again is across outskirts normally made out of transfers from migrant workers abroad to their relatives in their nations of origin (Solin & Zerzan, 2010). This service is generally conveyed by a combination of cash transfer services, for example, Western Union and the mobile money service. Global cash transfers utilizing mobile money are not significantly accessible in Ghana; nonetheless, as rivalry extends and new cases of mobile money are created, it is probably going to pull in the consideration of service providers.

2.4.3 Payments for Goods and Services

Mobile payments can be utilised to pay for things bought from shopping centres and vendors. At the point of sales, payment is done by crediting the mobile money accounts of retailers which reflects in a split second. In Ghana, since the transaction can be performed across networks, such payments can be made whether both the dealer and the purchaser are utilising a similar mobile money service or not.

Mobile money service likewise enables clients to pay for fundamental utility services, for example, water, power, which gives more significant convenience and efficiency to customers of these services (Solin & Zerzan, 2010). Utilising mobile money to pay for utilities is one of the services in Ghana that is accessible on the list of services rendered by all the mobile services providers. Utilising mobile money to pay for utilities should be possible in either the offices of the utility organisation, at banks, at the sources of specific payments networks, or at retail shops that have an agency agreement with these service organisations (Amrik & Mas, 2009). By the utilisation of mobile money, purchasers can undoubtedly take care of utility bills and stay away from the burden of traditional payment methods. Mobile money could likewise be utilised for public transport fare payment in some countries across the world (IFC, 2011).

2.5 Security of Mobile Phones, Mobile Money, M-Payment Services

Mobile payment is empowered by an assortment of arising technologies, huge numbers of which are still developing (Eze *et al.*, 2008). These technologies are expected to address different payment industry needs which incorporate authentication infrastructure on cell phones which are secured, validation registries, secure transmission infrastructure for wireless payment, and virtual “wallets” stored on a cell phone or accessible over a network (Taga *et al.*, 2004).

Regardless of all the advancements in technology in mobile phones, security is as yet a significant issue with M-payment. For instance, NFC has been recognised to have the weakness of a man-in-the-middle attack; in which an assailant could intercept data exposed during the correspondence with the reader, which is for the most part inside a

10cm radius (Lee *et al.*, 2013). Essential phones with mobile money ability could be portrayed as Global System for Mobile (GSM) viable telephones with installed services, for example, SMS and USSD (World Bank, 2012). There is nonetheless, no end-to-end security for SMS, insurance ends in the GSM or UMTS (Universal Mobile Telecommunications System) network. Besides, USSD has no different security properties; rather it depends on the GSM/UMTS signaling plane security component (simply like SMS). It is additionally contended that the security systems of message integrity, authentication, proof of receipt and proof of execution, replay detection, and sequence integrity, message confidentiality, and an indication of security mechanisms exist; notwithstanding, it relies upon the applications whether these security instruments are actualised and whether their cryptographic quality is adequate (Schwidorski-Grosche & Knospe, 2002).

2.5.1 Mobile Money Fraud and Scams

Fraud with regards to mobile money can be supposed to be the purposeful and intentional activities attempted by players in the mobile financial services system, pointed toward inferring financial profits, denying different players income, or harming the reputations of different partners. The occurrence and prevalence of fraud are reliant on the implementation stage of the mobile money service. Subsequently, as deployment develops, the kinds of fraud advance with it (Mudiri, 2012; Gilman and Joyce, 2012).

Key empowering agents of mobile money fraud incorporate development of the mobile money services, powerless or non-standard process, social issues, absence of compliance monitoring (Mudiri, 2012), and any new worth-added services not thoroughly considered appropriately, for instance, the post-paid plan wherein the

transaction is applied to the telephone bill of the customer to be paid later (Merritt, 2010).

According to Mudiri (2012), fraud regarding mobile money can be arranged into ~~merchant~~ merchant or agent-driven fraud, customer-driven fraud, system administration fraud, business partner related fraud and MNO fraud” as clarified beneath:

- Consumer-driven frauds are frauds committed by consumers either on other consumers, vendors, or service providers. Extortion, phishing SMS, unapproved utilisation of PIN, unapproved renouncement of funds, impersonation of business, and counterfeit money are instances of this sort of fraud. This fraud is more pervasive during the initiation of transactions of the business when customers start to believe the MNO offering the services but are yet to completely understand the potential dangers related to the service. Client mindfulness is one of the vital ways of tending to this kind of fraud.
- Agent or Merchant driven fraud is the fraud caused by the merchant or the employees and appears as an agent or a merchant duping another merchant, the merchant duping sub-merchants, or the merchant swindling the MNO service provider. This kind of fraud is pervasive toward the start of deployment, promoted by early product pricing loopholes.
- Business partner-related fraud is fraud committed by business partners on consumers, customers on merchants, and business partners. This is predominant during the worth expansion phase of the organisation. This kind of fraud is still in its growing stage as business transaction adoption is still in its incipient stages.

- System administration fraud is a sort of fraud that covers all fraud exercises influencing the mobile money services through system or process shortcomings and cut across various partners in the mobile money environment. The system-related fraud is at its peak when the platform has deficient controls to guide in the processing of transactions and is common during the stage of deployment of transaction activation and keeps on developing into the stage of value addition. Instances of system-related frauds include weak PIN, Password, or PIN sharing, lack of duties segregation, and weak mobile money platforms that could be hacked. The moderation controls for this fraud incorporate standardization and process controls.
- MNO Fraud is a kind of fraud that is generally perpetuated by the workers of the service provider. The casualties of this kind of fraud incorporate the service provider, agent, merchant, or client. Instances of this fraud incorporate the service provider taking the electronic money of customers, unapproved transfer of funds from the account of clients, and collusion between deceitful mobile money workers and different fraudsters to do unapproved swapping of SIM and transaction from the mobile money wallets of clients. Numerous occurrences of this sort of fraud have been accounted for in the news media.

Fraud circumstances for mobile network operators (MNOs) can be high; yet as a result of MNO's non-disclosure, the degree of fraud with mobile money is obscure. Brand damage, low adoption of mobile money services because of trust issues, loss of clients, and loss of income are a few instances of the effect of fraud on mobile money service providers. As mobile money frauds have desperate outcomes, MNOs that have mobile money services have conceded to a typical system for dealing with the danger of mobile money fraud.

According to Gilman and Joyce (2012), this system comprises of the accompanying four components: decide mobile money risk appetite, recognise and evaluate the sources of mobile money fraud, build up compelling controls and monitor its adequacy of controls.

- Determine mobile money risk appetite: to effectively organize and control the danger of mobile money fraud MNOs must comprehend their risk craving or the costs they are to convey comfortably in a mobile money transaction. Risk appetite is communicated in either qualitative or quantitative scales (Gilman & Joyce, 2012). Without a statement of formal risk appetite, the MNOs will have control issues (HM Treasury, 2006).
- Identify and survey sources of mobile money fraud: after setting up the risk appetite, the MNO must attempt to comprehend the possible sources of the mobile money fraud that may emerge. When distinguished, these sources must be contrasted with the setup risk appetite, and any fraud risk that falls outside the risk appetite must be additionally researched. Controls ought to be actualized to oversee or lessen these fraud chances until they are at an adequate level (Gilman & Joyce, 2012).
- Establish powerful controls: as the different likely sources of fraud are recognized, the MNOs must utilise strategies to alleviate them. Controls can be either preventive (decrease the probability of fraudulent activities) or detective (monitor system access activities or give SMS alerts to clients). The controls set up must not be effortlessly evaded, must be appropriately reported, checked on, and tested to guarantee its adequacy.
- Monitor and review mobile money risk management technique adequacy: checking the controls set up and surveying the mobile money chances over the

long-term is essential to keep up a powerful risk relief system in mobile money fraud. All the more significantly, as the client base develops and deployment advances with more items added, the controls must be evaluated to guarantee ongoing viability.

2.5.2 M-Payment, E-Commerce and User Perception about Security

Numerous researches on security in the field of information systems centre essentially around technical and usage-related issues. However, most customers just see security from the abstract domain (Taga *et al.* 2004), which is typically brooded through promotions and public information (Karnouskos, 2004). Security and trust are among the vital contemplations for the appropriation of M-Payment systems. For instance, a study by Mallat (2007) into the adoption of mobile payment has indicated that the absence of perceived security is one purpose behind restraint to the reception of the solution. Tending this inhibitor to the appropriation of mobile payment solutions or any electronic payment systems implies security must be broadly addressed.

The idea of security has been put into two measurements by researchers, and these are objective and subjective security. Objective security is an application or platform security dependent on solid technical qualities (Kreyer, *et al.*, 2002). These security attributes are mostly the worries of security experts, owners of the system, and backend IT staff. It has been contended that only one out of every three clients can appreciate or assess the technicalities of objective security (Egger & Abrazhevich, 2001). Conversely, subjective security, or the perceived sensation of the security of the procedures from the viewpoint of the customer or consumer, is contended to be a more applicable measure to check how mobile payment security influences consumer adoption.

Embracing a security approach that tends to address the dimensions of security, that is objective (security with technical attributes) and subjective security (generally procedural and from the client perspective) is basic for organisations making the most of business opportunities while building certainty for the security of their services. Security necessities of integrity, confidentiality, authorization, authentication, and non-repudiation are basic to the fulfilment of both subjective and objective security of mobile payments (Egger & Abrazhevich 2001).

Objective and subjective security are neither independent nor disjoint. However, it tends to have contended that subjective security can affect objective security since the security discernments and activities of customers can affect objective security. In a study on subjective security of m-payment among 4,998 respondents, privacy was found to be the main goal of clients (Linck *et al.*, 2006).

Subjective security can have an impact on objective security, for example, the cell phone used for the mobile money service. In research to distinguish cell phone clients' data security practices in Ghana (Seakomo, 2012), the following were found as the factors affecting the manners in which cell phone clients ensure their telephones:

- Longevity of cell phone use affects cell phone protection: a longer period of cell phone use has a positive effect on the security practices of the cell phone use and therefore, the data security dangers that the cell phone user faces. Also, the security practices of clients do improve over the long run since the degree of knowledge and awareness on security techniques increase over the long-term, in this way diminishing the probability of mistakes by users.

- Awareness level and prevailing practice culture: the finding additionally recommends that imperfect prevailing practice culture have a negative effect on security practices and can prompt increase security dangers and events of such dangers. However, the good prevailing culture and high levels of knowledge emphatically influence the security practices of a cell phone user.
- Self-obligation, decisions, and principles: the obligations of cell phone users to themselves, their individual qualities or principles, and their own choices affect their security practices in their cell phones protection.
- Handling and environment of use: the logical or physical in which the cell phones are utilised affect security practices that are adopted by the users. For instance, in an unfriendly environment, users can be more cautious with the security of their cell phones than in a safe environment.
- Worth of mobile phone and substance stored information: the more costly the cell phone is, the more it will be kept well to forestall loss and prevent others from accessing it. This has an aberrant effect on parts of the security practices of the cell phone user. For instance, the individuals who utilise more affordable cell phones notwithstanding the substance of information on it do not care about how they handle these phones as compared with the individuals who use more costly cell phones.

2.5.3 Security dangers to cell phones and mobile money

Loss of cell phones, improper disposal, theft, malware, and unauthorized access are distinguished as some of the components influencing the security of cell phones. Cell phones are essentially small in size and the chance of them being lost or taken is high, subsequently, it turns into an obvious objective for theft. Appropriate measures,

subsequently, must be set up to confine unauthorized access to cell phone information to forestall sensitive information exposure that might be saved on them or available from them in case of theft (NIST SP800-124, 2008).

An overview of taxi organisations in Sweden, Great Britain, Australia, Denmark, France, Germany, Norway, Finland, and the U.S. uncovered that a huge number of advanced gadgets (counting cell phones) were erroneously abandoned (Checkpoint, 2005). Notwithstanding the trade-off of consistent and actual information, a cell phone with dynamic help, for example, mobile money service could be gotten to without approval, prompting robbery of cash from mobile money wallets. Moreover, the cell phone itself could have huge financial esteem and can be re-established to its unique settings physically and reused effectively, regardless of whether the substance of the client put away on the telephone are cleaned away (NIST SP800-124, 2008).

Available user authentication systems on cell phones are PINs, passwords, and patterns. While these methods of verification systems are not fool-proof, they are the principal line of safeguard to forestall unapproved access to cell phones. Be that as it may, cell phones and their substance access can be obtained up by guessing or forging the credentials of authentication or completely bypassing the system of authentication (NIST SP800-124, 2008). Strangely, most cell phone clients scarcely use security systems incorporated with the cell phone, and regardless of whether they do, frequently they use settings that could be guessed without much difficulty, for example, using 0000 or 1234 as a PIN or password (Knijff van der, 2002).

Shortcomings in the methods of authentication are another way that fraudsters can take advantage of. This is because a few devices have a master password that is built with the authentication component, which permits access without limit when entered, including bypassing the security lock set by the user (Knijff van der, 2002; NIST SP800-124, 2008). A portion of the mechanisms used to acquire master password is: calculating it straightforwardly from the equipment identifier (Jansen & Ayers, 2007), the utilisation of secondary passage to bypass all or part of the control system (Withers, 2008), moreover forensic tools likewise exist that could be used to bypass security components built-in to recoup the substance saved on the cell phone (Ayers R. *et al.*, 2007; Breeuwsma M *et al.*, 2007 and Troy 2008).

Malware is another danger to the security of cell phones. Communications networks are once in a while used to convey infections and different types of malware to cell phones. Malware can spread in an assortment of ways, for example, linked to received SMS, web downloads, and Bluetooth messages. Malware can eavesdrop on the input of users and take delicate data stored on the cell phone and can likewise be utilised to permit an assailant to obtain free access (NIST SP800-124, 2008).

2.6 Empirical Review

Researchers have carried out several studies which have discoveries significant for this study. Some of these are discussed in this section.

2.6.1 Measure to enhance mobile money security to prevent fraud

The principal safeguard is to use danger scenarios to recognize and manage possible dangers. Mobile wallet applications produced for mobile money services must be analysed completely to identify threat scenarios, for example, spoofing, repudiation, tampering, and data disclosure. Ensuring sensitive data saved on the cell phone, for

example, account numbers or validation information (PINs or passwords), is an essential consideration (Hoseph & Anpalagan, 2007). Sensitive information must be encrypted when being sent or saved on the cell phone. Isolated techniques that are available ought to likewise be applied to guarantee that trusted applications and substances are safeguarded from different applications on the device (NIST SP800-124, 2008).

Moreover, exposure to delicate information could be decreased by not saving sensitive data, for example, personal and financial data on a cell phone. Valuable information ought to rather be kept on removable memory cards and saved independently from the device (NIST SP800-124, 2008). Maintaining control of a cell phone which utilises mobile money is another significant shield. It must be handled carefully, much the same as a credit card, keeping up control consistently and saving it safely when left unattended. Notwithstanding cell phone cost, the theft or loss of it might put private data saved on the telephone in danger of robbery (NIST SP800-124, 2008).

Detective and preventive instruments can likewise be used as a shield to safeguard against malware and different types of attack. Wide scopes of these components, which can expand the security of the cell phone are now present in most cell phones (NIST SP800-124, 2008). It should, in any case, be seen that add-on security software projects may contain or present shortcomings and ought to be appropriately assessed before use (Fogie, 2006). A portion of the accessible preventive components that could be employed are:

- Registration of Device
- Installation of customer software, control settings, and policy rules

- Controls over secret key length and number of entry attempts
- Remote erasure or locking of the cell phones
- Firewall installation, antivirus, interruption identification, and anti-spam
- Reporting compliance status of the device

2.6.2 The link between Mobile Phone Protection and Mobile Money Security

A study among 2,980 family units in Tanzania uncovered that the overall perception about mobile money utilisation by registered clients both in the rural and urban areas is that the service is for sending or getting cash. Strangely, 55% of nonusers likewise think the service is for sending or accepting cash as it were. Despite the general acceptance that mobile money is used for transfer and getting cash, it is the second most popular method for investment funds in Tanzania and Kenya (Jack & Suri, 2011). Aside from utilising mobile money for payment purposes, in Tanzania, 14% of the 2,980 families studied use it for non-payment purposes, for example, tax, school fees, salaries, and utility bills. This is followed by 12% of clients who utilise the platform to buy goods and services (InterMedia, 2013). The overall employments of mobile money in the middle to high-income nations, for example, the USA, Sri Lanka, Brazil, and Thailand are for transport fare payment. Mobile money transfers are viewed as the least used (IFC, 2011).

Another survey in Kenya (Merritt, 2010) uncovered that to do mobile money deposit (cash in) or transfer money through a specialist, the client must give a type of an ID, as a method of “know-your-client” (KYC). In another study in Kenya by Jack and Suri (2011), it was reasoned that mobile money clients are bound to be literate more than non-clients. This was likewise affirmed in another survey led in Tanzania, which

uncovered that the more learned people are, the almost certain they are to use mobile money.

Out of the 2,980 families studied, 65% of them had primary education, 22% of them had secondary education while 14% of them had no formal schooling (InterMedia, 2013). The survey in Tanzania uncovered that 33% of family units shared their mobile money PIN (secret word) with different people, 33% said they share their PIN “consistently”, and another quarter revealed sharing their PIN “frequently.” Of the individuals who shared their PINs, 55% shared with mobile money agents while 45% shared it to close relations, for example, life partner, kin, and spouse. Besides, 78% of the individuals who shared their PINs likewise said they do not have any idea how to change their PIN (InterMedia, 2012). They further uncovered that 14% of mobile money clients may have done m-cash exchanges with the assistance of the agent and might have shared their PINs with the agent (InterMedia, 2012).

In Kenya, Githui (2011) presumed that even though mobile money operators had organisation and industry standards that guide them, they have not been implemented and completely embraced, prompting the chance of technological sharp individuals utilising their skills to accomplish their unlawful targets of fraud and trick. For instance, a mean of 18% of respondents in the 2,980 family units in Tanzania has had cash taken from their m-cash account because of fraud or a trick (InterMedia, 2013).

A study on security and privacy concerns related to mobile money in Africa uncovered that mobile money clients have a significant task to carry out in securing their mobile money. The absence of legitimate consideration regarding essential

security details on the cell phones customers makes them vulnerable to various dangers, the most harmful of which is the loss of cash if an assailant gets the cell phone. Moreover, security is a two-sided part between both client and the service provider since it is conceivable technically adept enemy might have the option to exploit weak security plans inside mobile money applications or bypass ineffectively executed encryption (Harris *et al.*, 2013). Hence the two clients and financial organisations must think about a scope of danger model activities to make the service secured.

Another survey in Africa to find out security issues of mobile money clients uncovered that if legitimate consideration regarding the security of the cell phone is not taken, the client might be vulnerable to crime (Harris *et al.*, 2013). This was additionally certified in an investigation of 2,000 Tanzanian adults which likewise uncovered that both nonusers and users of mobile money services keep on communicating worries about the security of mobile money, with the end goal that they fear losing cash from their mobile wallet if their cell phone is lost or taken (InterMedia, 2012).

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter discusses the methodology used for this study. It highlights the research design, the sources of data, the population and sampling method used, as well as the data collection instrument and data analysis technique used. It also gives a profile of the case study organization.

3.2 Profile of the Study Area

The study was conducted in Patasi, a residential area and a suburb in the Kwadaso Municipality. The area was chosen due to its proximity to the researcher. Kwadaso Municipal Assembly is located in the Ashanti Region of Ghana. It was part of the newly created Assemblies out of then Kumasi Metropolitan Assembly in 2018. The Municipality was established by the LI 2292 of 2017, inaugurated on March 15, 2018, with Kwadaso as its administrative capital. The Municipality has a projected population of about 251,215 (2018) with a growth rate of 2.3 percent. The males constitute 139,304 of the total population, while females are 111,911 (Ministry of Finance, 2019).

3.3 Research Design

Research design serves as the architectural blueprint of research work, linking design, data collection, and analysis activities to the research questions and ensuring that the complete research agenda is addressed.

Considering the research questions of finding out what measures can be put in place to enhance mobile money security and to get the perception of mobile money subscribers on what they think is the linkage between the protection of the mobile phone and the mobile money security, the research was designed to be both exploratory and descriptive which adopted a quantitative approach. The research was exploratory in that the study sought to find ways the mobile money service can be better secured to prevent fraud. This goal was accomplished by investigating what measures are implemented at the case study company and the general measures that have been revealed in the literature review about mobile money security. This research was also descriptive because the researcher collected data and analysed the data to understand and describe what mobile money users think is the linkage between mobile phone protection and mobile money security.

For better interpretation and presentation of findings, a quantitative research approach was employed in this research. This process was employed in the following ways: a questionnaire with closed-ended questions was used to collate information from mobile money users on their perception about mobile phone protection and mobile money security. This was analyzed to draw inferences about their opinions on these linkages.

3.4 Study Population

The study population is the group of persons with similar characteristics from which a sample is drawn for the study. According to Mugenda and Mugenda (1999), a population is well-defined as a set of people, services, elements, and events, groups of things, or households that are being explored.

For the purpose of this study, the study population comprised the subscribers of MTN mobile money services in Kwadaso in the Ashanti Region.

3.5 Sample Size and Sampling Technique

Since a researcher cannot study all people and all locations relevant to the problem under study, one of the greatest “inventions” for social research is sampling. Sampling allows the researcher to study only a subset of the units of interest and then generalize to all these units.

The sample size for the study was calculated using the relation by Krejcie and Daryle (1970) for a finite population which is given by: Sample size (s) = $X^2 NP(1 - P) \div d^2 (N - 1) + X^2 P(1 - P)$, where N is the study population. The study population was considered to be the estimated daily users of MTN Mobile Money in the study area. According to the Ministry of Finance (2019), there is an estimated number of 400 subscribers who use MTN Mobile Money services daily in the study area. ‘n’ is the desired sample for the study, X^2 is the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841), P is the population proportion which is assumed to be 0.5 (since it will provide the maximum sample size) and d is the degree of accuracy expressed as a proportion (0.05).

Therefore, $s = \frac{3.841 \times 400 \times 0.5(1-0.5)}{0.0025(400-1) + 3.841 \times 0.5(1-0.5)} = 198$. A sample of 150 respondents was

obtained when the questionnaire was sent online.

A total of 150 subscribers were selected for the study. Deliberate convenient sampling was employed by selecting some contact centres from the Kumasi Metropolis where subscribers do Mobile money transactions.

3.6 Data Collection Instrument

The main instrument for the study was the questionnaire which was developed by the researchers and used to collect data for the purpose of this study. The questionnaire is one of the research tools that are simple and effective (Kothari, 2014). The questionnaire comprised close-ended questions that allowed respondents to make choices. It is advised that a good questionnaire requires more than writing questions. The questionnaire was developed online using Google forms.

3.7 Pre-Testing

After designing the questionnaire, the researcher printed hard copies and tested them using ten (10) Mobile Money subscribers in Tanoso in the Kumasi Metropolis. This was to ensure the validity and reliability of the questionnaire. The challenges that were associated with the understanding of respondents regarding the questions were revealed through the pre-testing revealed. It was also through the pre-testing that, corrections were made in the questionnaire and ensured that it still achieved the study objectives.

3.8 Data Collection Technique

The respondents were provided with closed and opened-ended questions that will require them to tick the most appropriate choice. The questionnaire was designed in Google form and sent to the respondents through e-mail and social media platforms for them to be completed.

3.9 Data Analysis Method

Data analysis is working with the data, organizing it, breaking the data into manageable units, synthesizing it, searching for patterns, discovering what is important, what is to be learnt, and deciding what the researcher wants to tell others (Bogdan & Biklen, 1982). It can be deduced from this that meaning must be made from the research data collected to draw inferences to answer the research questions and achieve the required purpose of the research in general.

Frequency and descriptive statistics were used to analyse the generated data. Data from the field was cleaned, coded, grouped according to study variables, and then entered into the Statistical Package for Social Sciences (SPSS) version 16. The data was then transferred into Microsoft Excel for analysis. Descriptive frequency tables and charts were then used to represent the analysed data.

3.10 Ethical Consideration

The study was conducted in conformity to ethical codes in social science research. The ethical considerations include ensuring voluntary participation, anonymity, and confidentiality of the respondents. The purpose of the research was explained to all respondents and respondents were interviewed based on their informed consent and voluntary participation. Respondents were also assured of their anonymity and the confidentiality of their responses. The study also adhered to other codes of ethics regarding data collection and information retrieval, as well as attributing secondary data to valid sources.

CHAPTER FOUR

RESULTS PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents the results of the data collected from the field for the study and the discussion of the results. The presentations are according to the study objectives.

4.2 Results

This section presents the result from the data collected from the field using the research instrument. The results of the data are presented in frequency tables and descriptive statistics.

4.2.1 Demographic characteristics of the respondents

This sub-section presents the demographic characteristics of the respondents. These include the age group, sex, level of education, and occupation of the respondents.

Table 4.1: Age group of respondents

Age group	Frequency	Percentage (%)
less than 18 years	6	4.0
18-25 years	27	18.0
26-30 years	20	13.3
31-35 years	42	28.0
36-40 years	30	20.0
40-45 years	14	9.3
46-50 years	9	6.0
above 50 years	2	1.4
Total	150	100.0

Source: Field survey, 2021

Out of the 150 respondents, 4.0% was less than 18 years old, 18.0% was aged 18-25 years, 13.3% was aged 26-30 years, 28.0% was aged 31-35 years, 20.0% was aged 36-40 years, 9.3% was aged 40-45 years, 6.0% was aged 46-50 years and 1.3% was aged above 50 years.

Table 4.2: Sex of respondents

Sex	Frequency	Percentage (%)
Male	94	62.7
Female	56	37.3
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 62.7% were males and 37.3% were females.

Table 4.3: Level of education

Level of education	Frequency	Percentage (%)
Basic	3	2.0
Second cycle	65	43.3
Tertiary	82	54.7
Total	150	100.0

Source: Field survey, 2021

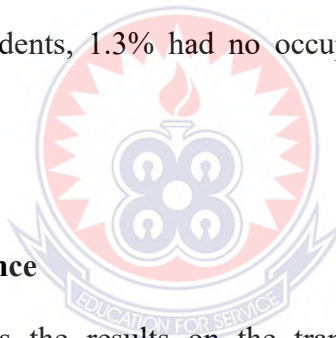
Out of the 150 respondents, 2.0% had attained basic education, 43.3% had attained secondary education and 54.7% had attained tertiary education.

Table 4.4: Occupation

Occupation	Frequency	%
Civil servant	54	36.0
Trading	27	18.0
Farmer	6	4.0
Artisan	13	8.7
Student	40	26.7
None	2	1.3
Others	8	5.3
Total	150	100.0

Source: Field survey, 2021

Of the occupation of the 150 respondents, 54 out of 150 representing 36% of the respondent were civil servants, 18.0% were traders, 4.0% were farmers, 8.7% were artisans, 26.7% were students, 1.3% had no occupation and 5.3% were into other occupations.



4.3 Transaction Preference

This sub-section presents the results on the transaction preference of the study participants. The researcher was interested in finding out how the respondents prefer MTN mobile money transactions to other transactions.

Table 4.5: Whether respondents have a bank account

Response	Frequency	Percentage (%)
Yes	117	78.0
No	33	22.0
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 78.0% had bank accounts and 22.0% had no bank account.

Table 4.6: Services operated by the respondents

Services	Frequency	Percentage (%)
MTN Mobile money	148	98.7
None	1	.7
Others	1	.7
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 98.7% indicated that they operate MTN mobile money account, 0.7% of them operated neither MTN mobile money nor ATM and e-ZWICH and 0.7% also operated other services.

Table 4.7: How long respondents have been using mobile money services

Years of use	Frequency	Percentage (%)
less than 2 years	10	6.7
2-5 years	55	36.7
more than 5 years	85	56.7
Total	150	100.0

Source: Field survey, 2021

Out of the 150 respondents, 6.7% had operated MTN mobile money for less than 2 years, 36.7% had operated it for 2 to 5 years and 56.7% had operated it for more than 5 years.

Table 4.8: Services preferred by the respondents

Services	Frequency	Percentage (%)
MTN mobile money	147	98.0
ATM and e-ZWICH	1	.7
None	2	1.3
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 98.0% preferred MTN mobile money, 0.7% preferred ATM and E-ZWICH, and 1.3% preferred none of them.

Table 4.9: The services that respondents use for domestic cash transfer

Services	Frequency	Percentage (%)
MTN mobile money	134	89.3
ATM and e-ZWICH	15	10.0
Others	1	.7
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 89.3% use MTN mobile money, 10.0% use ATM and E-ZWICH, and 0.7% other services for domestic cash transfer.

Table 4.10: The services that respondents used for international money transfer

Services	Frequency	Percentage (%)
MTN mobile money	54	36.0
ATM and e-ZWICH	8	5.3
None	55	36.7
Others	33	22.0
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 36.0% use MTN mobile money, 5.3% use ATM and E-ZWICH, and 36.7% use no one of the above services, and 22.0% of them use other services for international cash transfer.

Table 4.11: The service that is easy to use

Services	Frequency	Percentage (%)
MTN mobile money	147	98.0
ATM and e-ZWICH	2	1.3
None	1	.7
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 98.0% said MTN mobile money is easy to use, 1.3% said ATM and E-ZWICH are easy to use and 0.7% none of the services is easy to use.

Table 4.12: Services that respondents ever used in paying for utilities

Services	Frequency	Percentage (%)
MTN mobile money	108	72.0
ATM and E-ZWICH	6	4.0
none	36	24.0
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 72.0% said they had ever used MTN mobile money, 4.0% said they have ever used ATM and E-ZWICH and 24.0% said they have never used any of the above services in paying for utilities.

Table 4.13: Whether respondents have ever stopped using the Mobile Money Account

Response	Frequency	Percentage (%)
Yes	85	56.7
No	65	43.3
Total	150	100.0

Source: Field survey, 2021

Of the 150 respondents, 56.7% was they have ever stopped using their mobile money accounts and 43.3% of them said they have never stopped using their mobile money accounts.

Table 4.14: Why respondents stopped using their Mobile Money account

Reasons for stopping	Frequency	Percentage (%)
My account was blocked	9	10.6
Because of fraudsters	12	14.1
Difficult to locate an agent	58	68.2
My phone was missing	5	5.9
Others	2	2.4
Total	85	100

Source: Field survey, 2021

Of those who indicated that they have ever stopped using their mobile money account, 10.6% said their accounts were blocked, 14.1% said because of a fraudster, 68.2% said it was due to difficulties in locating mobile money agents, 5.9% of them said their mobile phones were missing and 2.4% of them said it was due to other reasons.

4.3.1 Current MTN mobile money security measure

This section presents the current security measures that the respondents employ in preventing Mobile money fraud.

Table 4.15: Descriptive Statistics on current MTN mobile money security measure

Statement	N	Min	Max	Mean	Std. Deviation
Suspicious transaction suspended until confirmation	150	1.00	5.00	4.5267	1.04076
The true identity of the sender and the receiver is verified before a transaction is processed.	150	1.00	5.00	4.6800	.89981
Unsolicited calls from anonymous callers concerning MTN mobile money are avoided.	150	1.00	5.00	4.6600	.95419
I do not share my Mobile Money PIN with close friends and families.	150	1.00	5.00	4.6067	.97552
The phone is not given to a friend and a family member to transact in my absence.	150	1.00	5.00	4.5400	1.09072
Transaction details are not exposed to third parties.	150	1.00	5.00	4.6467	.89845
Suspicious MTN mobile money fraudulent activities are reported to MTN customer care.	150	1.00	5.00	4.6667	.90980
I do not do transactions at suspected agent points. For example, agents who are situated in secret corners.	150	1.00	5.00	4.6333	1.00613
The use of strong PINs instead of weak PINs such as date of birth.	150	1.00	5.00	4.5467	1.01391
I ensure every mobile money transaction I do is safe and secured. That is, I do not transact with people I know.	150	1.00	5.00	4.6000	1.01002
Valid N (listwise)	150				

Source: Field survey, 2021

The majority of the respondents agreed that suspicious transactions should be suspended until confirmation (mean = 4.5267). Also, the majority of them agreed that the true identity of the sender and the receiver is verified before a transaction is processed (mean = 4.6800). Again, the majority of the respondents agreed that unsolicited calls from anonymous callers concerning MTN mobile money are avoided (mean = 4.6600). Furthermore, the majority of the respondents agreed that they do not share my Mobile Money PIN with close friends and families (4.6067). The majority of the respondents also agreed that their phones are not given to friends and family members to transact in my absence (mean = 4.5400). The respondents also agreed that transaction details are not exposed to third parties (mean = 4.6467). The majority of the respondents again agreed that suspicious MTN mobile money fraudulent activities are reported to MTN customer care (mean = 4.6667). The majority of the respondents agreed that they do not do transactions at suspected agent points. For example, agents who are situated in secret corners (mean = 4.6333). The majority of the respondents further agreed that they use strong PINs instead of weak PINs such as date of birth (mean = 4.5467). Lastly, the majority of the respondents agreed that they ensure every mobile money transaction they do is safe and secured. That is, they do not transact with people they know (mean = 4.6000).

4.3.2 Link between mobile device security and MTN mobile money account

Security

This section presents the views of the respondents on the link between the mobile device and the money account security.

Table 4.16: Descriptive Statistics on the link between mobile device security and MTN mobile money account security

Statement	N	Min	Max	Mean	Std. Deviation
Mobile phones should be registered and linked to mobile money accounts so that mobile money transactions cannot be done on different phones.	150	1.00	5.00	3.1267	1.55134
The use of special software on phones to track suspicious users of mobile money accounts.	150	1.00	5.00	4.5933	.99054
Software to check wrong mobile money PINs entry attempts.	150	1.00	5.00	4.5467	1.04648
Use a lock for your mobile device-a PIN/password or an app with a lock/unlock feature that you can use to block your phone remotely in case it gets stolen or lost.	150	1.00	5.00	4.6000	.93407
The use of a special feature, for example, figure print to access MTN mobile money account to avoid unauthorized users.	150	1.00	5.00	4.5667	.97909
Money on mobile money wallet can be lost if the mobile phone gets lost.	150	1.00	5.00	4.3333	1.25675
Third parties can access mobile money when passwords or PINs are disclosed to them.	150	1.00	5.00	4.5533	1.02018
The use of mobile payment apps that issue an immediate electronic receipt to help track mobile money transactions and evidence of payments.	150	1.00	5.00	4.6333	.94419
Make sure that mobile apps used for payments and banking are safe and legit.	150	1.00	5.00	4.6067	.91150
There is the possibility of retrieving your mobile money account if your mobile phone and the SIM card get missing since they have both been linked together.	150	1.00	5.00	3.9400	1.41530
Valid N (listwise)	150				

Source: Field survey, 2021

Most of the respondents agreed that mobile phones should be registered and linked to mobile money accounts so that mobile money transactions cannot be done on different phones (mean = 3.1267). Also, the majority of them agreed that the use of special software on phones to track suspicious users of mobile money accounts will ensure mobile money account security (mean = 4.5933). Again, the majority of the respondents agreed to software to check wrong mobile money PINs entry attempts will ensure mobile money account security (mean = 4.5467). Furthermore, the majority of the respondents agreed that the use of a lock for your mobile device-a PIN/password or an app with a lock/unlock feature that you can use to block your phone remotely in case it gets stolen or lost will ensure mobile account security (4.6067). The majority of the respondents also agreed that the use of a special feature, for example, figure print to access MTN mobile money account to avoid unauthorized users (mean = 4.5667). The majority of the respondents also agreed that money on mobile money wallet can be lost if the mobile phone gets lost (mean = 4.3333). The majority of the respondents again agreed that third parties can access mobile money when passwords or PINs are disclosed to them (mean = 4.5533). The majority of the respondents agreed that use of mobile payment apps that issue an immediate electronic receipt to help track mobile money transactions and evidence of payments (mean = 4.6333). The majority of the respondents further agreed that making sure that mobile apps used for payments and banking are safe and legit will secure mobile money account (mean = 4.6067). Finally, most of the respondents agreed that there is the possibility of retrieving your mobile money account if your mobile phone and the SIM card get missing since they have both been linked together (mean = 3.9400).

4.3.3 View of users about measures that can be put in place to enhance mobile money security to prevent fraud

this section also presents the views of the respondents on the measures that stakeholders can put in place to prevent MTN Mobile money frauds.

Table 4.17: Descriptive Statistics on views of respondents

Statement	N	Min	Max	Mean	Std. Deviation
Awareness and avoidance of unsolicited messages (scams).	150	1.00	5.00	4.6867	.94930
Check the authenticity of payment apps before using them.	150	1.00	5.00	4.6933	.89702
Effective use of valid identification cards for all cash-out transactions.	150	1.00	5.00	4.4600	1.24583
Do not trust anonymous calls when money is involved.	150	1.00	5.00	4.6467	.97717
Reporting of fraudulent activity to MTN mobile money service operator.	150	1.00	5.00	4.6800	.92917
The national communication authority must implement strict rules to monitor network operators on fraud issues.	150	1.00	5.00	4.6600	.94001
Network operators should identify and assess sources of mobile money fraud.	150	1.00	5.00	4.6733	.93044
Strict measures should be taken against suspected fraud issues.	150	1.00	5.00	4.6667	.97393
The network operators should suspend accounts of suspected frauds.	150	1.00	5.00	4.6400	.97815
Valid N (listwise)	150				

Source: Field survey, 2021

The majority of the respondents agreed that awareness and avoidance of unsolicited messages (scams) can enhance mobile money security (mean = 4.6867). Also, the majority of them agreed that checking the authenticity of payment apps before using them can enhance mobile money security (mean = 4.6933). Again, the majority of the respondents agreed effective use of valid identification cards for all cash-out transactions can enhance mobile money security (mean = 4.4600). Furthermore, the majority of the respondents agreed that they do not trust anonymous calls when

money is involved and this enhances mobile money security (4.6467). The majority of the respondents also agreed that reporting fraudulent activity to MTN mobile money service operators can enhance mobile money security (mean = 4.5667). The majority of the respondents also agreed that the national communication authority must implement strict rules to monitor network operators on fraud issues to enhance mobile money security (mean = 4.6600). The majority of the respondents again agreed that the network operators should identify and assess sources of mobile money fraud to enhance mobile money security (mean = 4.5533). Furthermore, the majority of the respondents agreed that strict measures should be taken against suspected fraud issues to enhance mobile money security (mean = 4.6677). Finally, most of the respondents agreed that the network operators should suspend accounts of suspected frauds to enhance mobile money security (mean = 3.9400).

4.4 Discussion

4.4.1 Demographic Characteristics of the respondents

The majority (64.7%) of the respondents were above 30 years old with most of them in the range of 31 to 40 years as displayed in table 4.1. It can be said that the respondents were mature enough to understand MTN mobile money, and the other cashless banking transactions. Also, in table 4.2 most (62.7%) of the respondents were males. All the respondents had formal education with the majority (54.7%) attaining tertiary education in referenceto table 4.3. Most (36.0%) of the respondents were also civil servants and the remaining were into other occupations with 26.7% of the respondents being students as shown in table 4.4. The use of MTN and other network mobile money transactions cuts across all forms of occupation as reflected in this study.

4.4.2 Level of preference for MTN Mobile Money as compared to bank transactions or other cashless transactions (ATM and e-ZWICH)

The results shown in table 4.5, that the majority (78%) of the respondents have a bank account. This was contrary to the GSMA (2012) which concluded that more than one billion clients in emerging markets have access to a cell phone however do not have a bank account. Although they had bank accounts, the majority (98.7%) of them still operated MTN mobile money services as displayed in table 4.6. The quick development in the utilisation of cell phones and the absence of admittance to formal bank services in most African nations are contributing variables to the fast development and the utilisation of mobile money services in many parts of the continent.

Most (56.7%) of the respondents have been using MTN mobile money services for more than five years, as per table 4.7, a very few (6.7%) had used the MTN mobile money services for less than 2 years. MTN mobile money services have been in existence in Ghana for more than a decade now and their use is fast growing in the country. This is because most people in the country have access to mobile phones of all kinds. This agrees with the World Bank (2012) that changes in technology in terms of more affordable phones and expanded networks enabled the possibility of mobile money.

Also, from table 4.8, almost all (98.0%) of the respondents preferred MTN mobile money services to ATM and e-ZWICH services which are also cashless banking services. The same percentage (98.0) further indicated that the MTN mobile money service is easy to use. They may be due to the easy accessibility and convenience of

using MTN mobile money services. Service providers are available almost in every place that people pass by, including the rural communities where there are no banking services. This also agrees with Au and Kauffman (2007) who also found that most customers like the convenience and usability of the service for transactions and payments from their cell phones; therefore, the market for m-payment is developing quickly.

The majority (89.3%) of the respondents used MTN mobile money for domestic money transfers in reference to table 4.9. The mobile money services permit the clients to store money either through a bank account held with a bank or an account held with the mobile network operator so that they can transfer it to other registered and non-registered mobile network users. In agreement with this finding, Solin and Zerzan (2010) found that in Ghana, some mobile money subscribers use their mobile money wallets to transfer cash from to other relatives and friends.

However, in table 4.10, a few (36.0%) of the respondents used MTN mobile money for international money transfers. International cash transfer is across outskirts normally made out of transfers from families abroad to their relatives in their nations of origin. Transacting international money transfers with mobile money is still not common in Ghana especially and most people still prefer using Western Union, MoneyGram, etc. contrary to this, Solin and Zerzan (2010) indicated that some mobile money service users in Africa use mobile money services in transferring money internationally.

The majority (72.0%) of the respondents indicated in table 4.12, that they used MTN mobile money services in paying for utilities. Many services providers are going digital and some utilities companies also accept mobile money payments in Ghana. This also agrees with Solin and Zerzan (2010) who concluded that mobile money service enables clients to pay for fundamental utility services, for example, water, power, which gives more significant convenience and efficiency to customers of these services.

4.4.3 Measures that respondents have put in place to enhance mobile money security to prevent fraud

The majority of the respondents agreed that suspicious transactions were suspended until confirmation (mean = 4.5267). The mobile money agent or merchant can initiate fraud and when they are suspected, it is necessary to terminate the transaction with them. This agrees with Mudiri (2012) who also contended that fraud is more pervasive during the initiation of transactions of the business when customers start to believe the MNO offering the services.

Also, the majority of them agreed that the true identity of the sender and the receiver is verified before a transaction is processed (mean = 4.6800). In securing the mobile money transactions, it is necessary to confirm and validate the receiver before proceeding to transact. This finding agrees with Schwiderski-Grosche and Knospe (2002) who argued that before mobile money transactions are made to a receiver, the sender needs to verify whether the money is being sent to the right receiver from the mobile money agent before allowing the transaction to proceed.

Again, the majority of the respondents agreed that unsolicited calls from anonymous callers concerning MTN mobile money are avoided (mean = 4.6600). Mobile money fraudsters usually call their victims and ask them to follow some instructions they will give them. It is, therefore, necessary to avoid any unsolicited calls especially those that concerns promotions with some unknown instructions. This agrees with Gilman and Joyce (2012) who suggested that mobile frauds are advancing and several methods including phone calls are used in getting to the victims.

Furthermore, the majority of the respondents agreed that they do not share my Mobile Money PIN with close friends and families (4.6067). Most mobile money subscribers are become aware of the importance of their mobile money PINs and therefore avoid sharing them with other people. This finding is contrary to the findings of InterMedia (2012) in Tanzania which uncovered that almost all the study participants shared their PINs with families, friends, or mobile money agents.

The majority of the respondents also agreed that their phones are not given to friends and family members to transact in my absence (mean = 4.5400). The respondents also agreed that transaction details are not exposed to third parties (mean = 4.6467). This may be because the respondents have some level of formal education. Most people who have formal education can make mobile money transactions without the assistance of another person. This agrees with the findings of Jack and Suri (2011) in Kenya in which they concluded that mobile money clients are bound to be literate than non-clients and will not, therefore, make other persons transact on their behalf.

The majority of the respondents again agreed that suspicious MTN mobile money fraudulent activities are reported to MTN customer care (mean = 4.6667). It is appropriate to always report any fraudulent activities to the MTN customer care centre for further action. MTN customer care has a shortcode for reporting such activities through a text message. This also agrees with Gilman and Joyce (2012) who argued that another way of controlling mobile money fraudulent activities is to report to the customer care centre of the MNO.

The majority of the respondents further agreed that they use strong PINs instead of weak PINs such as date of birth (mean = 4.5467). Available user authentication systems on cell phones are PINs, passwords, and patterns. This agrees with the NIST SP800-124 (2008) that these methods of verification systems are not fool-proof and they are the principal line of safeguard to forestall unapproved access to cell phones.

4.4.4 Link between mobile device security and MTN mobile money account security

Most of the respondents agreed that mobile phones should be registered and linked to mobile money accounts so that mobile money transactions cannot be done on different phones (mean = 3.1267). It was therefore agreed by most of the respondents that there is the possibility of retrieving the mobile money account if the mobile phone and the SIM card get missing since they have both been linked together (mean = 3.9400). When the mobile phone is registered and linked with the mobile money account, no person can use the mobile phone to perform any transactions except the person who registered it, since there will be the need for verification. This agrees with Fogie (2006) who also asserted that mobile device registration will help prevent fraud since no one can use the device except the client who registered it.

Also, the majority of them agreed that the use of special software on phones to track suspicious users of mobile money accounts will ensure mobile money account security (mean = 4.5933). Again, the majority of the respondents agreed to software to check wrong mobile money PINs entry attempts will ensure mobile money account security (mean = 4.5467). There are add-ons security software that can help prevent frauds especially those that can give the subscriber an alert. These findings agree with Fogie (2006) who again indicated that some of the accessible preventive components that could be employed include the installation of customer software.

Furthermore, the majority of the respondents agreed that the use of a lock for mobile device-a PIN/password or an app with a lock/unlock feature that users can use to block their phone remotely in case it gets stolen or lost will ensure mobile account security (4.6067). This agrees with Fogie (2006) who further indicated that remote erasure or locking of the cell phones is another way of preventing fraud since the user can easily lock the mobile device remotely to prevent its use by the fraudster.

The majority of the respondents also agreed that the use of a special feature, for example, figure print to access MTN mobile money account to avoid unauthorized users (mean = 4.5667). Fingerprints are unique and stronger than passwords and PINs and will therefore be appropriate to protect the mobile money account. This agrees with Hoseph and Anpalagan (2007) who indicated that ensuring sensitive data saved on the cell phone, for example, account numbers or validation information are protected with PINs or passwords including figure prints is an essential consideration.

The majority of the respondents again agreed that third parties can access mobile money when passwords or PINs are disclosed to them (mean = 4.5533). With the MTN mobile money service, all a person needs is to know the mobile money PIN of the subscriber to do mobile money transactions. It therefore easy for a third party to have access to the mobile money account once the PIN is disclosed to them. This agrees with the NIST SP800-124 (2008) that the Mobile phone should be treated as a credit card and the PIN should be a secret to the subscriber alone.

The majority of the respondents agreed that the use of mobile payment apps that issue an immediate electronic receipt to help track mobile money transactions and evidence of payments will help secure mobile money account (mean = 4.6333). Also, the respondents further agreed that making sure that mobile apps used for payments and banking are safe and legit will secure mobile money account (mean = 4.6067). When there is an app that can print receipts and also track transactions it will be appropriate but not enough unless the app is verified to be legit. This agrees with the findings of a study by Harris *et al.* (2013) on security and privacy concerns related to mobile money in Africa which uncovered that mobile money clients will have a significant task to carry out in securing their mobile money through the verification of apps and software they use in their transactions.

4.4.5 View of users about measures that can be put in place to enhance mobile money security to prevent fraud

The majority of the respondents agreed that awareness and avoidance of unsolicited messages (scams) can enhance mobile money security (mean = 4.6867). It is the responsibility of the mobile money client to have knowledge of which messages are scams and avoid them. This agrees with Seakomo (2012) who argued that the security

practices of clients do improve over the long run since the degree of knowledge and awareness on security techniques increase over the long-term, in this way diminishing the probability of mistakes by users.

Also, the majority of the respondents agreed that checking the authenticity of payment apps before using them can enhance mobile money security (mean = 4.6933). Every app that is to be used for cash transactions needs to be very verified or authenticated before use. This agrees with the findings of a study by Harris *et al.* (2013) who again uncovered that mobile money clients will have to verify apps and software they use in their transactions.

Again, the majority of the respondents agreed that the effective use of valid identification cards for all cash-out transactions can enhance mobile money security (mean = 4.4600). MTN mobile money transaction, especially cashouts now requires the use of a valid identification card from the client. The number of the identification card is input in the cash transaction process to verify the person redrawing the money. This agrees with a survey in Kenya by Merritt (2010) who found that to do mobile money deposit (cash in) or transfer money through a specialist, the client must give a type of identification card, as a method of “know-your-client”.

The majority of the respondents also agreed that reporting fraudulent activity to MTN mobile money service operators can enhance mobile money security (mean = 4.5667). It is appropriate to always report any fraudulent activities to the MTN customer care centre for further action. MTN customer care has a shortcode for reporting such activities through a text message. This also agrees with Gilman and Joyce (2012) who

further argued that another way of controlling mobile money fraudulent activities is to report to the customer care centre of the MNO.

The majority of the respondents also agreed that the national communication authority must implement strict rules to monitor network operators on fraud issues to enhance mobile money security (mean = 4.6600). The National Communication Authority is the legal body that regulates the Mobile Communication Networks (MCNs) and therefore has the power to put in place some measures that will ensure that the MCNs are putting the security of the client prime to their mobile money operations. This agrees with the HM Treasury (2006) which indicates that to effectively organize and control the danger of mobile money fraud MNOs must comprehend their risk craving or the costs they are to convey comfortably in a mobile money transaction.

The majority of the respondents again agreed that the network operators should identify and assess sources of mobile money fraud to enhance mobile money security (mean = 4.5533). Understanding the sources of the frauds or the fraud risks is the first step in tackling the risks. This agrees with the assertion by Gilman and Joyce (2012) who indicated that fraud can be avoided by identifying and surveying the sources of mobile money fraud and that the MNO must attempt to comprehend the possible sources of the mobile money fraud that may emerge.

Furthermore, the majority of the respondents agreed that strict measures should be taken against suspected fraud issues to enhance mobile money security (mean = 4.6677). They, therefore, agreed that the network operators should suspend accounts of suspected frauds to enhance mobile money security (mean = 3.9400). Although the

clients are always aware of the frauds that involve mobile money transactions, the MNO also has a part to play to protect the transactions of the client. This also agrees with the HM Treasury (2006) which further indicated that to effectively organize and control the danger of mobile money fraud MNOs must comprehend their risk craving or the costs they are to convey comfortably in a mobile money transaction.



CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the major findings, the conclusion, and the recommendation of the study. The presentation under each heading is done according to the study objectives.

5.2 Summary

The result of the study shows most of the respondents preferred the MTN Mobile money account as compared to conventional banking and ATM and e-ZWICH. It was found that 98.7% of the respondents mostly operate MTN mobile money account as compared with ATM and e-ZWICH. It was also found that 56.7% of the respondents have been using it for more than 5 years. Also, 98.0% of the respondents preferred MTN mobile money services to ATM and e-ZWICH services. The same percentage (98.0) further indicated that the MTN mobile money service is easy to use. Also, the study revealed that 89.3% of the respondents use MTN mobile money for domestic money transfer, 36.0% use it for international money transfer and 72.0% use it in paying for utilities.

The study also revealed that some of the measures currently put in place by the MTN Mobile money subscribers to enhance mobile money security include suspension of a suspicious transaction until confirmation, verifying the true identity of the receiver, avoiding unsolicited calls from anonymous callers concerning MTN mobile money, avoiding sharing of mobile money PINs, not giving mobile phones to other people to

transact on their behalf and reporting fraudulent activities to the mobile money customer care centre.

The study further found that mobile phones should be registered and linked to mobile money accounts so that mobile money transactions cannot be done on different phones, the use of special software on phones to track suspicious users of mobile money accounts will ensure mobile money account security, the use of a remote lock for a mobile device will ensure mobile account security, the use of fingerprint access MTN mobile money account to avoid unauthorized users and the use of mobile payment apps that issue an immediate electronic receipt to help track mobile money transactions and evidence of payments will help secure mobile money account.

Finally, the study revealed that awareness and avoidance of unsolicited messages (scams) can enhance mobile money security, checking the authenticity of payment apps before using them can enhance mobile money security, effective use of valid identification cards for all cash out transactions can enhance mobile money security, reporting of fraudulent activity to MTN mobile money service operator can enhance mobile money security, MNO identifying and analysing the sources of frauds can enhance mobile money security and strict measures should be taken against suspected fraud issues to enhance mobile money security.

5.3 Conclusion

The study concludes that mobile money subscribers prefer operating MTN mobile money account as compared with ATM and e-ZWICH. Also, mobile money subscribers have been using MTN mobile money services for more than 5 years and

they still preferred MTN mobile money services to ATM and e-ZWICH services. The MTN mobile money service is easy to use and subscribers use the services for domestic money transfer, paying for utilities, and sometimes for international money transfers.

The study also concludes that some of the measures currently put in place by Mobile money subscribers to enhance mobile money security include suspension of a suspicious transaction until confirmation, verifying the true identity of the receiver, avoiding unsolicited calls from anonymous callers concerning MTN mobile money, avoiding sharing of mobile money PINs, not giving mobile phones to other people to transact on their behalf and reporting fraudulent activities to the mobile money customer care centre.

The study further concludes that mobile phones should be registered and linked to mobile money accounts so that mobile money transactions cannot be done on different phones, the use of special software on phones to track suspicious users of mobile money accounts, the use of a remote lock for mobile device, the use of fingerprint access MTN mobile money account to avoid unauthorized users and the use of mobile payment apps that issue an immediate electronic receipt to help track mobile money transactions and evidence of payments are some of the means that will help secure mobile money account with the mobile phone or mobile device.

Finally, the study concludes that awareness and avoidance of unsolicited messages (scams, checking the authenticity of payment apps before using them, effective use of valid identification cards for all cash-out transactions, reporting of fraudulent activity

to MTN mobile money service operator, MNO identifying and analyzing the sources of frauds and taking strict measures against suspected fraud issues are the means of enhancing mobile money security.

5.4 Recommendations

Based on the findings of the study, the following recommendations are made:

- Both agents and subscribers should be allowed to register with guarantors who are well-known and already have mobile money account so that they could be contacted in case of fraud and emergency.
- MTN Ghana should allow customers to provide personal information like date of birth and other vital details before accessing self-service so that customers would not be lured to disconnect themselves after they have been frauded.
- Because all mobile money transactions depend on the network of the mobile service providers, the improvement in the network will improve the security of the mobile money services.
- The mobile money service providers, in this case, MTN must set up password expiring time for mobile money subscribers to change their passwords quarterly and authenticate it through answering questions regarding personal identification.
- The mobile money agents need to assist the mobile money provider to identify the agents who are not authorized in the market.
- The mobile network operators should include features that will enable people who send money through mobile money agents to also receive an alert on their mobile phone confirming the transaction and identity of the receiver.

- The MNO needs to vet mobile money agents for a good character during their recruitment process.
- MTN Ghana should make it a point to audit their agents from time to time in order to keep them on track to avoid mobile money fraud.
- Future studies can look into the benefits of mobile money services to subscribers, especially in Ghana.



REFERENCES

- Afanu, K.E & Mamattah, S.R. (2013). *“Mobile Money Security – A Holistic Approach”*. MSc. Information Security, Luleå University of Technology.
- Amrik, H. & Mas, I. (2009). *Seeking Fertile Grounds for Mobile Money*, Bill & Melinda Gate Foundation.
- Au, Y. A & Kauffman, R. J. (2007). *“The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application”* *Electronic Commerce Research and Applications*, viewed 20 February 2013, www.elsevier.com/locate/ecra.
- Ayers, R., Jansen, W., Moenner, L., & Delaitre, A. (2007). *“NIST Interagency Report (IR) 7387’ Cell Phone Forensic Tools: An Overview and Analysis Update”*, viewed 15 December 2012, <http://csrc.nist.gov/publications/nistir/nistir-7387.pdf>.
- Bickman, L. & Rog, D. J. (1993). *Applied research design a practical approach*, (1st ed.). SAGE Publications, Inc.
- Bogdan, R, & Biklen, S K (1982). *Qualitative research for education: An introduction to theory and methods*. Boston, MA: Allyn & Bacon.
- Breeuwsma, M, de Jongh, M, Klaver, C, van der Knijff, R & Roeloffs, M (2007). *“Forensic Data Recovery From Flash Memory”*, *Small Scale Digital Device Forensics Journal*, 1(1).
http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf
- CIO East Africa (2012). *Vulnerabilities and attack exposure (2012)*. 28 February 2012.

- Crowe, M. (2010). "The Mobile Payments Landscape." *Presentation, Federal Reserve Bank of Boston*, Viewed 23 February 2013, <http://www.bos.frb.org/economic/cprc/presentations/2010/Crowe022310.pdf>; accessed February 13, 2021.
- Egger, F & Abrazhevich, D (2001). "Security & Trust: Taking Care of the Human Factor," *Electronic Payment Systems Observatory Newsletter*, vol. 9, 2001.
- Eze, UC, Gan, GG, Ademu, J & Tella, SA (2008). "Modelling user trust and mobile payment adoption: A conceptual framework" *Communications of the IBIMA*, Volume 3.
- Fogie, S. (2006). *Air scanner vulnerability summary: Windows mobile security software fails the test*, *informIT*, Viewed 1 November 2012, <http://www.informit.com/articles/article.aspx?p=607375>
- Gartner, C. P (2012). *Mobile Payment Market Will Experience Fragmented Service Offerings in the Short Term*, viewed 04 December 2012
- Gilman, L. & Joyce, M. (2012). "GSMA — Mobile Money for the Unbanked", *Managing the Risk of Fraud in Mobile Money*, Viewed 12 January 2013 http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobilemoney.pdf
- Githui, D. M. (2011). *Mobile money transfer in Kenya: an ethical perspective*, *Research Journal of Finance and Accounting* ISSN 2222-1697 (Paper) ISSN 2222-2847 (Online) 2(2). www.iiste.org/Journals/index.php/RJFA/article/download/191/75
- GSMA Mobile Money Tracker (2012). "Global Mobile Money Deployment Tracker." Viewed 02 February 2013: Available at <http://www.wirelessintelligence.com/mobile-money> GSMA Website 2012:

Mobile Money for the unbanked, viewed 02 February 2013

<http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-theunbanked/programme-overview>

Harris, A., Goodman, S., & Traynor, P. (2013). *Privacy and security concerns associated with mobile money applications in Africa*, 8 Washington Journal of Law, & Arts 245 (2013), viewed 12 April 2013,

<http://digital.law.washington.edu/dspacelaw/handle/1773.1/1198>

Herzberg, A. (2003). *Payments and banking with mobile personal devices*, 2068 *Communications of the ACM* 46(5) (2003) 53–58.

HM Treasury (2006). *Thinking about risk - managing your risk appetite: a practitioner's guide*, viewed 15 June 2013,

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191520/Managing_your_risk_appetite_a_practitioners_guide.pdf

Hoseph, L & Anpalagan, A (2007). *Trends and challenges in handheld wireless application development*, IEEE Canadian Review, No. 55, October 2007.

IFC (2011). *Mobile money study: Summary report*. International Finance Corporation.

<http://www.ifc.org/wps/wcm/connect/fad057004a052eb88b23ffdd29332b51/MobileMoneyReport-Summary.pdf?MOD=AJPERES>

InterMedia (2012). *Tanzania mobile money tracker study - Wave 3 Report*, Viewed 2 May 2013,

<http://www.audiencescapes.org/sites/default/files/Tanzania%20Mobile%20Money-Q3.pdf>

Jack, W. & Suri, T. (2011). *Mobile money: the economics of M-PESA*. Viewed 1 May 2013, <http://www.mit.edu/~tavneet/M-PESA.pdf>

- Jansen, W & Ayers, R. (2007). *Guidelines on cell phone forensics*, NIST Special Publication 800-101, Viewed 20 May 2013,
<http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>
- Karnouskos, S. (2004). "Mobile Payment: A journey through existing procedures & standardization initiatives " *IEEE Communications Surveys & Tutorials*, 44-66.
- Knijff van der, R. (2002). *Embedded systems analysis, handbook of computer crime investigation*, Edited by Eoghan Casey, Academic Press.
- Krejcie R.V. & Daryle, W.M (1970). *Educational and psychological measurements*, 30, 607-610.
- Kreyer, N., Pousttchi, K. & Turowski, K. (2002). *Mobile payment procedures: scope and characteristics*, *e-Service Journal* 2, 7–22.
- Lee, Y. S, Kim, E & Jung, M. S. (2013). "A NFC based Authentication method for defence of the Man in the Middle Attack" *3rd International Conference on Computer Science and Information Technology (ICCSIT'2013)* January 4-5, 2013 Bali, Indonesia.
- Linck, K., Pousttchi, K. & Wiedemann, D. G. (2006). *Security issues in mobile payment from the customer viewpoint*. In Ljungberg, J. (Hrsg.): Proceedings of the 14th European Conference on Information Systems (ECIS 2006).
- Mallat, N. (2007). "Exploring consumer adoption of mobile payments - A qualitative study," *Journal of Strategic Information Systems*, 16, 413-432, 2007.
- Merritt, C. (2010). *Mobile money transfer services: the next phase in the evolution in person-to person payments*. Viewed 19 April 2013,
http://www.frbatlanta.org/documents/rprf/rprf_resources/wp_0810.pdf

- Ministry of Finance (2019). *Composite budget for 2020-2023*. Programme based budget estimates for 2020.
- MTN (2015). About Mobile Money. <http://mtn.com.gh/personal/mobile-money/about-mobile-money> [Retrieved on November 19, 2020]
- MTN Group Limited (2018). Integrated Report for the year ended 31 December 2018
- Mudiri, J.L. (2012). *Fraud in mobile financial services*, MicroSave Publication , Viewed 20 May 2013, http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf
- Mugenda, M. & Mugenda, G. (2008). *Research Methods, Quantitative and Qualitative Approaches*.
- NIST (National Institute of Standards and Technology) (2008). Special Publication 800-124 2008, *Guidelines on Cell Phone and PDA Security*, <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>
- Pénicaud, C., & Katakam, A. (2013). State of the industry 2013: mobile financial services for the unbanked. GSMA. Retrieved from http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2014/02/SO_TIR_2013.pdf
- Schwiderski-Grosche, S. & Knospe, H. (2002). *Secure M-Commerce*, Information Security Group, Royal Holloway University of London, Egham TW20 0EX, UK.
- Seakomo, S. (2012) *Mobile phone users' information security practices, situation of students in Ghana*, Master's Thesis number LTU-EX-2012-41518700, Luleå University of Technology, Sweden.

- Solin, M. & Zerzan, A. (2010). *Mobile money methodology for assessing money laundering and terrorist financing risk*, GSMA Discussion Paper, <http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/03/amlfinal35.pdf>
- Taga, K., Karlsson, J. & Arthur, D. (2004). *Little Global M-Payment Report*, Austria, Vienna.
- The Economist Webpage (2012). *One business where the poorest continent is miles ahead*, viewed 04 Nov. 2012, <http://www.economist.com/node/21553510>
- Troy, L (2008). *Apple iPhone passcode work-around, digital forensic lab*, Fort Worth Police Department, Viewed February 26, 2013, http://mobileforensics.files.wordpress.com/2008/02/iphone_passcode_workaround.pdf
- Withers, S (2008). Whoops! iPhone passcode bypass a cinch, viewed November 28, 2013 <http://www.itwire.com/content/view/20273/53/>
- World Bank (2012). *Information and communications for development 2012: Maximizing Mobile*, Washington, DC: World Bank. DOI: 10.1596/978-0-8213-8991-1; viewed 6th

APPENDIX

QUESTIONNAIRE

UNIVERSITY OF EDUCATION, WINNEBA

Dear Respondent,

I am a student of the University of Education Winneba conducting a study on **MOBILE MONEY SECURITY AWARENESS AMONG MTN MOBILE MONEY USERS IN GHANA**". I would be pleased if you could kindly spare a few minutes of your time to answer the questions in this survey, I wish to assure you that your response will be confidential and used for academic purposes only.

SECTION A: Demographic Characteristics

1. Sex: Male () Female ()
2. Age: Less than 18 years () 18-25 years () 26-30 years () 31-35 years ()
36-40 years () 41-45 years () 46-50 years () Above 50 years ()
3. Level of education: Nil () Primary () Secondary () Tertiary ()
4. Occupation.....

SECTION B: Transaction preference

Please tick (√) in the appropriate bracket to indicate your response

1. Do you have a bank account? Yes () No ()
2. Which of the following Electronic Accounts do you operate? MTN Mobile money () ATM and E-ZWICH () other specify.....
3. How long have you been using MTN mobile money services?
Less than 2 years () 2-5 years () more than 5 years () None ()

4. Which of the following will you prefer? MTN Mobile money ()
ATM and E-ZWICH () other specify
5. Which of the services do you use for domestic cash transfer? MTN Mobile money () ATM and E-ZWICH () other specify
6. Which of the services do you use for international money transfers? Mobile money () ATM and E-ZWICH () other specify
7. Which of the following is easy to use? MTN Mobile money () ATM and E-ZWICH () other specify
8. Which of the following have you ever used in paying for utilities? MTN Mobile money () ATM and E-ZWICH () other specify
9. Have you ever stopped using your Mobile Money account? Yes () No ()
If Yes Go to question 10
10. Why did you stop using your Mobile Money account?

SECTION C: Current MTN mobile money security measures

Indicate the level to which you agree or disagree with the statements below regarding the current measures you (as a user) put in place to ensure the security of your MTN mobile money account.

1-Strongly Disagree 2-Disagree 3-Neutral 4-Agree 5-Strongly Agree

#	Statement	1	2	3	4	5
1	Suspicious transactions are suspended until confirmation.					
2	The true identity of the sender and the receiver is verified before a transaction is processed.					
3	The use of a valid ID for all MTN mobile money transactions to ensure I am the true user of the account.					
4	I don't share my MTN mobile money PIN with close friends and families					

5	The phone is not given to a friend or family member to do a transaction in my absence.					
6	Transaction details are not exposed to third parties.					
7	Suspicious MTN mobile money fraudulent activities are reported to MTN customer care.					
8	I do not do transactions at suspected agent points. Example agents who are situated at secret corners					
9	The use of strong PINs instead of using weak PINs like date of birth.					
10	I ensure every mobile money transaction I do is safe and secured, that is I do transactions with people I know.					

SECTION D: Link between mobile phone protection and MTN mobile money security

Indicate the level to which you agree or disagree with the following regarding the link between your mobile phone protection and your mobile money account security

1-Strongly Disagree 2-Disagree 3-Neutral 4-Agree 5-Strongly Agree

#	Option	1	2	3	4	5
1	Mobile phones should be registered and linked to Mobile money accounts so that Mobile money transactions cannot be done on different phones.					
2	The use of special software on phones to track suspicious users of Mobile money accounts					
3	Software to check wrong MTN mobile money PINs entry attempts					
4	Use a lock for your mobile device – a PIN/password or an app with a lock/unlock feature that you can use to block your phone remotely in case it gets stolen or lost.					
5	The use of special features example fingerprint to access MTN mobile money account to avoid unauthorized users					

6	Money on mobile money wallet can be lost in the event that the mobile phone gets lost.					
7	Third parties can access mobile money when passwords and PINs are disclosed to them.					
8	The use of mobile payment apps that issue an immediate electronic receipt to help track mobile money transactions and evidence of payments.					
9	Make sure that mobile apps used for payments and banking are safe and legit					
10	Possibility of retrieving your Mobile money account if your mobile phone and the sim card get missing since they have both been linked together					

SECTION E: Measures to enhance mobile money security

Indicate the level to which you agree or disagree with the statements below regarding the measures that can be put in place to prevent MTN mobile money fraud.

1-Strongly Disagree 2-Disagree 3-Neutral 4-Agree 5-Strongly Agree

#	Statement	1	2	3	4	5
1	Protection of Personal Identification Numbers PINs from third parties.					
2	Awareness and avoidance of unsolicited messages (scams)					
3	Check the authenticity of payment apps before using them					
4	Effective use of valid identification card for all cash-out transactions					
5	Don't trust anonymous calls when money is involved.					
6	Reporting of fraudulent activity to MTN mobile money service operator					
7	The national communication authority must implement strict rules to monitor network operators on fraud issues.					
8	Network operators should identify and assess sources of mobile money fraud					

9	Strict measures should be taken against suspected fraud issues.					
10	The network operators should suspend accounts of suspected fraud					

THANK YOU

