UNIVERSITY OF GHANA

COLLEGE OF HUMANITIES

DEPARTMENT OF SOCIOLOGY

EXPLORING THE EXPERIENCES OF MOBILE MONEY FRAUD VICTIMS IN MADINA MARKET

BY

AFUA AGYEIWAA ADDAE-SAKYI

(10481701)

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF MPHIL IN SOCIOLOGY DEGREE

OCTOBER, 2020

DECLARATION

This is an independent work carried under the supervision of Professor Michael Okyerefo and Dr. Rosemond Hiadzi for the award of a Master of Philosophy (Sociology) degree. I declare that this work is my own work and every other person's work has been fully acknowledged. I declare that this thesis has not been submitted to any other University and all shortcomings are my own responsibility.

……. …29th October 2020……

Afua Agyeiwaa Addae-Sakyi Date

STUDENT

…..*mpkokyerefo,* …… *29.10.2020*…….

Prof. Michael Okyerefo Date

(PRINCIPAL SUPERVISOR)

…. ……29th October, 2020……

Dr. Rosemond Hiadzi Date

(SUPERVISOR)

ACKNOWLEDGEMENT

I wish to acknowledge my supervisors Professor Michael Okyerefo and Dr. Rosemond Hiadzi for their generous support, encouragement, and corrections during the writing of this dissertation.

My final gratitude goes to my parents and friends who in one way or the other contributed to my success in this program.

ABSTRACT

Mobile Money usage has grown significantly with reports from Bank of Ghana indicating a 73.4 percent growth rate between 2012 and 2016 and accounting for 94.11 percent of total non-cash payment. Mobile money fraud is one area of cybercrime that has gained notoriety in Ghana in recent times because of the increasing number of subscribers and volume of transactions. This study explores the experiences of Madina market traders who have been victims of mobile money fraud. It further examines the factors that influence mobile money fraud amongst the traders. The study adopted a sequential mixed method approach: a survey of 235 mobile money users from Madina market and interviews with 3 respondents who had been victims. Quantitative findings revealed that apart from gender that has an influence on mobile money fraud, educational background and telecommunication network do not influence mobile money fraud among the traders. Interviews with victims of mobile money fraud revealed that victims feel reluctant to report incidents of fraud to police or network operators because of their inability to resolve issues. The study also disclosed that, the emotional pain experienced by victims of mobile money fraud can deter them from using mobile money for any financial transaction. The study recommends that service providers increase the education on mobile money fraud in local languages in order to reach traders with no formal education.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 Motivation of study

On the 3rd of January 2019, just a few days after the new year, I was at home with my parents and siblings and we had just had supper and listening to the evening news on Radio. Shortly, there was a news report on man named Stephen Nyuur who had been defrauded through mobile money. He was invited to the studio and asked to explain his ordeal to the listeners of the station. Stephen explained that he owns a shop close to Dome where he sells provisions. He works alone and this makes it difficult for him to go to his suppliers to get goods for his shop. Very often he pays for his goods through mobile money and have them delivered to his shop. Also, when regular customers come by to pay for goods, he accepts payment through mobile money as it is easy to use and convenient for customers who want to pay later. This was how one of Stephen's customers sent her payment of 10,000 Ghana cedis through mobile money and later received a call from another person who claimed to have been calling from the MTN office. They claimed that his recent payment was yet to fall in his account and he only needed to allow cash out for the problem to be resolved. Stephen explained that once he allowed cash out, his money of 14, 000 in his wallet was all gone. He tried calling the number back and the line was just not going through. Later that day, he sent a report to the Nima Police station and he said the police is yet to start investigations.

Later that evening, after listening to the news report, my mum just received a call from an unknown number about money being mistakenly sent into her account. The caller explained that he was sending 500 Ghana cedis to his sister and made a mistake while typing the number and the

money got on to my mum's phone. While still on a call, she received an SMS about money being deposited into her mobile money wallet. She checked this SMS and it was indeed 500 Ghana cedis which the guy claimed to have deposited. Without double checking her account, and this being the first time she received such a call, she quickly wore her glasses and sent GH 500 back to the caller. It was only after this transaction was done that my dad asked what calls she had been busy with. She then narrated the story to us all over again and we immediately knew there was something wrong. We quickly asked her to check her balance and lo and behold, her 500 Ghana cedis was gone just like that. We decided to call the number and he picked up only to tell my mum that he has already spent the money and will not be able to refund it. We then decided on two things, that is, to report the matter to MTN and also to inform the Police. We first called MTN and we were told that the guy had already withdrawn the money so there was nothing they could do about it. However, if we keep calling to remind them, anytime he makes a deposit, they will block the money and send it to my mum. After calling MTN, we passed by the Atomic Hills Police station and we were made to write a report. The number of the fraudster was taken and the police assured as those investigations will start as soon as possible. They also explained that once they get hold of him, they were going to call us. It's been over a year now and neither the Police or MTN has been able to get my mum's money back to her or even gotten hold of the fraudster.

This fraud in which my mum fell victim of has happened to a lot of people over the past year and the number keeps increasing. However, it is very difficult to tell why this is happening. Many people fall victims and it is difficult to tell whether service providers or other authorities are putting in the right measures to protect their customers. Then again, others can argue that, is it the motivated nature of these fraudsters that lead them to do this to innocent victims?

1.2 Background of Study

The system of using mobile phones for financial transactions has grown exponentially in recent times. This is primarily because, Mobile Money (MM) as it is popularly called, has addressed the problem of accessibility which excluded people from rural and remote areas from the banking system. According to Global System for Mobile Communication Association (GSMA), MM systems are said to be available in 90 countries worldwide registering 143 million subscribers in 2018 only, and the total number of registered subscribers is estimated to be 866 million with daily transactions totaling $1.3 billion (GSMA, 2017).

Mobile money is an electronic cash that is stored using the Subscriber Identification Module (SIM) in a mobile phone as identifier (Bank of Ghana, 2017). Mobile Money has transformed the financial space because it uses ICT and non-bank retail channels to deliver financial services to clients who were never part of traditional bank system. Mobile Money services has evolved over time and it includes peer-to-peer (P2P) transfers using electronic-wallets, payment of utility bills, buying airtime, receiving salary and governments to person payments (G2P) (GSMA, 2013).

With increasing access to mobile phones in Africa, MM has become an important channel to deliver financial services to rural areas. Mobile Money was first introduced in Africa in Kenya by the network operator, Safaricom in March 2007 (Demombynes & Thegeya, 2012). The mobile money platform was called M-PESA (M standing for mobile and PESA standing for payment in Swahili) has become the model for the implementation of Mobile Money by network operators in other African countries (Demombynes & Thegeya, 2012; Jack & Suri, 2011).

Mobile Money was first introduced in Ghana in 2009 by the network operator Mobile

Telecommunications Network (MTN) (Yu & Ibtasam, 2018). Since then, other network operators like Airtel-Tigo and Vodafone run mobile money platforms. This has created job opportunities for MM agents, service providers, Fintech companies, merchants and retailers. Mobile Money usage has grown significantly with reports from Bank of Ghana indicating a 73.4 percent growth rate between 2012 and 2016 and accounting for 94.11 percent of total non-cash payment (Bank of Ghana, 2017). The report also highlighted that there were about 12 million active accounts out of the over 31 million registered accounts and 190,000 active agents out of the 350,000 registered agents. Additionally, mobile money transfers were close to GH¢160 million by the end of the third quarter of 2018 compared with GH¢ 109 million during the same period in 2017. BOG also recorded mobile money interoperability between May and September, 2018 at GH¢104.85 million and 1,118,315 in terms of volume. Reports from other African countries like Kenya, Uganda and Nigeria also indicates a high growth rate in mobile money usage (Diniz et al., 2011).

Mobile money systems are recent technologies which still need development and innovations (Eze et al., 2008). These innovations are needed to address specific areas such as security authentication in mobile devices, security of wireless transmission of funds, trust/validation directories and virtual "wallets" stored on a mobile device or accessible over a network (Taga et al., 2004). Security is of paramount concern when it comes to Mobile payment because of the vulnerability of a man-in-the-middle attack: interception of confidential information by an attacker. Lee et al (2013) found out that man-in-the middle attacks were more common with near-field communication (NFC) payment systems where attackers were able to intercept relevant information during communication with the reader within 10cm radius.

Mobile devices capable to perform mobile money services are described as GSM compatible phones with embedded services such as SMS and unstructured supplementary service data (USSD) (World Bank, 2012). The lack of end-to-end security properties in SMS and USSD services means protection ends in the GSM or UMTS (Universal Mobile Telecommunications System) network. Schwiderski-Grosche and Knospe, (2002) argued that, though some security mechanisms (such as authentication, message confidentiality, message integrity and proof of receipt) exists in mobile devices, it depends on the applications to implement these security mechanisms and determine whether their cryptographic strengths are sufficient.

Mobile money, like every good innovation, is gradually being filled with some level of crime which poses a lot of threat to users and service providers. For instance, reports from GSMA, have explained that fraud has now seriously began in the mobile money system and this fraud takes three main forms. They include, transactional fraud, agent fraud and internal fraud (GSMA, 2017).

1.3 Theoretical Framework

Mobile phones or mobile technology is one of the most influential inventions in recent times which has changed the way we live and communicate with each other. As mobile and computer technologies continue to grow, criminals have taken advantage of these technologies to commit deviant acts. Crimes that are committed with the help of computer technologies is referred to as Cybercrime- a new breed of crime. Cybercrimes, unlike conventional crime, is difficult to combat because the identity of the perpetrators are not known.

There exist a number of theories that explains human deviant behaviours. Some of these theories can be applied to cybercrime even though they were originally meant to explain

conventional crime. These theories include general strain theory, situational crime prevention theory, social learning theory, routine activity theory, situational crime prevention theory.

1.3.1 Social Learning Theory

Social learning theory was propounded by Bandura (1977). According to social learning theory (also known as observational learning theory), people can learn new behaviors by observing others (Edinyang, 2016). This also refers to the reciprocal relationship between environmental social features, how they are perceived by individuals, and how motivated and capable a person is to replicate the behaviors they observe. This theory is founded on the premise that we learn by our interactions with others in a social setting and mimic it, especially if their observational experiences are good or include rewards associated with the observed action (Nabavi, 2014). Social learning theory is an important theory in sociology and in criminology. Social learning theory is a general theory of crime that has been used to explain different forms of deviant behaviours (Akers, 1998). According to social learning theory, deviant behaviours are borne out of an individual's association with deviant peers which in turn develops an individual's motivation and skills to commit crime.

Through this exposure to deviant behaviours, an individual is provided with attitudes, values and orientations that become rationalizations for committing crime. In addition to deviant association, criminal behaviour is learned by observing rewards and punishment associated with a particular behaviour: behaviours that are rewarded regularly become enticing and those that are constantly punished are avoided. The theory further explains that learning is a cognitive process which can occur in a social context through observation and imitation; people exhibit criminal behaviours because they have watched others with those traits and try to imitate them (Burruss et

al., 2012). In the context of cybercrime, social learning theory applies to sophisticated forms of cybercrime (e.g., hacking, malware/virus distribution) and unsophisticated or 'low-tech' forms of cybercrime (e.g., cyberbullying, cyberstalking). In sophisticated forms of cybercrime, perpetrators are unlikely to have the technical-know-how without associating with skilled offenders. Also, in cybercrimes that require low technical skills, offenders need to learn tactics and methods needed to conceal identity from other sources. Thus, the central theme of social learning theory is that rationalizations and skills must be learned and deviant behaviour is reinforced through the association and observation of others (Akers, 1973).

1.3.2 Routine Activity Theory

Felson and Lawrence (1979) proposed the routine activity theory. The theory is popular among criminologists because unlike other theories of criminality, routine activity theory studies crimes as an event, relating it to its environment and place a higher importance on its ecological process (Holt & Bossler, 2013; Kigerl, 2012; Pratt et al., 2010) The basic tenet of the theory is that crime or victimization can only occur with the right opportunity given in relation to time and space (Felson & Lawrence, 1979). According to the theory, the causes of crime has very little to do with social factors like poverty, inequality and unemployment but rather opportunities afforded to offenders as a result of technological inventions as in the case of cybercrime (Cohen & Felson, 1979). That is, the increase in the use of mobile money has created an opportunity for offenders to commit crime by defrauding subscribers.

In routine activity theory, crime is likely to be committed when three situations meet in space and time: motivated offender, suitable target, and absence of a capable guardian. A motivated offender refers to any individual who is most likely and willing to commit a crime with

the little opportunity available; a suitable target refers to any vulnerable individual that indirectly makes himself or herself available and accessible to the offender; absence of a capable guardian refers to an object or person which can deter or stop an individual from falling prey to the offender (Cohen & Felson, 1979).

Reyns et al. (2011) applied RAT to cyberstalking victimization on 974 college students. The authors also looked at the effects of on-line visibility, accessibility, and guardianship. The study concluded that the online exposure variables has little effects across the types of pursuit behaviours. The variable "adding strangers" was the only on-line proximity variable that appeared to be significantly related to victimization.

Leukfeldt & Yar (2016) studied the effect of the three essentials of RAT on six major types of cybercrime victimization on 9,161 respondents. They concluded that a visible target can at alltime be used to explain cybercrime victimization however the absence of a capable guardian varies; personal guardianship better explains cybercrime victimization as compared to technical guardianship which they believe has no relation in explaining cybercrime victimization.

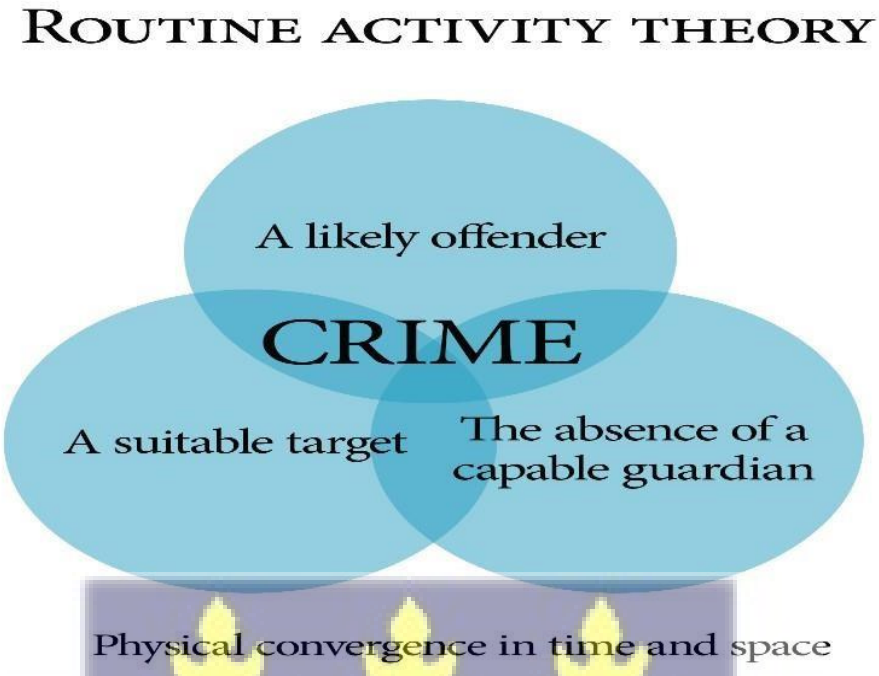


Figure 1: Routine Activity Theory

Source: *Wikipedia*

1.4 Problem Statement

The use of technology or computers to assist in crime or any form of deviance can be termed as Cybercrime (Holt & Bossler, 2014). In the early 2000s, cybercrime in Ghana was only limited to credit card fraud (Warner, 2011) but now it has taken different forms with time probably because of weak or absent cybersecurity infrastructure to mitigate these crimes. In the year 2010, Ghana was considered part of the top ten countries in the world with very high cybercrime.

Mobile money fraud is one area of cybercrime that has gained notoriety in Ghana in recent times because of the increasing number of subscribers and volume of transactions. Cybercrimes

associated with mobile money include theft of customer data, technical attack on mobile money services, internal fraud within service provider environment, subscription fraud, and account hijack or takeover (Subsex, 2017). The modus operandi of mobile money fraud perpetrators is to use social engineering techniques on unsuspecting victims to divulge confidential information.

This, in most cases leaves victims in a state of helplessness because the identity of the perpetrators is not known. In some social groups, victims of these fraud schemes are perceived as unwise and, in some instances, greedy. This has led to most victims not reporting cases of mobile money fraud for fear of being victimized.

Most studies done in Ghana has focused on the benefits of mobile money and a few on mobile money fraud. However, not many studies have assessed the knowledge of the ordinary Ghanaian, who are mostly victims, on mobile money fraud. To holistically tackle mobile money fraud, it is imperative to know how much security conscious is the mobile money subscriber. Could it be that people fall victims to these schemes because they do not know simple mobile security tips such as not disclosing your PIN to strangers or differentiating a genuine message from network operators from fake ones. Answers to these questions will assist network operators to implement targeted interventions to tackle this menace. My study seeks to explore the experiences of mobile money fraud victims in Madina market and assess the knowledge of the Madina market traders on mobile money fraud.

1.5 Aim and objectives

The aim of the study is to explore the experiences of Madina market traders who have been victims of mobile money fraud. The study specifically is set out to:

1. Examine the factors that influence mobile money fraud among traders in the Madina market.
2. Explore the impact of mobile money fraud on the traders who are victims.
3. Identify how and why traders of the Madina market get defrauded through mobile money.

Research questions

1. What factors influence mobile money fraud among traders in Madina market?
2. How do traders in Madina market get defrauded?
3. How does mobile money fraud impact traders who are the victims?

1.6 Significance of Study

This study presents a number of significant contributions to the field of cybercrime and is useful in adding to existing knowledge on mobile money fraud in Ghana. As more traders sign up to mobile money platforms, there is a high chance they might fall victims to mobile money fraud schemes because majority of them are illiterate and may not have any idea how these platforms work as far as security is concerned.

This study will throw light on the experiences of victims of mobile money fraud: the impact on their business and their psychological well-being. The relevance of this is underscored considering the growing academic and policy discussions surrounding cybercrime and mental health. Findings from the study will aid in giving the needed attention to victims of mobile money fraud as well as educating people on the risks of being a victim of mobile money.

Finally, although the purpose of this research is to fulfil a part of an academic requirement for a master of philosophy degree, findings from the research conducted will inform policy makers

and telecommunication networks to implement policies targeted at enlightening traders or workers in the informal sector on mobile money security.

1.7 Scope of the Study

The scope of the study is to explore the experiences of those who have been victims of mobile money fraud and assess the knowledge of traders on mobile money. Although, mobile money fraud affects everyone, this study will focus on traders at Madina market who have subscribed to at least one mobile money platform. The geographical context for the study is Ghana. The institutional scope of the study is Madina Market because of the high number of traders who visit on a daily basis.

Definitions of concepts

1. **Vishing or Smishing:** transactional fraud which has to do with making phone calls or sending SMS in order to gain some form of knowledge like the pin or personal details of the account holder (Yeboah-Boateng & Amanor, 2014).
2. **Advance fee scams:** fraud wherein customers are lured to send their money to the fraudsters at fake instances and this also constitutes a type of transactional fraud (Chawki, 2009).
3. **Reversal requests**: occur when customers are asked to return funds which were successful. Usually, when the customer attempts to refund the money all the money in their account is rather taken out of their account. This type again falls under transaction fraud (Chawki, 2009).
4. **False transactions:** occurs when customers receive SMS about successful transactions which are fake (Donchev, 2021).

5. **Split transactions** involve agents usually receiving a commission on any money that is sent. Hence, with this type of fraud connotes splitting the transactions in order to receive multiple commissions. The split transaction is a type of agent fraud (Chawki, 2009).
6. **Registration fraud:** has to do with creating multiple accounts in order to receive more than one commission. This type of fraud is also an agent fraud. Anytime agents register new subscribers, they receive some form of commission. Therefore, they sometimes create fake accounts in order to get more commission (Chawki, 2009).
7. **Identity theft** happens to be the last type of fraud mentioned by the GSMA and this type of fraud involves employees accessing information without the permission of the customer or exploiting the customer without their consent (Yeboah-Boateng & Amanor, 2014).

1.8 Outline of Chapters

The study is made up of six chapters. The first chapter describes two events of mobile money fraud, one from a radio interview and the other from my mother. This brings out the motivation of the study and sets the ball rolling on mobile money fraud and the experiences of victims in Ghana.

The first chapter also discusses the main objectives of the study, it's significance as well as the breadth of the study. The second chapter focuses on existing literature in the area of theories of cybercrime victimization, fraud in mobile financial services, types of mobile money fraud and prevalence of mobile money fraud. It discusses the routine activity that underpins cybercrime and mobile money fraud in detail. In chapter three, the research methodology is discussed. The explanatory sequential mixed method is used and justifications are given for each section. The quantitative process is discussed which is then followed by the qualitative process. Again, issues on ethics is discussed and the chapter is concluded with issues on COVID-19 protocols. Chapter four analyses data collected

through the questionnaire. Here, knowledge on why and how traders fall victims to mobile money fraud is discussed. The fifth chapter is dedicated to analyse the victims of mobile money fraud. Various themes are established and discussed in relation to the routine activity theory and the quantitative data. The final chapter is made up of the findings of the study, the limitations of the study as well as suggestions for future research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction.

Mobile money, despite its few years of operation, has created millions of dollars but has also been a conduit for fraud. However, in order to gain more understanding in the area, work that has been done by other scholars has to be reviewed. The first section looks at online fraud and victims of online fraud. Several types of fraud exist online and there are different types of victims associated with online fraud. These discussions will be a necessary starting point for understanding mobile money fraud and victims of mobile money fraud. Finally, mobile money fraud in Africa and Ghana will be discussed with attention given to victims of mobile money fraud. This section discusses the major points looking at the prevalence and state of mobile money fraud in Ghana and Africa as a whole and also to look at the extent to which mobile money users know about mobile money fraud. There are different types of mobile money fraud and these various types of mobile money fraud as discussed as well as the types

which are usually seen in the Ghanaian society.

2.2 Review of empirical literature

2.2.1 The nature of mobile banking in Ghana and its importance

The use of the mobile phone to engage in some financial services is known as mobile financial service (Boyd & Jacob, 2007). The increase in the use of mobile phones all around the world has resulted in the success of mobile financial services (Baptista & Oliveira, 2015). Mobile financial services include; mobile banking, mobile money transfer and mobile payments (GSMA, 2008). Mobile banking involves the use of the mobile phone to transact bank services. It comes in two forms which are either additive or transformational (Porteous, 2006). As an additive service, it is seen as an additional platform to compliment the banking hall where clients can perform transactions using their mobile phones whereas as a transformational service, it is aimed at creating new markets that is, finding customers who do not have bank accounts and including them into the larger banking system. Asongu (2015) asserts that mobile banking in sub-Saharan Africa has been successful due to a number of factors including education, bank density, urban population, internet penetration and ease in receiving remittances. In a comparative study of South Africa and Nigeria, it was realized that, SMS alerts were the most used forms of mobile banking and the adoption of the system has been due to literacy level, convenience and awareness. One major benefit of mobile banking in Africa has been the inclusion of the unbanked especially in developing countries (Baptista & Oliveira, 2015). It should be noted that mobile money users are more likely to be literate than non-users such that the more educated individuals are, the more likely they are to use money (Jack & Suri, 2011).

Mobile banking in Ghana evolved as a result of the high use of mobile money. In Ghana, mobile banking can be accessed in two ways. Firstly, by downloading bank specific apps and secondly by dialing short codes given by specific banks. The services offered are usually additive services which include, getting SMS alerts on transactions, checking one's own account, accessing a mini bank statement, transferring money and making bill payments.

Mobile payment is another form of mobile financial service which also falls under electronic payments (Porteous, 2006). Wang et al. (2016) categorize mobile payments under five types: mobile payment as the point of sale (POS), mobile payment at the POS, mobile payment platform, independent mobile payment system and direct carrier billing. Mobile payment at the POS is usually referred to as the mobile wallet and the mobile payment platform is used to make purchases from multiple merchants and retailers. This when the built-in apps like Google Wallet or Apple Pay can be used to make payments for services at the Point of Sale. For instance, an individual can scan their credit or debit card on their phone or enter the card number manually onto Google Wallet or Apple Pay account and verify their bank. When everything is correct, they approve and you can now pay for items using these apps at the Point of Sale. Mobile payment at the POS is the type of payment is when the mobile phone is used as the Point of Sale and usually used by merchants. In order to use this method, one has to download an app onto their mobile phones and connect their credit card to it. With that, purchases can be paid directly. An example of such app is the Square Register. The mobile payment platform method involves the use of online payment services. Independent mobile payment system is very similar to the mobile payment platform. However, the major difference here is that, payment apps are created by individual bodies and can be used only on purchases from that company.

Mobile money has been used for diverse purposes. For instance, evidence from Tanzania among 2,980 households in Tanzania revealed that the mobile money usage by registered users both in the urban and rural areas is that the service is for sending or receiving money (InterMedia, 2013). Despite the general believe that mobile money is used for transfer and receiving money, it is the second most popular means of savings in Tanzania and in Kenya (Jack & Suri, 2011). Aside using mobile money for remittance purposes, in Tanzania 14% of the 2,980 households surveyed use it for non-remittance purposes such as school fees payments, government fees and taxes, utility bills, and salaries, followed by 12% of users who use the platform to purchase goods and services in shops (InterMedia, 2013). The general uses of mobile money in the middle to high income countries such as Brazil, Sri Lanka, Thailand and USA are for transport fare payment. Mobile money transfers (P2P) is considered the least usage (IFC, 2011).

2.2.2 Overview of online fraud in Ghana

Online fraud is prevalent in many African countries and costing these countries a lot of money. Quarshie et al., (2012) indicate that banks in Zambia, Rwanda, Kenya, Uganda and Tanzania together lost US$245 million to cyber fraud. The major types of online fraud in Africa include advance fee scams, banking fraud, money transfer scams and mobile phone payments fraud (Busuulwa, 2016). Advance fee fraud can also come in different forms and these include: lottery notifications, investment invitations and inheritance notifications.

In Ghana, Osei-Boateng & Ampratwum, (2011) indicate that according to Criminal and Investigative Department of the Ghana Police, the major types of complaints about online fraud include, marriage deals, gold deals, inheritance and money in accounts. Most victims according to

the police are usually Europeans and Americans. Furthermore, the Criminal Investigation department of the Ghana Police explained that, cyber fraud has cost Ghana about $97 million between August 2016 and 2018 alone. However, just about 5.7% of these cases have been investigated since victims are not willing to cooperate with the police.

In recent years, the mobile phone has become a very essential device which can be used for many purposes. However, one very important use of the mobile phone is to conduct financial services. Boyd & Jacob, (2007) explain that the use of the mobile phone to engage in some financial services is known as mobile financial service. Mobile financial services have existed in Ghana for some years, and the largest form of mobile financial service being used is mobile money. GSMA (2013) indicates that mobile financial services come in different types and some of these include; mobile banking, mobile money transfers and mobile payments. Mobile money platforms have the highest cases of fraud among other mobile financial services in Africa (CGAP, 2017).

GSMA (2012) reports that there are eight types of fraud that are likely to occur in mobile money systems. These frauds can be categorised into transactional fraud, agent fraud and internal fraud. Transactional fraud is usually committed by fraudsters who understand the system of mobile money and use the opportunity to dupe others who do not fully understand the system; agent fraud occurs among agents mainly merchants and mobile money operators who seek to steal from customers; internal fraud is perpetrated by workers of telecommunication companies.

Akomea-Frimpong et al., (2020) identified common mobile money fraud schemes in Ghana. These include anonymous calls and text messages from fraudsters; false promotions; and false cash out SMS. In a study conducted by Annan (2017) in some six Ghanaian communities,

approximately 22% of transactions through agents or merchants go fraudulent especially for huge amounts and mostly occurs more when sending money than when receiving money.

2.2.4 Prevalence of mobile money fraud in Ghana

Mobile money fraud is prevalent in most African countries. As reported by Busuulwa (2016) the number of fraud cases in Uganda as at 2016 stood at 53% of the entire mobile money transactions in Uganda. Kenya had about 50% of mobile money fraud from total transactions. Morawczynski (2015) also indicates that, in Uganda MTN had lost about US$3.4 million through from fraud. Again, Mugisha (2014) shows that in Rwanda, Tigo lost US$700,000 in 2014.

In Ghana, there is no exact figure by the police about mobile money fraud. However, according to Akomea-Frimpong et al., (2020), a report shows that mobile money fraud in Ghana stood at 23 percent indicating how Ghana is at a high risk of mobile money fraud. The indication of prevalence of mobile money fraud in the literature is very sparse. However, telecommunication networks like MTN, AirtelTigo and Vodafone through the Ghana chamber of telecommunications have indicated that a total number of 338 fraud cases were reported in 2016 with amounts of money ranging from 70 Ghana cedis to 4000 Ghana cedis. In 2015, however, the figures reported were 278 cases. This shows that the number of fraud cases keeps increasing and not decreasing.

There have been a number of reports when it comes to understanding mobile money fraud perpetrators. The Director-General in charge of the Cybercrime Unit of the Criminal Investigations Department (CID), Assistant Commissioner of Police (ACP) Dr. Gustav Herbert Yankson has expressed that the success rate of their arrest and prosecutions were at 6.2%,

indicating how low perpetrators of this crime are found whilst the Communications Minister Ursula Owusu-Ekuful also hinted that only 10% of reported mobile money fraud cases have been investigated and prosecuted (Daily Guide Network, 2019). This low percentage of investigations has also led to a minimal report of mobile money cases by customers as very little can be done about the situation.

Again, according to Ghana's communication minister, 50% of mobile money subscribers were at risk of mobile money fraud with about 400,000 scammed SMS being blocked from reaching their targets of fraud as well as telecommunication companies receiving about 380 complaints of attempt of mobile money fraud a month from mobile money subscribers (Daily Guide Network, 2019). There are several victims of mobile money fraud and their wellbeing after being victimized is not covered in the literature. It is important therefore to study victims of mobile money fraud and to gain understanding of their experience of fraud and after being victimized.

2.3.5 Victims of online fraud and mobile money security.

The presence of the internet has revolutionized the way crime is committed. For instance, perpetrators of online fraud are able to find suitable targets overseas and execute their fraudulent schemes without even crossing any border (Button et al., 2014). This calls for different approach in tackling cybercrime because of the complexity of these types of crimes. Cybercrimes include, online fraud, malware, cyber threats or bullying and hacking or computer intrusion (Bergh & Junger, 2018).

A victim of online fraud is someone who has made some form of financial loss by responding in one way or the other to the requests of a scammer (Cross, 2015). Studies have shown

that a large number of online frauds goes unreported to police or appropriate authorities because of victim blaming; victims are seen as greedy and gullible and some don't receive the necessary support. In Europe and America, less than one-third of victims' report fraud cases (Cross, 2015). The same can be said about big organizations because they fear losing trust of stakeholders (Boateng et al, 2011). Victimization of victims of online fraud has several negative effects on the individual. Tade and Adeniyi (2017) explain that victims of ATM fraud in Nigeria tend to suffer many consequences including, post fraud trauma where by victims have a hard time bouncing back to their previous selves especially when they have planned out monies that have been stolen from them. In extreme cases where victims can't bear the harsh consequences of being frauded, they commit suicide (Cross, 2015).

Victims of online romantic fraud also experience a double hit as they tend to lose their money and go through psychological distress (Whitty & Buchanan, 2015).

Button et al., (2014) indicated that online victims fall prey to scams several times because of the small amount of money usually requested by scammers. Some scammers will usually request just a small amount of money and this will distract the victim from actually thinking that they are falling prey to a scam. Others also fall prey to these scams due to the type of smart technique adopted by these fraudsters. Again, the amount of knowledge displayed by scammers make it easy for people to fall prey to cyber fraud. As a result, when displaying their wealth of information, it becomes very difficult for the victim to detect a possibility of scam in their reaction.

Evidence from Tanzania suggests that although mobile money operators have company and industry principles guiding them, they have not been implemented and fully adopted, leading to the possibility of technological savvy people using their technologies to achieve their illegal targets of fraud and scam (Githui, 2011). For example, an average of 18% of respondents in the 2,980

household survey in Tanzania have had money stolen from their m-money account due to fraud or a scam (InterMedia, 2013).

It should be noted that in terms of privacy and security concerns associated with mobile money, mobile money users have an important role to play in securing their money. According to Harris et al. (2013), the lack of proper attention to basic security features on users' mobile phones make users vulnerable to numerous threats, the most damaging of which is the loss of money if an attacker gains physical control of the mobile phone. Furthermore, security is a bilateral role between both user and the service provider because it is possible a technically adept adversary may be able to take advantage of poor security design within mobile money apps or bypass poorly implemented encryption (Harris et al., 2013). Therefore, it is critical that both users and financial institutions consider a range of risk model activities to protect the service. Thus, if proper attention to security of the mobile phone is not taken, the user may be vulnerable to criminal activity (Harris et al., 2013).

2.2.6 Online Lifestyle, Capable Guardianship and Cybercrime Victimization

Several criminology studies (Bossler & Holt, 2009; Holt & Bossler, 2009; Marcum, 2008) have applied Routine activity theory framework to the study of crime and criminals in cyberspace despite some criminologist (Yar, 2005; Grabosky, 2001; Newman & Clarke, 2003) contending its applicability to cybercrime. Studies that have applied RAT framework to cybercrime have provided modest and sometimes inconsistent support for its utility in understanding the risks of cybercrime victimization. Overall findings from these studies reveal that engaging in online risky behaviours and activities such as downloading files from unknown websites, opening unknown email attachments and clicking on pop-up messages significantly increase the chances of online

victimization (Marcum, 2008). Simply put, the routine activities of an individual online determines the risk of being a cybercrime victim.

Examining the element of exposure to motivated offenders, previous studies have looked at how one's daily online activities, both legal or illegal, influence their proximity to motivated offenders. As for the element of exposure to motivated offenders, previous research has examined how daily computer activities, both legal and illegal, place individuals in differential proximity to motivated offenders. The evidence does not support the hypothesis that the amount of time spent online increase risk of cybercrime victimization. However, participation in certain online activities and associating with motivated offenders significantly increases the chances of being a cybercrime victim. In applying RAT to online harassment, Holt and Bossler (2009) concluded that the use of computer for playing video games, checking e-mail or shopping did not significantly increase the chances of respondents experiencing online harassment. Rather, the time spent in chat rooms and the use of instant message chat did.

In studying the association between capable guardianship and cybercrime victimization, researchers have categorized guardianship into two: physical and personal. Physical guardianship represents computer softwares that protect computer systems from computer criminals (e.g., antivirus, anti-spyware and firewall programs) whilst personal guardianship refers to an individuals' information technology (IT) skills. With regard to the association between physical guardianship and cybercrime victimization, the evidence is inconsistent. While some studies reveal a negative significant association between computer security (such as anti-virus, antispyware and firewall protection) and the likelihood of experiencing cybercrime victimization (Choi, 2008), others (Holt & Bossler, 2009; Marcum, 2008) have indicated that computer security systems have no influence on cybercrime victimization. The case is similar for personal guardianship as previous

research has found no impact of personal guardianship on the likelihood of cybercrime victimization (Holt & Bossler, 2009; Marcum, 2008).

Throughout its inception, the MOMO system has been plagued by a number of fraudulent activities carried out by fraudsters with the sole purpose of weakening the service's public value and exploiting the systems to their advantage. Scammers or fraudsters perpetrate mobile money fraud on purpose in order to gain an unfair edge over mobile money customers, the service providers, and the various small scale business setups who act as mobile money agents (Subex, 2017; Merritt, 2011). Fraudsters use a well-trained complete act to take advantage of service stakeholders. Scammers plan for a long time and occasionally obtain financial and technical assistance from cartels that profit from system vulnerabilities (Maurer, 2012).

According to Kanobe et al. (2017), mobile money services have enabled the unbanked in developing world to participate in formal financial services. They argue that this situation has arisen as a result of a regulatory system that has encouraged fraudulent activities to flourish. They assessed the administration of mobile money services using an interpretative qualitative method based on Activity Theory (AT), with a focus on information security rules, regulatory papers, and processes. Their studies revealed the causes for the shortcomings in information security management in emerging economies' mobile money services. They also detailed the duties performed by mobile money providers' workers in ensuring the service's information security.

A study by Akomea-Frimpong et. Al, 2019 on "Control of fraud on mobile money services in

Ghana: an exploratory study" found out that service conditions for employees and agents are poor. It was discovered that the majority of the participants (nearly 60%) blamed poor remuneration of personnel and momo agents for mobile money fraud. Employees complain that their salaries and commissions are insufficient, hence in order to survive the economic downturn, they engage in illegal activities to support their take home pay. Between 2012 and 2016, Ghana's economy struggled greatly, causing widespread struggles for its citizens (Ile and Boadu, 2018). According to the findings of the study, poor salary of employees working in the MOMO division causes fraud in mobile money services. According to the respondents, some employees conspired with subscribers and other employees to steal money from mobile money operators on purpose. Employees of mobile money operators collaborate with them to manipulate the systems in order to profit from them (Maurer, 2012; Merritt, 2011).

2.3 Research gap

The introduction of online transactions, particularly mobile banking, has greatly benefited the financial sector. Mobile banking has made it easier to conduct financial transactions between financial institutions as well as between individuals without involving banks. As a result, mobile banking has made banking and life in general a lot easier. Although mobile banking has reduced the stress that consumers face when doing traditional banking, it is clear that some people have taken advantage of the system to commit fraud.

According to the available research, mobile money fraud is very common in Ghana and has resulted in the loss of millions of cedis over the last decade. The studied literature, on the other hand, was focused on the total Ghanaian population, rather than on fraudulent behaviors among

traders. The majority of Ghanaian traders work in the informal sector and are primarily from the lowest socioeconomic strata. It should be noted that traders are one of the most common groups in Ghana who utilize mobile banking in their daily lives, making them more vulnerable to mobile money fraud. As a result, it's a good idea to look at their experiences with mobile money fraud and their exposure to it. The study goes on to look at the many elements that make traders more prone to mobile money fraud.

In addition, the existing literature concentrated on the financial consequences of mobile money fraud for victims. Most literature has disregarded issues such as the impact on victims' businesses as well as their families. As a result, the goal of this study is to find out how mobile money fraud impacts the victims' businesses and their families as a whole, as well as how they can be safeguarded in the future.

2.4 Hypotheses

1. Older adults are more likely to experience defraud than younger adults.

2. Participants with lower education will have higher experiences of fraud than those with higher education.

3. Male participants are more likely to experience defraud compared to Female participants.

4. MTN users are more likely to experience fraud as compared to AirtelTigo users

CHAPTER THREE

METHODOLGY

3.1 Introduction

This chapter presents the quantitative approach describing the study population, sample size, sampling method used, the type of data collection instrument and how the data was analysed. This was followed by the qualitative approach describing data collection instruments, the process through which data was collected and how data was analysed. Specifically, the sequential explanatory mixed method approach was used. Finally, the ethical issues involved in this study was discussed and how these issues were resolved also discussed.

3.2 Research Design

The sequential explanatory mixed method approach was used in the study. In a mixed-method study, "the investigator collects and analyzes data, integrates the findings, and draws inferences utilizing both qualitative and quantitative approaches or methodologies in a single study," (Tashakkori & Creswell, 2007, p.4). In order to address an issue or a research problem, mixed method research typically gathers perspectives from a variety of sources. "To acquire diverse but complementary data on the same issue," Morse (1991, p.122) explained why this type of design was used. Furthermore, it is said that results obtained through the application of two or more procedures are more appropriate and "enhances our conviction that the results are real and not a methodological artifact" (Bouchard, 1976, p. 268).

Thus, mixed methods research draws on the strengths of both qualitative and quantitative research. These two methods bring out the depth and breadth of any study. In a single research study, both qualitative and quantitative strands of data are collected and analysed separately, and integrated

– either concurrently or sequentially – to address the research question. Combs and Onwuegbuzie (2010) assert that mixed analyses involve the use of at least one qualitative analysis and at least one quantitative analysis – meaning that both analysis types are needed to conduct a mixed analysis".

In this study, an exploratory sequential mixed method research design was selected in order to broadly assess knowledge about mobile money fraud and explore victim's experiences. It is a mixed research approach whereby the researcher starts with a quantitative method (collecting and analysing data) and based on the results, selects some respondents for a qualitative study. Data from all participants was analysed using quantitative methods but only participants who have been victims of mobile money fraud were interviewed in the qualitative section. This research design was ideal because, quantitative methods were used to estimate the prevalence of mobile money fraud, to know why and how traders got defrauded and assess the knowledge of traders about mobile money fraud whilst employing qualitative methods helped to get deeper understanding of victims' experiences of mobile money fraud as well as the impact this has had on them.

3.3 Study Area

The study was done at Madina market in the La Nkwantanang Madina Municipal District in the Greater Accra Region of Ghana. It is the second largest market in Accra a with an average of 19,000 visitors per day (La Nkwantananag Municipal Assembly, 2016). According to the Madina zonal council, the Madina market starts from a main bus stop known as Zongo junction and spreads all the way to behind the Madina Police station. Madina market was selected for this study because of the large number of traders that come there every day and the proximity of the market to the University of Ghana. Due to its unique location, traders from all other regions are able to have easy access into the capital to sell their goods.

3.4 Quantitative Method

3.4.1 Study Population

The study population for the quantitative section included all traders in Madina market who had subscribed to at least one mobile money platform. Although most traders were very familiar with using mobile phones and had heard about mobile money, not all of them had registered for the service. For the purpose of this study, individuals who come to the market to buy only were not considered. The rationale behind this was because, many buyers who had fallen victims will not be readily available for a subsequent interview. Again, the study focused on traders who did not only sell in the market but also lived in the Municipal area.

3.4.2 Sample Size

As at march 2020, there were 14.7 million active mobile money accounts according to a Summary of Economic and Financial Data published by Bank of Ghana (Bank of Ghana, 2020). With a population of 29.66 million, 14.7 million mobile money subscribers represent approximately 50% of Ghanaians. Using a confidence level of 95% and assuming the population of market traders (sellers only) to be 600 (based on interactions with Madina zonal council), the sample size was calculated to be 235 using Krejcie and Morgan (1970) formula as follows:

S: Required Sample Size

N: Population size (assumed to be 600)

P: Population proportion (assumed to be 0.5) **X:**

Z statistic for the level of confidence (1.96) **d**:

degree of accuracy (0.05)

$$s = \frac{X^2 NP(1-P)}{d^2(N-1)+X^2P(1-P)}$$

S = 235

Source: *Adapted from Krejcie and Morgan (1970)*

3.4.3 Sampling Technique

Study participants were randomly selected based on the presence of outcome of interest. Traders who were willing to participate in the study were spoken to and had the chance to fill in the questionnaire. With information from the Madina council about the whole area of the Madina market, these randomly selected traders were found all around the Madina market. Most of the traders were excited about the research and happily filled out the questionnaire. Some of the traders also introduced the researcher to other traders who were ready to speak.

3.4.4 Data Sources

There are two categories of data sources: primary and secondary. Primary data sources require that the researcher collects his or her own data for the study. Secondary data sources on the other hand refers to data collected by a third party (such as government agencies, censuses,

surveys, books, journals, websites etc) and made available for researchers to use for their own studies. The primary data sources include observations, interviews and administering questionnaires.

✦ **Observation:** This approach is suitable for studies with fewer study participants because it requires the researcher to observe every study participant in order to obtain the data. With this method, the researcher collects data by just observing respondents without any interview. The information collected usually represents the current situation or occurrence of an event of interest or future intentions of the respondents. In summary, observation is very important because, little details which are usually not captured in questionnaires or even interviews can easily be seen. Data collection which is usually done by observation fall under three main categories. These categories include natural observation, controlled observation and participant observation. In a controlled observation the researcher uses a homogeneous process to watch respondents or the environment whereas in a natural observation the researcher observes the respondents in their natural conditions. However, in a participant observation the researcher observes by becoming part of the group that are being studied. This means of observation has many advantages such as developing a good relationship with respondents.

✦ **Interview**: This is a qualitative method of data collection that seeks to obtain in-depth information about a particular study. Interviews are helpful when researchers seek to gain from indepth data on a relatively small group of people with a focused topic which can better be answered by gaining more knowledge. Very often, interviews are put in two main categories, that is, the structured interviews and the unstructured interviews. Structured interviews include a set of questions and is quite similar to a questionnaire. However, for unstructured interviews, there can

be different questions for each participant and the structure of the interview is dependent on the answers of other questions.

✦ **Questionnaire:** It is a widely used method for collecting quantitative data for research, surveys, census etc. It comprises of a set of questions printed in a structured manner on a form or set of forms. The questionnaire researchers use has to go through a careful procedure to ensure that all relevant information can be collected (Saunders et al., 2008). Again, aside the careful preparation, the researcher has to have a pilot test of the questionnaire to ensure that he/she is on the right path. Once minor inconsistencies have been realized after the pilot test, the researcher, makes the required changes. This is a very important thing to do because quality data can then be collected and little errors can also be avoided (Bickman & Rog, 1993).

3.4.5 Data Collection

Data was collected through a structured questionnaire. The questionnaire captures data on demographics of study participants, their knowledge on mobile money fraud and the general information about mobile money fraud in Madina market. Respondents who can read and write will be allowed to fill the questionnaire on their own whereas respondents who cannot read and write will be assisted to do so.

According to Bell (2005, p. 147), "however pressed for time you are, do your best to give the questionnaire a trial run, as without a trial run, you have no way of knowing whether your questionnaire will succeed". To Saunders et al (2007), the purpose of getting a pilot study done is to test the questionnaire the researcher has developed on a small group of people before the major study. Preliminary questionnaires were developed and administered to ten randomly selected traders to ascertain if the meaning the questionnaires seek to get from the traders were what was

gotten. After this piloting was done, it was seen that, some of the questions had to be added. Again, some of them had to be rephrased as some of the traders found it hard to understand. This process was very important as it brought into light some of the important information the researcher could have missed. There was a questionnaire which was given traders who could read and write to fill out. For traders who could not read and write, the questions were read to them and their various responses were noted down by the researcher.

3.4.6 Method of data analysis

To draw inferences, meaning and conclusions from data collected, data collected from respondents were processed in three ways, namely, coding, data entry and data cleaning. After collection of the data, the closed ended questions were coded as such whiles the open-ended questions were themed for coding since there were varied responses for those questions. After coding, the data was entered into the computer using the statistical package for social sciences (SPSS) software, version 22. Data cleaning was done to identify and correct errors during coding. Errors found were referred back to the questionnaire and rectified accordingly. With the help of the SPSS software, the data was interpreted into univariate and bivariate analysis. At the univariate level, the frequencies of variables were generated to describe the variables. At the bivariate level, the strength of associations between the variables was established using chisquare test of independence and independent t-test. The next section discusses the qualitative approach to the study.

3.5 Study 2 Qualitative approach

3.5.1 Target population

As mentioned earlier, the explanatory sequential mixed method approach is what was used in this study. Therefore, after quantitative data had been collected and analysed, respondents who had fallen victims of mobile money fraud were identified. However, after the collection of the quantitative data, it was seen that three people had fallen victims to mobile money fraud. These victims included two men and one woman. They were aged, 32, 50 and 33 respectively. The various respondents who fell victims to mobile money fraud were the target population for the qualitative study. These respondents now qualified as participants who participated in interviews in order to gather information on their experiences of mobile money fraud as well as the impact mobile money fraud had on them.

3.5.2 Sampling technique

The technique which was used to sample was purposive sampling. Purposive sampling was used for the study due to three main reasons. The first reason was as a result of the type of participants required for the study. These participants were victims coming from the earlier 235 respondents selected for the study. Some participants were conveniently available but were adequate enough for the study. What this means is that, some people were near victims but not exactly victims. People had tried to defraud them but they did not succeed. These people were not spoken to. Again, due to the area which is selected for the study that is the Madina market, participants needed to come from the Madina market and also be a trader. Finally, due to the sample size I used for the study, the participants had to be purposively selected. These victims were purposively identified and then interviewed.

3.5.3 Sample size

Creswell (2014) and Morse (2000) indicate that for qualitative research, the adequate sample size ranges from 3-10 participants. Hence, the sample size which was used for the qualitative research was also be 3 participants. Although with this in mind, the researcher could not really control how many people were going to fall victims. By the end of the quantitative study, coincidentally, the traders had also fallen victims. Also, those who formed part of the sample had diverse backgrounds, educational levels and gender and this sought of ensured full representation and understood which group of people tend to fall victims more.

3.5.4 Data collection procedure

In order to collect data from the participants, an interview guide was made of various questions which were asked, so that all information needed were collected. With the routine activity theory which says that for fraud to take place, a motivated offender (offenders were not identified and interviewed but victims gave information about how offenders managed to get their monies), a suitable target and the lack of a capable guardian were to be available, these questions involved demographics, questions on the offender, the victim, and the aftermath of the incidence. In relation to the victim, the everyday realities in relation to the impact of fraud was sought. Information about how lost money had affected them and the consequences it had in their domestic lives was sought. With permission from respondents, notes were taken of the interview.

3.6 Ethical Considerations

Ethical clearance was sought from the Ethics Committee for Humanities (ECH), University of Ghana. The Ethics Committee for Humanities granted clearance after which data collection

commenced. Also, an introductory letter was obtained from the Sociology Department. According to Creswell and Hanson (2007), research participants have a right to; voluntary participation, informed consent, protection from harm, anonymity, confidentiality, dignity and respect. These ethical codes were upheld to ensure the authenticity of the study and ensure the safety of the participants. All participants and respondents who did not feel like participating in the research were not forced to be part of it. The real names of the victims were withheld. Participants were duly informed about the subject matter of the study and consent was sought from individual participants before any writing was done, this was done to ensure the protection of participants right to privacy. Also, in the course of data analysis, codes were used instead of names or any other information that may make it possible to identify the participant. All information gathered at the end of the study were held in strict confidence by the researcher.

3.7 Covid-19 Protocols

With the ongoing corona pandemic in the country, all safety protocols including wearing of face and nose masks, washing of hands, the use of alcohol-based sanitizer were observed and social distancing was also practiced before data was collected. I wore a face mask and hand gloves and ensured that all respondents were also in their face masks before data was collected. I sanitized my hand after every questionnaire and sprayed every questionnaire with rubbing alcohol before putting it into my bag. For respondents who could fill the questionnaire on their own, they were required to wash their hands or sanitize them before given the questionnaire to fill and were to wash or sanitize their hands again after they are done filling the questionnaire. For respondents who did not have water or hand sanitizers, I provided hand sanitizers for them and ensured that they used it. Again, interviews were conducted face to face but with the maximum required spacing being ensured.

CHAPTER FOUR

RESULTS

4.1 Introduction

This section of the study deals with the analyses, presentation and meaningful discussions of data gathered from the field. The main objective of the study was to examine the factors that influence mobile money fraud among traders in the Madina market. A total of 235 participants were employed for the study. The Statistical Package for Social Sciences (SPSS) was used to analyse the data. This chapter presents analysis of data. Data presented here covers demographic characteristics of participants, duration of network and mobile money usage, fraud and vulnerabilities to fraud.

4.2 Socio-demographic characteristics of study participants

The table below shows the various demographic characteristics of the participants with regards to their gender, age, educational qualification, ethnic affiliation, religion, type of trade. The total number of participants of the study are 235, out of this number, 151 (64.1%) of the sample are males while 84 (35.9%) of them are females clearly indicating that a majority of the traders who participated in this study are males.

With regards to age distribution of participants, it was observed that 85 (36.5%) of the respondents are below 25 years whiles, 72 (30.7%) of the sample fell between the age range of 26-31 years and finally, 77 (32.8%) fell in the 32 years and above group. This distribution informs that, traders in market are very youthful, with most of them being below 25 years. Meaning either

they are supporting their parents at work or have setup a livelihood for themselves. It is worthy to note that this age group are ideally a school going population, thus the distribution from the educational column of the results will determine whether a majority of them are actually schooling, have completed or are dropouts.

With regards to the traders with highest level of education, the results indicate that at the basic level, 7 (3.1%) of the market people have attained at least basic education, whereas, 80 (33.9%) and 112 (47.9%) have completed JHS and SHS respectively. In addition, 32 (13.5%) of the respondents have completed tertiary education, whiles 4 (1.6%) of them have no form of educational qualification at all. This indicates that a vast majority of the market people in Madina have at least attained a basic education. It complements information from the age distribution, because the distribution indicates a youthful population it is only ideal that most of them would have attained up to secondary education, but in this case even some have attained tertiary education

From the distribution, it is observed that the greatest tribal representation were Akans 144 (61.5%), followed by the Gas who were 32, representing 13.5% of the sample, and 28 (12.0%) of the participants who were Ewes. Mole Dagbanes and Guans recorded 26 (10.9%) and 5 (2.1%) participation respectively. The distribution below suggests that Madina market, a township which falls close to the Eastern Region and on a tribal faction makes room for diverse tribes.

Again, from the distribution in Table 2 below, it can be inferred from the type of trade column that majority of the respondents were into the sale of building and household materials, followed by Clothing and accessories 27.6% (65) made up of fabrics, cosmetics, clothes, shoes and bags, jewellery etc. The next group that falls on the distribution, are those who trade in Foodstuff and kitchenware who represented 25.0% (59) of the study population. These products include disposable materials used in the kitchen, bowls and plates, fresh fruits and vegetables,

provisions, grains and so on. Then those who trade in electronics; 16.1% (38) this includes laptops, mobile phones and accessories among many others. The least represented product sold at the market is books and stationery which recorded 2.6% (6).

By virtue of our pre-independence era, the Ghanaian religious space has been significantly influenced. Ghanaians have been identified as very religious generally, because religion defines the moral boundaries of the behaviours of citizens in addition to laws established by the state. From the field data gathered, it was observed that most of the traders at the market are Christians 83.3% (196) followed by Muslims 15.1% (35).

Table 2 Socio-demographic characteristics of participants (n=235)

Variables	Frequency	Percentage (%)
Age (in years)		
Below 25	85	36.20
26-31	72	30.7
32 above	77	32.8
Gender		
Male	151	64.1

Female	84	35.9

Table 1 **continued**

Variables	Frequency	Percentage (%)
Educational Qualification		
Basic Education	7	3.1
Junior High School	80	33.9
Senior High School	112	47.9
Tertiary	32	13.5
No Education	4	1.6
Ethnicity		
Akan	144	61.5
Ewe	28	12.0
Ga	32	13.5
Mole Dagbane	26	10.9

Guan	5	2.1
Religion Christian	196	83.3
Muslim	35	15.1
No Religion	4	1.6
Type of Trade		
Electronics	38	16.1
Clothing and Accessories	65	27.6
Foodstuff and Kitchenware	59	25.0
Books and Stationery	6	2.6
Building Materials	67	28.6

Source: Researcher's Fieldwork, 2020

4.3 Descriptive analysis of Study participants by variables

This section encompasses the distribution of study participants' rating on the various variables such as their mobile networks, duration of usage of such networks, their use of mobile money among others. The distributions are presented in tables below.

4.3.1 Distribution of study participants by mobile networks

The mobile money industry has been sustained by the presence of three main service providers which happen to all be telecommunication companies specifically, MTN, Vodafone and AirtelTigo. They run a system where their customers register for the Mobile Money service and go on to make transactions at their fingertips. In December 2018, the total number of registered Momo accounts in Ghana was approximately 32 million (Bank of Ghana, 2020). However, from the table below based on data gathered from the field, out of 235 registered users, MTN has the largest number of subscribers of 182 representing 77.6% of the participants, followed by Vodafone who has 14.1% (33) subscribers and finally AirtelTigo who have 8.3% (20) subscribers. These statistics affirm the fact that MTN is the largest mobile money service provider in Ghana, probably because it was the first to introduce Mobile Money to Ghana in 2009 (Yu & Ibtasam, 2018). It also informs the distribution of mobile money network subscription in Ghana using traders at Madina market as a test sample. This information corroborates the findings that the total mobile network subscribers by March 2015 was 31,154,420. MTN had 14,207,778, representing 46% of the total customers subscribed then Vodafone with a subscriber base of 7,159,566, representing 23%, and finally Tigo with 4,315,719, (14%) (National Communications Authority, 2015). Airtel, GLO and Expresso recorded 12, 5 and 1 per cent market share, respectively.

Table 3 Distribution of study participants by mobile networks

Network	Frequency	Percentage (%)
MTN	182	77.6
Vodafone	33	14.1
Airtel-Tigo	20	8.3
Total	**235**	**100**

Source: Researcher's Fieldwork, 2020

4.3.2 Distribution of study participants by duration of use of mobile network

Though the population of traders at the Madina market according to the field data is a youthful and very young population, most of them 66.1% (155) have been using their various mobile networks for more than 5 years, with 28.6% (67) found to be using their mobile networks for just a period of 1-5 years and 5.2% (12) of the traders using their network for less than a year as shown in table 4 below. This component of the data is key to findings of this study as it displays that a large number of traders at the Madina market possess some experience when it comes to mobile phone usage.

Table 4 Distribution of study participants by duration of use of mobile network

Duration of use (years)	Frequency	Percentage (%)
Less than 1	12	5.2
1 – 5	67	28.6
Above 5	155	66.1
Total	**235**	**100**

Source: Researcher's Fieldwork, 2020

4.3.3 Distribution of study participants by duration for mobile money usage

Though 66.1% (155) of the traders have used a specific mobile network for more than 5 years, only 38% (89) have used mobile money for above 5 years. Also, from the table above, 44.8% (105) of the total sample have used mobile money for 1-5 years and 17.2% (40) have used mobile money for less than a year. These figures are still inclined towards more years of mobile money usage among traders at the Madina market. However, according to the Bank of Ghana (2020), active holder of mobile money accounts in Ghana in 2018 stood at 13,056,978. This suggests that aside

traders, more Ghanaians have adopted this new financial service as a way of life due to its convenience and ease of access. Thus, there is a need to strengthen security systems surrounding its use and protect the vulnerable from exploitation.

Table 5 Distribution of study participants by duration of mobile money use

Duration of use (years)	Frequency	Percentage (%)
Less than 1	40	17.2
1 – 5	105	44.8
Above 5	89	38.0
Total	**235**	**100**

Source: Researcher's Fieldwork, 2020

4.3.4 Distribution of study participants by purpose for mobile money usage

From the table above, a summary of the data from the field shows that when it comes to purpose of mobile money usage, most traders at the Madina market used the service for sending

and receiving money 43.8% (103). Mobile money operators in Ghana allow subscribers to conveniently transfer money. This can be done by both registered or non-registered user to any destination, within and across platforms by virtue of interoperability. Money can also be sent from abroad to Ghana (Solin & Zerzan, 2010). Then another 15.6% (37) used the service for payment settlements whereas 11.5% (27) used the platform for strict business transactions. From table 6 below, 6.8% (16) used mobile money for business and personal transactions. Also, 11.5% (27) used the platform as a medium for savings because in Ghana, subscribers are permitted to use their wallets as bank accounts where they are able to keep their money. Again, merger between bank accounts and mobile money accounts permits subscribers to send money and receive money while using the account as a savings. Of all the traders who filled the questionnaire, 3.6% (8) of the them used the platform for exclusive personal use. The results further showed that 1% (2) participants used the system for placing bets, 3.1% (7) used it for credit transfer and another 3.1% (7) used it for buying data. From this observation, it can be said that most people prefer the convenience and ease of access when using the service for payments, transactions, staking bets among many others from some few touches on their mobile phones, these are some of the pull factors that keeps attracting people to the service (Au & Kauffman, 2008).

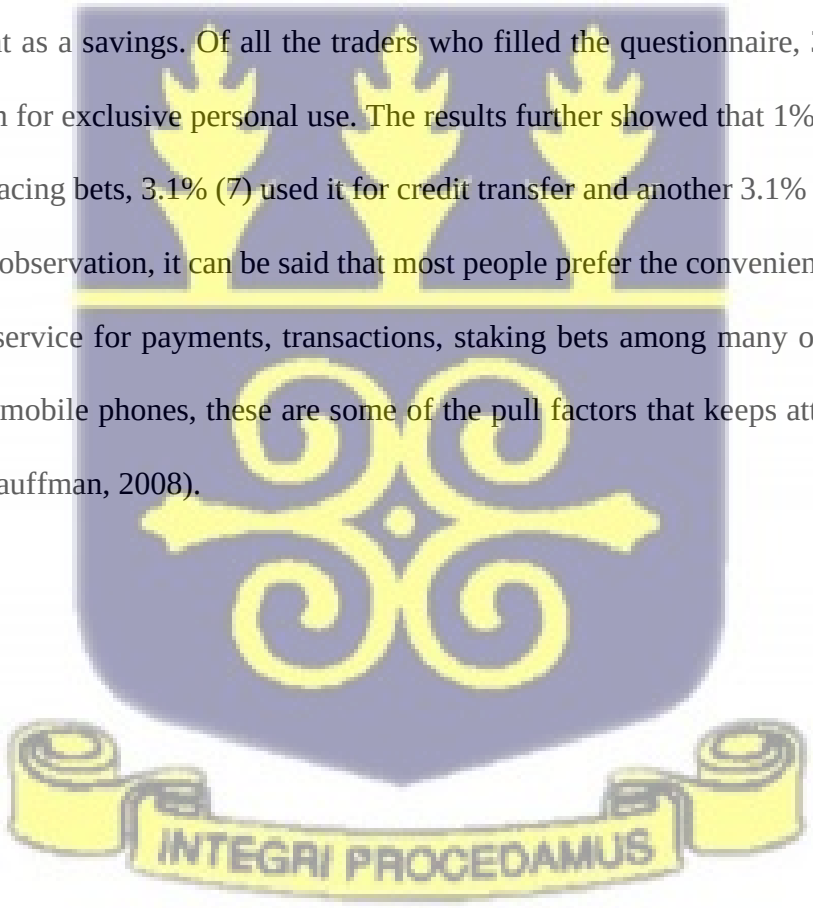


Table 6 Distribution of study participants by purpose for mobile money usage

Purpose of use Payments	**Frequency** 37	**Percentage (%)**
		15.6
Personal use	8	3.6
Business and personal	16	6.8
Send and receive money	103	43.8
Save	27	11.5
Business	27	11.5
Stake bet	2	1.0
Credit transfer	7	3.1

Buying data	7	3.1

Source: Researcher's Fieldwork, 2020

4.3.5 Distribution of study participants by source of knowledge of mobile money fraud

After its launch, the mobile money service has been saturated with a range of nefarious activities by fraudsters whose main purpose is to undermine the good of the service to the public.

From the distribution, most people heard of mobile money fraud through media 59.4% (140) this includes radio, TV and social media applications; then from family and friends 21.4% (50) and finally from personal experiences 19.3% (45).

Table 7 Distribution of study participants by source of knowledge of mobile money fraud

Source	Frequency	Percentage (%)
Media	140	59.4

Family and Friends	50	21.4
Personal Experience	45	19.3

Source: Researcher's Fieldwork, 2020

4.3.6 Why do traders get defrauded?

When participants were asked why Madina traders got defrauded, their responses were that because a high number of them were gullible 30.2% (32) they were more susceptible to such activities. Again, it was reported that greed on the part of some of the victims 24.5% (26) was the reason why they were frauded, 15 (14.2%) of them were clueless as to why whiles 11.3% (12) thought the victims were just careless. A study by Akomea-Frimpong et al (2020) reported, causes of mobile money fraud include, Low public education and training on the core methods of operation of mobile money. In their study, they uncovered that this poor information dissemination was the root cause of why mobile money fraud was on the rise. This is also in line with information gathered from traders at the Madina market. Due to the nature and operations at market, it is difficult or impossible for traders to catch up with advertisements and other forms of education that may be going on in the media. Thus, a participant from Akomea-Frimpong et al (2020) reported to not having an idea of educational information on air.

Table 8 Distribution of study participants by reasons why traders get defrauded

Reasons	Frequency	Percentage (%)
Illiteracy	21	19.8
Greed	26	24.5
Carelessness	12	11.3
Gullible	32	30.2
No idea	15	14.2

Source: Researcher's Fieldwork, 2020

4.3.7 How do traders get defrauded?

It can be observed from the table above that 55.8% (24) of the participants reported that the mode of mobile money fraud was through a prank call, whiles 13.9% (6) gave out their pins. Also, 9.3% (4) of the participants alluded to a fake SMS while 0.5% (1) of the participants alluded to a fake promotion and another 1 (2.3%) sent money wrongly. However, 7 (16.3%) could not remember what exactly happened when they were frauded.

Table 9 Distribution of study participants by how they got defrauded

Mode of fraud	Frequency	Percent Frequency
Sent money wrongly	1	2.3
Gave pin out	6	13.9
Alluded to a prank call	24	55.8
Alluded to a fake SMS	4	9.3
Alluded to a fake promotion	1	2.3

Cannot remember	7	16.3

Source: Researcher's Fieldwork, 2020

4.3.8 Why are traders target of mobile money fraud?

The table below shows us information on the factors that make an individual to mobile money fraud. It is observed that, most people confirmed that ignorance 32.3% (76) was the leading factor followed by poor service from network providers 15.1% (35) then, the fact that some market women are illiterates 14.6% (34) that is why they are more likely to be targeted. In addition, 10.4% (20) people attributed it to the fact that there is generally poor education about the service whiles 7.3% (17) people attributed it to the type of business the traders run, and 13 (6.8%) said it was because victims showed their pincode to others. From table 10 below, 6.8% (12) participants were clueless about the factors that lead to fraud, whiles 3.6% (8) participants said it was because people were constantly making transactions. Again, 2.6% (6) participants reported that the victims were just greedy whereas 1.6% (4) and 0.5% (1) participants respectively said it was due to carrying large sums of money in their wallets and finally that it could have been anyone.

Table 10 Distribution of study participants by reasons why they are targets for mobile money fraud.

Reasons	Frequency	Percentage (%)
Greedy individuals	6	2.6
Illiterates	34	14.6
Ignorance	76	32.3
Poor service from network providers	35	15.1
The type of business being run	17	7.3
Showing your PIN code to others	16	6.8
Poor education about the service	24	10.4
People with huge sums in their wallets	4	1.6

People constantly transacting	8	3.6
Anyone can be a target	1	0.5
I do not know	12	5.2

Source: Researcher's Fieldwork, 2020

4.4 Hypothesis Testing

4.4.1 Hypothesis 1 - Older adults are more likely to experience defraud than younger adults.

Chi-square was used to test the hypothesis that older adults are more likely to be defrauded than younger adults. Results of this test show that almost all the participants regardless of their age said no to ever being frauded before. Majority 36.6% (86) of the respondents who fell below age 25 followed by people above the age of 32 years responding Yes 1.7% (4) and No 31.6% (73) and finally, 30.64% (72) between ages 26-31 years reporting No. This explains the relationship between the variables, however, was not statistically significant. Therefore, the hypothesis was supported.

Table 11 Chi-square test of independence comparing age and personal experience of fraud

	Defrauded through Mobile money			
Age (years)	Yes	No	Chi-square	P-value
Below 25	0	86 (36.60%)	6.240	*0.044
26 - 31	0	72 (30.64%)		
32 above	3 (1.70%)	73 (31.06%)		

*P-value < 0.05

Although, the hypothesis was supported, it is seen that, three people who were above the age of 32 fell victims to mobile money fraud. Of this number, one man who was 50 years old had actually fallen a victim twice. He was the oldest victim and others can relate his age to the number of times he was defrauded.

4.4.2 Hypothesis 2 – Participants with lower education will have higher experiences of fraud than those with higher education.

In testing to find which educational group had been defrauded through MM before, a Chi-square test of independence comparing level of education on personal experience of fraud. From the table displaying the results it can be seen that majority 47.23% (111) of the respondents responded No and they were SHS holders, whiles 33.19% (78) and 13.19% (31) who responded No were JHS and Tertiary holders respectively. Finally, 3.4% (8) who are Basic School level educated and 1.7% (4) who had no education all reported no. With the p value, being above 0.05, the hypothesis that people with lower education are more likely to be defrauded than people with higher education was not supported.

Table 12 Chi-square test of independence comparing level of education and personal experience of fraud

	Defrauded through Mobile money			
Age (years)	Yes	No	Chi-square	P-value
No education	0	4 (1.70%)	1.16	0.885
Basic School	0	8 (3.40%)		
JHS	1 (0.43%)	78 (33.19%)		

SHS	1 (0.43%)	111 (47.23%)
Tertiary	1 (0.43%)	31 (13.19%)

*P-value < 0.05

It can be seen from the test above that the hypothesis was not supported. However, a critical look at the data indicates that one person who had fallen victim acquired only basic education (JHS). Another victim had completed senior high and the last victim had completed tertiary education. These varied levels of education indicate that, people can fall regardless of your level of education. However, other factors can also be involved in making an individual fall victim to fraud.

4.4.3 Hypothesis 3 – Male participants are more likely to experience defraud compared to Female participants.

The results from the Table show that the mean difference between males and females were statistically insignificant [t (233) = 0.72, p > .05]. Therefore, the hypothesis that "males are more likely to be frauded compared to females" was not supported.

Table 13 Independent t-test comparing males and females on personal experience of fraud

	Gender	N	Mean	Std Dev	df	T	P-value
Personal experience of fraud	Male	151	7.84	0.92	233	0.72	0.47
	Female	84	7.93	0.91			

*P-value < 0.05

Although, the hypothesis was not supported, it can be seen that out of the three victims of mobile money fraud traders in the Madina market, two of them were male and one was female. Perhaps, if the number of victims were high, there could have been a clearer picture of which sex falls victims more. However, with the current data, two males fell victim with only one female falling victim.

4.4.4 Hypothesis 4 – MTN users are more likely to experience fraud compared to AirtelTigo users

The results from the Table show that the mean difference between MTN users and AirtelTigo users were statistically insignificant [t (200) = 0.64, p > .05]. Therefore, the hypothesis that "AirtelTigo users are more likely to have experienced fraud compared to MTN users" was not supported.

Table 14 Independent t-test comparing MTN users and AirtelTigo users on personal experience of fraud

	Gender	N	Mean	Std Dev	df	T	P-value
Personal experience of fraud	MTN	182	1.98	0.14	200	0.64	0.5246
	AirtelTigo	20	2.00	0.00			

*P-value < 0.05

All three individuals who had fallen victims of mobile money fraud explained that they used MTN.

4.5 Summary of Findings from Quantitative Analysis

The findings from the study are spelled out as follows:

1. Age is a determiner of likelihood to experience fraud.
2. Education is not a determiner of likelihood to experience fraud
3. Gender is not a determiner of likelihood to experience fraud.
4. Network usage has no bearing on likelihood to experience fraud.

4.6 Findings for Qualitative study (study 2)

In order to fully understand the factors that make traders susceptible to fraud as demonstrated in the quantitative study (study 1), a qualitative study was conducted to provide more information about traders' experience of fraud. The qualitative data was analysed using thematic analysis. Thematic Analysis was employed in analysing the response provided by the participants who were interviewed in their various conducive environments to ensure privacy and confidentiality. Three major thematic areas were developed from these interviews including subthemes. The themes are experience of fraud, impact of fraud and security measures. These themes are discussed with subthemes and supported with verbatim quotations from participants in the below paragraphs.

4.6.1 Experience of Fraud.

This theme highlights the general experiences of some participants who have been duped via mobile money. The overarching theme of experience was informed by subordinate themes such as frequency, fraud process, precaution, amount lost and filing of report. When deepening into the analysis of the experience of the victims the following was found.

Frequency: The respondents in this study demonstrated an understanding of what it means to have been a victim of fraud and were also able to identify the number of times it happened. Majority of the participants (*n*=2) reported that they had been victims of fraud just once, while one participant had experienced it on two occasions. According to the participants, they were caught off-guard as they were very active and going about their normal businesses before they experienced the fraud.

One participant gingerly expressed his disappointment of being a victim of fraud and responded as follows:

> *"Oh, me this year naaaaaaa somewhere around March there… Ei after that time I will never allow anyone to even try (laughs) I would rather die. I have been caught once" (Participant q27, 32 Male)*

Just like the first participant, participant 2 proved to know what it means to be defrauded. He has experienced this on two occasions and seemed to be very distraught about the experience to the extent that the fraud has compelled him to stop using mobile money. He had this to say:

> *'Six months ago, this 2020… I don't use it anymore but back then I used to keep money on it… I have faced this problem twice' (**Participant q46, 50 Male)***

This brings up a nuanced discussion in relation to the quantitative data which was initially collected. From the quantitative data retrieved, it was seen that, some traders believed that the

lack of formal education was one of the factors that led to one being a victim of fraud. However, looking at the three participants who fell victim, they all had formal education and it can hence be argued that, although traders had a different belief about why they got defrauded, these three also present a different scenario. Also, just one out of the three had gone through the experience twice.

Fraud process: It was established from the data gathered from the interviews that all participants (n=3) did not suspect foul play during the process of being defrauded. Some had complete trust in the process with the assumption that nothing could go wrong. It was also realised that the trickery was easily done based on the method employed by the scammers.

For example, one participant who is a trader lamented how she was duped via the following statement:

> *"oh, the person called me. He called and said that they had not received payment for the goods I was buying so I thought it was one of my suppliers that give me goods o. so I sent him the money" (Participant q121, 33 female).*

Some participants reported that they were defrauded while performing mobile money transactions. This normally happens without suspecting any foul play, thereby having a complete trust in the process with the assumption that nothing could go wrong. One participant explained how he was scammed while using the mobile money transaction for bet.

He said:

> *"I usually bet, so I saw a page on Instagram who give correct predictions to football scores but I sent them the money and they did not give me the prediction." (**Participant q27, 32 Male).***

Linking this to the routine activity theory, it is seen that a suitable target and a motivated offender are two of the three requirements needed for fraud to occur. All these victims had offenders who were highly motivated to take their monies. Although none of these victims knew who the perpetrators were, it can be assumed especially for the woman who wrongly sent money to the scammers that this offender had been listening to her conversations and knew that she was to send some money to her suppliers. The offender took advantage of that and made the call earlier than the real supplier. In the case of participant two, who sent money for his bet to be predicted, the offender had an Instagram page claiming to giving out correct predictions for football matches. Once this man sent his money, the owner of the account just blocked him on Instagram. It can also be seen from the quantitative data that although 2.3% of traders believe individuals will usually send money wrongly, 55.8% believed that most victims will allude to prank calls.

Precaution: The researcher probed to see if there were any suspicions before they got defrauded and if it aroused any alarm in the participants. The responses of the respondents were indicative of the fact that they had no idea that they were being defrauded and as such they took no precaution at the time of the mishap.

One participant said;

"I didn't discuss with anybody because I knew I had to pay my suppliers some money so I just sent it". (*Participant q121, 33 female*)

The participants were so sure of themselves they had not been extra careful. As seen in from the routine activity theory, a suitable target refers to any vulnerable individual that indirectly makes himself or herself available and accessible to the offender. These three victims were

perfect targets as they unconsciously availed themselves to these offenders. They had so much confidence in what they were doing and trusted these highly motivated offenders who then took advantage of them.

Filing report: Another subtheme which run across the participants was that of filing report after being defrauded. All participants admitted to reporting the incident either to the police or their network providers. However, each of the participants concluded that no help was offered to them as their issues were unable to be resolved.

One participant said;

"oh, when it happened me, I went to the Darkuman police station to go and report what had happened to them because I know when stuffs gets stolen, we report to the police ...they didn't do anything, nothing" (*Participant q121, 33 female*)

All the victims had made sure they reported to the right authorities. However, it can be seen above that none of them were truly satisfied with the results. This again brings us to the third element of the routine activity theory which is the capable guardian. In this case not only did the authorities not protect them but they were not able to identify the perpetrators and get their monies for them.

4.6.2 Impact of fraud

This theme focuses on the various impacts mobile money fraud had on the participants. The subthemes that emerged under this theme were the experience of emotional pain, and loss of money.

Emotional pain: Individuals process events differently. What was evident, though, was that all participants experienced some amount of emotional pain as a result of being defrauded of their heard earned income. One participant said;

> *"It pains me o. But it did not affect my finances like that because first of all it was a bet so all could have lost just that I felt bad that someone take my money free like that k3k3" (Participant q27, 32 Male).*

Being deprived of one's savings or bills for hospital care can be quite devastating for people. As seen in the literature, some may be tempted to take their own lives or venture into theft to cover the cost incurred for being scammed. Participant 2 expressed his feelings saying;

Loss of money: Falling a victim, to mobile money fraud did made these victims lose their money in addition to the emotional pain to them. These monies that were lost had different purposes. This ranged encompassed monies allocated for fees and business. A 50-year old man complained that part of the money that was taken from him was meant to pay his hospital bill.

He lamented thus;

> *"it affected me because it was for check-up and I wanted to take it out and add some to it so I go the hospital the following Monday. It happened on a Sunday you see. Since then that I missed that check-up I haven't been able to go again for it"*
>
> ***(Participant q46, 50 Male)***

Some of the participants also indicated that the money they lost was meant for their businesses as well as the payment of their wards' school fees. A 32-year-old man who had been

defrauded just once explained that "*the money was for payment of my son's school fees*". Another participant expressed that the money she lost to the scammers were meant for her business and her loss has had a negative impact on her business. She had this to say:

"it was for my goods, to buy some clothes as well as money for my work.''

(Participant q121, 33 female)

5.2.4 Security measures.

With the alarming increase in fraud cases, both security and service providers attempt to curb the ever-rising mobile money fraud by placing in certain checks. However, participants did not know of any such checks and also did not think the police or network providers are very helpful in fighting this canker and such have to rely on themselves to fight fraud. Subthemes such as post-fraud precautions and activities of service providers emerged under this theme.

Post- Fraud precautions: Participants explained that after being defrauded, they have resorted to being extra alert in their dealings. Some also initially decided to quit using the mobile money services. One participant said;

"Oh from that time if I have to use Momo to pay for something I make sure that I receive the thing before I use the Momo to pay koraaa. If I don't see I don't pay or send you anything as for prediction dieeer forget" (Participant q27, 32 Male).

Some of the participants were of the opinion that the police or network supplies were not very helpful in battling this canker and that they had to rely on themselves to tackle fraud. Thus, participants themselves had to rely on their own strategies to make sure that they do not fall victim to these fraud acts again. Some participants revealed that they had taken to extra

alertness in their dealings after being defrauded. To some, they had stopped using mobile money services entirely. One participant had this to say:

> *"I do receive but I do not keep it for long for long because I do not know when it will disappear from it. I personally do not do any transactions on it at all''* (***Participant q46, 50 Male***).

With the unparalleled increase in cases of fraud, both security and service providers are attempting to curb the ever-increasing mobile money fraud by placing such checks. All the participants were of the opinion that it was not very beneficial for the police or network supplies to combat this canker and that they had to rely on themselves to counter fraud. One participant said:

> *"mmani dah)''(I am very alert) I don't think it will happen to me again.''* **(*Participant q121, 33 female*).**

Inadequate effort from service providers: Most of the service providers try the best to protect their clients from being defrauded. According to the participants, however, they do not think the service providers are doing their best in curbing this crime. Some participants went ahead to blame the service providers for allowing this to happen. One participant who expressed her disappointment in MTN said:

> *"nothing. 'm3di MTN ho yaw (I am disappointed in MTN)'. It pained me nso"*
>
> *(Participant q121, 33 female)*

Another also was of the view that since it mobile money fraud is still ongoing, then not much is being done about it. He said:

> *"For me no I don't think so because these people keep doing it to plenty people so I*

wouldn't know" (Participant q27, 32 Male).

According to participant two, he did not think that service providers are doing their best to curb this criminality. He suggested that network providers must laisse with the police in order to reduce how rampant this crime is. He went further to blame the service providers for this criminality. He expressed his dissatisfaction by saying that:

*"they can put things in place because me I surely suspect some of the fault is from their office as well… I think if the police deal with their tracking systems so that just like I have gone through this someone else would not need to pass through the same thing as well. I'm not the only one suffering. People are suffering as well." (**Participant q46, 50 Male**).*

All the victims saw the service providers as their main guardians to not only protect them but to help them find the fraudsters. This clearly indicates that they were all able to fall victims because they lacked that suitable guide at the point, they needed them the most. This was both before and after their incidences.

Themes	**Subthemes**
Experience of fraud	Frequency
	Fraud process
	Precaution
	Filing report
Impact of fraud	Emotional pain
	Loss of money

Security measures	Post-fraud precautions
	Inadequate effort from service providers

Conclusion of findings

Integrating the findings of the two studies, quantitative study revealed that gender, educational background and type of network are not determiners of who becomes victims of mobile money fraud. Similar results were found in the qualitative study as no differences were found. Further, the quantitative study shows the occurrence of mobile money fraud, however, the qualitative study establishes the psychological distress and impact that being defrauded has on the victims.

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter concludes the research by restating the purpose of the study, summarizing its main findings; whether they supported the hypothesis; or differed from it. It also looks at what other researchers found and descriptions for the results are provided. Limitations of the study are also outlined in this chapter as well as the repercussions of the findings. Finally, recommendations for future study and practical applications are outlined.

5.2 Main Findings of the Quantitative Study

5.2.1 Factors that influence mobile money fraud among Madina market traders

One objective of the study was to explore the factors that influence mobile money fraud among the Madina market traders. A series of chi-square analyses were conducted. Hypothesis one, which posited that older adults would be more susceptible to being defrauded than younger adults was not supported by the data. Results from the study showed that 36.60% of the respondents who fell below age 25 followed by people above the age of 32 years responding Yes 4(1.70%) and No 73(31.06%) and finally, 72(30.64%) between ages
26-31 years reporting 'No' to having been defrauded.

From the current research, it was found that both young and old were equally vulnerable to being victims of mobile money fraud. As affirmed by Shao et al., (2019) older adults are often victimized when it comes to being defrauded. Lichtenberg et al., (2013) are of the view that this is the case because of the presumed psychological vulnerability of older

adults. As a result of this assumed vulnerability, it makes them easy targets of monetary fraud. However, the findings from this study differ from what exits in literature, in that, both the young and old are defrauded equally without any statistically significant differences. Ideally, it would have been expected that more of the older generation should be defrauded than younger ones. This is because of the novelty of this cashless system and the fact that young ones are more tech savvy than older individuals. However, the data and available literature expresses a different opinion. This could be as a result of the fact that both age distinctions have not been properly oriented on the use of Momo or some of the common tricks used by fraudsters. Thus, adequate education on the system as well as sensitization programs on fraudulent practices will be needed for the populace. This will go a long way to help curb the rampant fraudulent acts from the system, allowing for subscribers to freely use the system without fear and devoid of risk of losing money to fraudsters.

Also, concerning gender differences, the hypothesis that females are more likely to be defrauded than males was unsupported by the current study. The current study found no statistically significant difference between male and female adults and which group is more likely to be victims of fraud. Considering that most traders in the Madina market are women, it was expected that they would experience it more than men would, however, that was not the case as per the current study. Whilst the researcher's hypothesis was unsupported, Jegede et al., (2016) conducted in a study in Nigeria and found out that not only are women not more susceptible than men, but women are also just as involved in fraudulent activities as men are. This contradicts the findings of this study and begs the question as to why both gender were equally susceptible to fraud. Outside the argument that the participants belong to specific gender, the underlying factor or similarity between both groups is the fact that they are actively engaged in performing sales and keeping records regularly. Once they have a divided attention, this sets them up easily for fraud, especially because they may not have the time and patience

to verify transactions or confirm the stories the fraudsters make in order to get individuals to send them their money or release their pin codes. In an interview with Karen Webster, "Stephen Ritter, chief technology officer of Mitek, said that "it's unfortunately very common that the fraudsters take advantage of moments of weakness. They try to achieve what they want to achieve when people are distracted" (PYMNTS, 2020). In addition to the above, the hypothesis that males are more likely to be knowledgeable about mobile money fraud compared to females was not supported, the data suggests that both male and female were equally knowledgeable about mobile money fraud.

Furthermore, the hypothesis that people with lower education are more likely to be defrauded compared to people with lower education was not supported by the data. As seen from the results, 47.23% of the respondents responded *No* to having been ever defrauded and they were SHS holders, whiles 33.19% and 13.19% who responded *No* to being defrauded were JHS and Tertiary holders respectively. Finally, 3.40% who are Basic School level educated and 1.70% who had no education all reported *No* to being victims of fraud. The assumption of the researcher that people with higher educational levels would easily spot a potential act of fraud much quicker than an individual who is not very highly educated proved to be untrue. The findings suggest that no matter one's educational pedigree, one is just as likely to be a victim of mobile money like any other person. According to Button et al (2014), due to the small amount of money normally demanded by scammers, online victims fall prey to scams several times. Usually, some scammers will ask for just a small sum of money and this will distract the victim from really realizing they are falling prey to a scam. Owing to the type of smart strategy embraced by these fraudsters, some often fall victim to these scams. Again, the amount of information shown by scammers makes it easy for individuals to fall victim to cyber fraud. As well as loopholes found in some of these schemes, some of these scammers know every detail about how the system operates. As a consequence, it becomes very difficult for the victim to

detect the possibility of fraud in their response when showing their wealth of knowledge. Ideally, it would be expected that highly educated people would be more cautious and easily spot these tactics used by scammers. However, the current research shows that higher education levels do not guarantee that one would spot such acts and thereby, leaving the individual just as vulnerable.

The above findings are supported by the victimization is the routine activity theory (RAT) which propose that various forms of crime, especially cybercrime can only occur with the right opportunity given in relation to time and space. As seen from the findings, being a victim of cybercrime has little to do with social factors, instead, it appears to occur based on technological inventions and the tact employed by offenders. As established from the quantitative results, age, education, gender and network type were all non-significant contributors.

5.3 Discussion of qualitative findings (Study 2)

This study particularly found that individuals do not suspect any foul play when being defrauded hence they become less suspicious and take less precaution. From the data gathered, it was quite evident that the participants interviewed were despondent about being scammed. However, those who were scammed just once were not as devastated as the participant who was scammed on two separate occasions. In line with the above, the fraud process often predicts the number of times an individual can be defrauded. It can be hypothesized that, one method of being scammed will scarcely work on the same victim twice. Mobile money is considered an online mode of transaction and the online method contributes to the process of fraud. Paying attention to details acts as a shield against fraud. Participants expressed their disappointment for not initially taking the step to authenticate the veracity of the messages they received. As explained by Button et al (2014), victims are preyed upon because of the benign requests of

the scammers. This foot-in-the-door approach serves as a ruse to take away the attention of the victims. After failing to take precautionary measures, victims of mobile money fraud then report to the police or the network service providers, an act which further exasperates them because, as in the case of these participants, most of the issues are unable to be resolved by the police or service providers. As in the case of the current study, Cross (2015) reported that in Europe and America, less than one-third of victims report fraud cases and this is because of victim blaming (Cross, 2015). This frustration experienced forms the basis for the next major theme of impact of fraud. Also, the findings revealed that mobile money fraud causes emotional pain as well as the loss of money to the victims. Fraud and scams affect people emotionally and mentally. This could come in the form of anxiety, shame, embarrassment, guilt, anger and loss of trust in people.

Participants in this study complained bitterly and emphasised that they were 'pained' by the occurrence. This finding is consistent with previous studies. For instance, Tade and Adeniyi (2017) point out that victims of ATM fraud in Nigeria appear to have experiences post-fraud trauma, where victims have had a hard time bouncing back to their former selves, particularly when they have planned money that has been stolen from them. Some victims commit suicide in extreme cases where victims cannot tolerate the harsh repercussions of being defraud (Cross, 2015). When a person is scammed, harm has always been done and it always seems like you can't do anything. Most of the time, the scammers cannot be identified, and people do their best to shield themselves from more financial or legal damage. It should be emphasized that the financial losses of fraud on victims add to the psychological trauma the victims go through. This finding corroborates existing literature. For instance, Cross et al. (2016) demonstrated that online fraud victims suffer significant financial and other losses, resulting in annual losses to the point where the financial impact of fraud, as well as the

emotional, psychological, interpersonal, and physical effects of their victimization, become unbearable.

Finally, the findings suggest that service providers have not done enough to combat the mobile money fraud menace. It is possible that some of the employees of the service providers have poor services conditions hence they connive with the scammers to engage in the mobile money fraud. Consistent with previous study, Akomea-Frimpong et al. (2020) reported that, some staff of service providers conspire with subscribers and other employees to steal money from mobile money carriers on purpose. Employees of mobile money operators collaborate with them to abuse the systems in order to profit from them (Maurer, 2012; Merritt, 2011). Some mobile money carriers and their agents have very inadequate internal procedures and financial controls, as well as insufficient oversight from top management to the lowest-ranking employee. Due to the weak and obsolete IT infrastructure used to regulate mobile money transfers, fraudulent practices are flourishing. According to the Routine Activity Theory (Felson & Lawrence, 1979), crime is likely to be committed when three situations meet in space and time: motivated offender, suitable target, and absence of a capable guardian. Therefore, when employees experience bad conditions at the workplace, they become motivated to curb such unfavorable conditions through fraud. Hence, the subscribers become the suitable target since most of them least suspect fraudulent activities especially from employees of service providers. These conditions coupled with poor supervision from top management level opens the doors to scammers to take advantage of subscribers.

5.4 Limitations and recommendations.

The research performed was carried out to the best of the researcher's knowledge, but was not without limitations from the research's conceptual, data collection, interpretation and results portion. Those restrictions are as follows: The research participants were sampled from

Madina alone but failed to touch on other areas and as a result, the findings on this current study cannot be generalized since traders of other locations areas were not included. It is difficult to infer and generalize the discrepancies found in the different variables in relation to gender, as a result of the unequal representation of male and female participants in the sample.

From the qualitative study, it was realised that PIN sharing is one way which opens one up to being scammed. It is recommended that service providers set up password age criteria to allow users to update their passwords on a quarterly basis. This must also be authenticated by answering questions of personal identity. Also, proposed that service providers should increase education on mobile money fraud. Constant messages must be sent to customers to keep them vigilant and also to serve as a reminder on why they should be alert and look out for any irregularities in the accounts. Future researchers could look at inter-market prevalence of mobile money fraud in Ghana. Also, specific features similar to reported cases of mobile money fraud can be examined.

5.5 Implications

The study has practical implications for sociologists and service providers. The findings suggest that mobile money fraud victims do not differ in terms of gender and educational background. This will therefore inform service providers to broaden the scope of mobile money fraud awareness campaign to include people from diverse background and across all age groups. As older people appeared to be more susceptible to mobile money fraud, it is imperative that campaign about mobile money fraud be intensified among that cohort.

Again, service providers are required to improve on their services. It is evident through this study that most subscribers have inadequate knowledge on some of the activities that make them susceptible to fraud. Therefore, it is incumbent on service providers to strengthen their mobile money security in terms of pin and other strategies that will curb the mobile money

fraud menace. Upgrading the security of service providers will increase the confidence subscribers have in them.

5.6 Conclusion

Mobile Money, (MM) as it is wide known is an electronic method of transaction that has bridged the accessibility gap which excluded people from rural and remote areas from the banking system. The current research work looks at the holistic approach to mobile money security and scrutinizes how prevalent it is among traders in Madina, and also examines how knowledgeable traders are in mobile money fraud. It also looked at the measures put in place by victims to prevent fraud. The study has demonstrated that from the quantitative study showed that demographic variables such as gender, age, educational level and type of network does not play a significant role in making one susceptible to mobile money fraud. However, it has been demonstrated through this study that fraud causes emotional pain and financial losses on the victims. Despite these grave impacts of fraud, it is clear that victims do not see the efforts that have been put in place by service providers to curb these fraudulent activities. Thus, mobile money fraud is a canker which sullies the smooth patronage of this mode of transaction. Hence, network providers must find alternative and innovative ways of curbing or reducing this menace of mobile money fraud.

REFERENCES

Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency. *Criminology*, *30*(1), 47–88. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

Akers, R. (1973). *Deviant behavior;: A social learning approach*.

Akers, R. L. (1998). *Social Learning and Social Structure: A General Theory of Crime and Deviance*. *By*. Boston: Northeastern University Press.

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., & Dwomoh-Okudzeto, Y. (2020). Control of fraud on mobile money services in Ghana: an exploratory study. *Journal of Money Laundering Control*, *22*, 300–317. https://doi.org/10.1108/JMLC-03-2018-0023

Annan, F. (2017). Fraud on Mobile Financial Markets: Evidence from a Pilot Audit Study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3049376

Asongu, S. (2015). The Impact of Mobile Phone Penetration on African Inequality. *International Journal of Social Economics*, *42*, 706–716. https://doi.org/10.1108/IJSE-11-2012-0228

Au, Y., & Kauffman, R. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic*

Commerce Research and Applications, *7*, 141–164. https://doi.org/10.1016/j.elerap.2006.12.004

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191.

Bank of Ghana. (2017). *Impact of Mobile Money on the Payment System in Ghana: An econometric Analysis.*

Bank of Ghana. (2020). *Summary of Economic and Financial Data*. www.bog.gov.gh

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Computers in Human Behavior*, *50*. https://doi.org/10.1016/j.chb.2015.04.024

Bell, G. G. (2005). Clusters, networks, and firm innovativeness. *Strategic management journal*, *26*(3), 287-295.

Bergh, C., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science*, *7*, 5. https://doi.org/10.1186/s40163-018-0079-3

Boyd, C., & Jacob, K. (2007). *Mobile Financial Services and the Underbanked: Opportunities and Challenges for Mbanking and Mpayments.*

Bouchard Jr, T. J. (1976). Unobtrusive Measures: An I nventory of Uses. *Sociological*

Methods & Research, *4*(3), 267-300.

Burruss, G., Bossler, A., & Holt, T. (2012). Assessing the Mediation of a Fuller Social Learning Model on Low Self-Control's Influence on Software Piracy. *Crime &amp Delinquency*, *59*, 1157–1184. https://doi.org/10.1177/0011128712437915

Busuulwa, B. (2016). *Mobile money fraud, crime rate increase in Uganda*. www.theeastafrican.co.ke/business/Mobile-money-fraud-and-crime-rate-increase-in-Uganda-/2560-3415786-quaydf/index.html/

Button, M., McNaughton Nicholls, C., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, *47*, 391–408. https://doi.org/10.1177/0004865814521224

CGAP. (2017). *International Funding for Financial Inclusion: Key Trends and Developments BRIEF*. http://www.cgap.org/sites/default/files/Brief-International-Funding-for-Financial-Inclusion-Dec-2017.pdf

Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of information, Law and Technology*, *1*(1), 1-20.

Choi. (2008). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

Clarke, R. V. (2018). *The Theory and Practice of Situational Crime Prevention*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190264079.013.327

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Combs, J., & Onwuegbuzie, A. (2010). Describing and Illustrating Data Analysis in Mixed Research. *International Journal of Education*, *2*. https://doi.org/10.5296/ije.v2i2.526

Creswell, J. W. (2014). *A concise introduction to mixed methods research*. SAGE publications.

Creswell, J. W. and Hanson, W. E. (2007). Qualitative research designs: Selection and implementation. *The counseling psychologist*, *35*(2), 236-264.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*. https://doi.org/10.1177/0269758015571471

Daily Guide Network. (2019). *Momo fraud- How scammers steal your money*. News Article. https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Momo-fraud-Howscammers-steal-your-money-791051

Demombynes, G., & Thegeya, A. (2012). *Kenya's Mobile Revolution and the Promise of*

Mobile Savings.

Diniz, H., Alburquerque, J., & Cernev, K. (2011). Mobile Money and Payment: A literature review based on academic and practitioner-oriented publications (2001-2011). *Proceedings of SIG GlobDev Fourth Annual Workshop*.

Donchev, D., Vassilev, V., & Tonchev, D. (2021, September). Impact of False Positives and False Negatives on Security Risks in Transactions Under Threat. In *International Conference on Trust and Privacy in Digital Business* (pp. 50-66). Springer, Cham.

Donner, C., Marcum, C., Jennings, W., Higgins, G., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, *34*, 165–172. https://doi.org/10.1016/j.chb.2014.01.040

Eck, J. E., & Clarke, R. V. (2019). Situational Crime Prevention: Theory, Practice and Evidence. In *Handbook on Crime and Deviance*. (pp. 355–376). https://doi.org/https://doi.org/10.1007/978-3-030-20779-3_18

Edinyang, S. D. (2016). The significance of social learning theories in the teaching of social studies education. *International Journal of Sociology and Anthropology Research*, *2*(1), 40-45.

Eze, U. C., Gan, G. G. G., Ademu, J., & Tella, S. A. (2008). Modelling user trust and mobile payment adoption: a conceptual Framework. *Communications of the IBIMA*, *3*(29), 224-231.

Felson, M., & Lawrence. E. C. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Fetters, M., Curry, L., & Creswell, J. (2013). Achieving Integration in Mixed Methods Designs-Principles and Practices. *Health Services Research, 48*, 2134–2156. https://doi.org/10.1111/1475-6773.12117

Githui, D. (2011). Mobile money transfer in Kenya: an ethical perspective. *Research Journal of Finance and Accounting*, *2*(2), 152-160.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime.* Stanford University Press.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles?. *Social & Legal Studies*, *10*(2), 243-249.

GSMA. (2008). *Brief History of GSM & the GSMA.*

GSMA. (2013). *The Mobile Economy 2013*. ATKearney. Http://Gsma.Com/Newsroom/Wp-Content/ Uploads/2013/12/GSMA-Mobile-Economy-2013.Pdf.

GSMA. (2017). *2017 State of the Industry Report on Mobile Money*.

Harris, J. Ile, I. and Boadu, E.S. (2013). *Representation theory: a first course* (Vol. 129). Springer Science & Business Media.

Harwell, M. R. (2011). Research design: Qualitative, quantitative, and mixed methods . In C. Conrad & R. C. Serlin (Eds.), *Pursuing ideas as the keystone of exemplary inquiry* . Sage

Hedrick, T. E., Bickman, L., & Rog, D. J. (1993). *Applied research design: A practical guide*. Sage Publications.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime : an empirical foundation for a theory of personal victimization*. Cambridge (Mass.) : Ballinger. http://lib.ugent.be/catalog/rug01:000508194

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, *26*, 383–402. https://doi.org/10.1057/sj.2013.25

Holt, T., & Bossler, A. (2009). "Mobile money: communication, consumption and change in the payments space". https://doi.org/10.1080/01639625.2013.822209

Holt, T., & Bossler, A. (2014). An Assessment of the Current State of Cybercrime

Scholarship. *Deviant Behavior*, *35*. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420–436. https://doi.org/10.1177/1043986213507401

Ile, I. and Boadu, E.S. (2018), "The paradox of youth empowerment: exploring youth intervention programme in Ghana", Cogent Social Sciences, Vol. 4 No. 1, pp. 1-15.

Jack, W., & Suri, T. (2011). *Mobile money: The economics of M-PESA (No. w16721).*

Jegede, O. O., Oluwadare, A. J., & Aremu, F. S. (2016). Micro-level determinants of innovation: analysis of the Nigerian manufacturing sector. *Innovation and Development*, *6*(1), 1-14.

Kanobe, F., Alexander, P.M. and Bwalya, K.J. (2017), "Policies, regulations and procedures and their effects on mobile money systems in Uganda", *The Electronic Journal of Information Systems in Developing Countries*, Vol. 83 No. 1, pp. 1-15.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, *30*, 470–486. https://doi.org/10.1177/0894439311422689

Krejcie, R. V, & Morgan, D. W. (1970). *Determinig Sample Size for Research Activities*. *38*,

607–610.

La Nkwantananag Municipal Assembly. (2016). *The composite budget of the La Nkwantanang Madina Municipal Assembly for the 2016 Fiscal year*.

Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing*, *13*(18), 1587-1611.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Lichtenberg, P., Stickney, L., & Paulson, D. (2013). Is Psychological Vulnerability Related to the Experience of Fraud in Older Adults? *Clinical Gerontologist*, *36*, 132–146. https://doi.org/10.1080/07317115.2012.749323

Marcum, D. (2008). *Egonomics: What makes ego our greatest asset (or most expensive liability)*. Simon and Schuster.

Mannon, J. M. (1997). Domestic and intimate violence: An application of routine activities theory. *Aggression and Violent Behavior*, *2*(1), 9–24. https://doi.org/https://doi.org/10.1016/S1359-1789(96)00023-7

Maurer, B. (2012), "Mobile money: communication, consumption and change in the payments space", *Journal of Development Studies*, Vol. 48 No. 5, pp. 589-604.

Merritt, C. (2011), "Mobile money transfer services: the next phase in the evolution of person-to-person payments", *Journal of Payments Strategy and Systems*, Vol. 5 No. 2, pp. 143-160.

Messner, S. F., & Tardiff, K. (1985). The Social Ecology Of Urban Homicide: An Application Of The "Routine Activities" Approach. *Criminology*, *23*(2), 241–267. https://doi.org/10.1111/j.1745-9125.1985.tb00336.x

Morawczynski, O. (2015). *"Fraud in Uganda: How Millions Were Lost to Internal Collusion."* Blog Post.

Morse, J. M. (1991). Approaches to qualitative-quantitative methodological triangulation. *Nursing research*, *40*(2), 120-123.

Morse, J. M. (2000). Determining sample size. *Qualitative health research*, *10*(1), 3-5.

Mugisha, I. R. (2014). *"Two Men Arrested for Allegedly Defrauding Rwf495m from Tigo.* Blog Post.

Nabavi, S. H., Alipour, F., Hejazi, A., & Rashedi, V. (2014). Relationship between social support and mental health in older adults. *Medical Journal of Mashhad University of Medical Sciences*, *57*(7), 841-846.

Newman, J., & Clarke, J. (2003). *Publics, politics and power: Remaking the public in public*

services. Sage.

Osei-Boateng, C., & Ampratwum, E. (2011). *The Informal Sector in Ghana*.

Patchin, J., & Hinduja, S. (2010). Traditional and Nontraditional Bullying Among Youth: A Test of General Strain Theory. *Youth & Society - YOUTH SOC*, *41*. https://doi.org/10.1177/0044118X10366951

Porteous, D. (2006). *The Enabling Environment for Mobile Banking in Africa*.

Pratt, T., Cullen, F., Sellers, C., Winfree Latham, J., Madensen, T., Daigle, L., Fearn, N., & Gau, J. (2010). The Empirical Status of Social Learning Theory: A Meta-Analysis. *Justice Quarterly*, *27*, 765–802. https://doi.org/10.1080/07418820903379610

PYMNTS. (2020, September 1). Authentication, Preventing Fraud Amid Distraction. PYMNTS.Com. Retrieved January 19, 2022, from https://www.pymnts.com/news/security-and-risk/2020/authenticating-consumers-andpreventing-fraud-in-an-age-of-distraction/

Quarshie, H., Martin-Odoom, A., Accra, & Sciences, G. (2012). Fighting Cybercrime in Africa. *Computer Science and Engineering 2012, 2012, 2(6): 98-100*, 98–100. https://doi.org/10.5923/j.computer.20120206.03

Reyns, B., Henson, B., & Fisher, B. (2011). Being Pursued Online: Applying Cyber lifestyle Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and*

Behavior - CRIM JUSTICE BEHAV, 38, 1149–1169. https://doi.org/10.1177/0093854811421448

Rice, K. J., & Csmith, W. R. (2002). Socioecological Models of Automotive Theft: Integrating Routine Activity and Social Disorganization Approaches. *Journal of Research in Crime and Delinquency*, *39*(3), 304–336. https://doi.org/10.1177/002242780203900303

Runions, K., Shapka, J., Dooley, J., & Modecki, K. (2013). Cyber aggression, victimization and social information processing: Addressing the medium and the message. *Psychology of Violence*, *3*, 9–26. https://doi.org/10.1037/a0030511

Saunders, M., Lewis, P. H. I. L. I. P., & Thornhill, A. D. R. I. A. N. (2007). Research methods. *Business Students 4th edition Pearson Education Limited, England*.

Schwiderski-Grosche, S., & Knospe, H. (2002). Secure mobile commerce. *Electronics & Communication Engineering Journal*, *14*(5), 228-238.

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse & Neglect*, *31*, 1–19. https://doi.org/10.1080/08946566.2019.1625842

Solin, M., & Zerzan, A. (2010). Mobile Money : Methodology for Assessing Money Laundering and Terrorist Financing Risks. *GSMA: Mobile Money for the Unbanked:*

GSMA Discussion Paper, *January*, 1–35.

Subex (2017), "Service providers combat mobile money frauds", available at: www.subex.com/subex/helps-service-providers-combat-mobile-money-frauds/ (accessed 19th January, 2021).

Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, *23*(3), 313–324. https://doi.org/10.1177/0269758017704330

Tashakkori, A., & Creswell, J. W. (2007). The new era of mixed methods. *Journal of mixed methods research*, *1*(1), 3-7.

Wang, Y., Hahn, C., & Sutrave, K. (2016). *Mobile payment security, threats, and challenges*. https://doi.org/10.1109/MOBISECSERV.2016.7440226

Warner, J. (2011). Understanding Cybercrime in Ghana: A View from Below. *International Journal of Cybercriminology*, *5*(1), 736–749.

Whitty, M. T., & Buchanan, T. (2015). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176–194. https://doi.org/10.1177/1748895815603773

World Bank. Information, Communication Technologies, & infoDev (Program). (2012). *Information and communications for development 2012: Maximizing mobile*. World Bank Publications.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.

Yu, S., & Ibtasam, S. (2018). *A Qualitative Exploration of Mobile Money in Ghana*. https://doi.org/10.1145/3209811.3209863

APPENDIX 1

QUESTIONNAIRE FOR DATA COLLECTION

TITLE: EXPLORING THE EXPERIENCES OF MOBILE MONEY FRAUD VICTIMS IN MADINA MARKET

Dear respondent, I am a student of University of Ghana, Department of Sociology. I am conducting a study as part of a requirement for a master's degree in Sociology. I would be very grateful if you could participate in this study by answering these questions. Confidentiality of the information provided is fully assured.

A. SECTION 1-SOCIO-DEMOGRAPHIC CHARACTERISTICS

1. Age _____
2. Gender _____
3. Highest level of education _____
4. Ethnicity _____
5. Type of trade _____
6. Religion _____

B. SECTION 2- MOBILE MONEY USE

7. What mobile network do you use?

A. Vodafone B. MTN C. Airtel-Tigo

8. How long have you been using that network?

A. Less than one year B. One to Five years C. More than five years

9. How long have you used mobile money?

A. Less than one year B. One to five years C. More than five years

10. How often will you use mobile money in a week?

……

10. Do you have bank accounts and how often do you use the bank in the week?

……

11. What exactly do you use mobile money for?

……

C. SECTION 3- KNOWLEDGE ABOUT MOBILE MONEY FRAUD

12. Have you heard about mobile money fraud before?

A. Yes B. No

13. If yes, where did you hear about mobile money fraud?

14. Have you been defrauded through mobile money before?

A. Yes B. No

15. Do you know anyone who has been defrauded through mobile money?

A. Yes B. N o

16. Do you think traders in the Madina market get defrauded through mobile money?

A. Yes B. No

17. If yes, why do you think traders get defrauded?

18. Do you know any trader of the Madina market who has been defrauded through mobile money?

A. Yes B. No

19. If yes, do you know why and how they got defrauded?

20. How often do you hear of such cases?

21. What do you think makes one a target?

22. Despite fraud, do you still see it as a useful service?

A. Yes B. No

23. Please explain your answer

24. Which cases or stories of mobile money fraud are common?

APPENDIX 2

IN-DEPTH INTERVIEW GUIDE FOR VICTIMS OF MOBILE MONEY FRAUD

TITLE: EXPLORING THE EXPERIENCES OF MOBILE MONEY FRAUD VICTIMS

IN MADINA MARKET

Dear participant, I am a student of University of Ghana, Department of Sociology. I am conducting a study as part of a requirement for a master's degree in Sociology. I would be very grateful if you could participate in this study by answering these questions.

Confidentiality of the information provided is fully assured**.**

A. SECTION 1- SOCIO-DEMOGRAPHIC CHARACTERISTICS

1. Age _____
2. Sex _____
3. Highest level of education _____
4. Ethnicity _____
5. Type of trade _____

B. SECTION 2-INCIDENCE OF MOBILE MONEY FRAUD

1. What mobile network do you use?
2. How long have you been using that network?
3. Do you have mobile money and why did you register for it?
4. How long have you used mobile money?

5. Do you use the same number for your calls and mobile money transactions?

6. What have your experiences been since you started using mobile money services?

7. What do you mainly use mobile money for?

8. Which month and year were you defrauded?

9. How many times have you been defrauded?

10. What was the process through which you were defrauded? (By a call or SMS or other please explain). How did it start? Did you have second thoughts? Did you discuss with anyone before going ahead?
11. How much did you lose to the fraudster?

12. Did you report to the police or the service provider or any authority?

13. What did they do about it and were you satisfied with what was done?

14. Would you say you did something wrong or right that made you a suitable target to the fraudster?

C. SECTION 3- IMPACT OF MOBILE MONEY FRAUD

15. What was the purpose of the money which you lost?

16. How did the stolen money affect you?

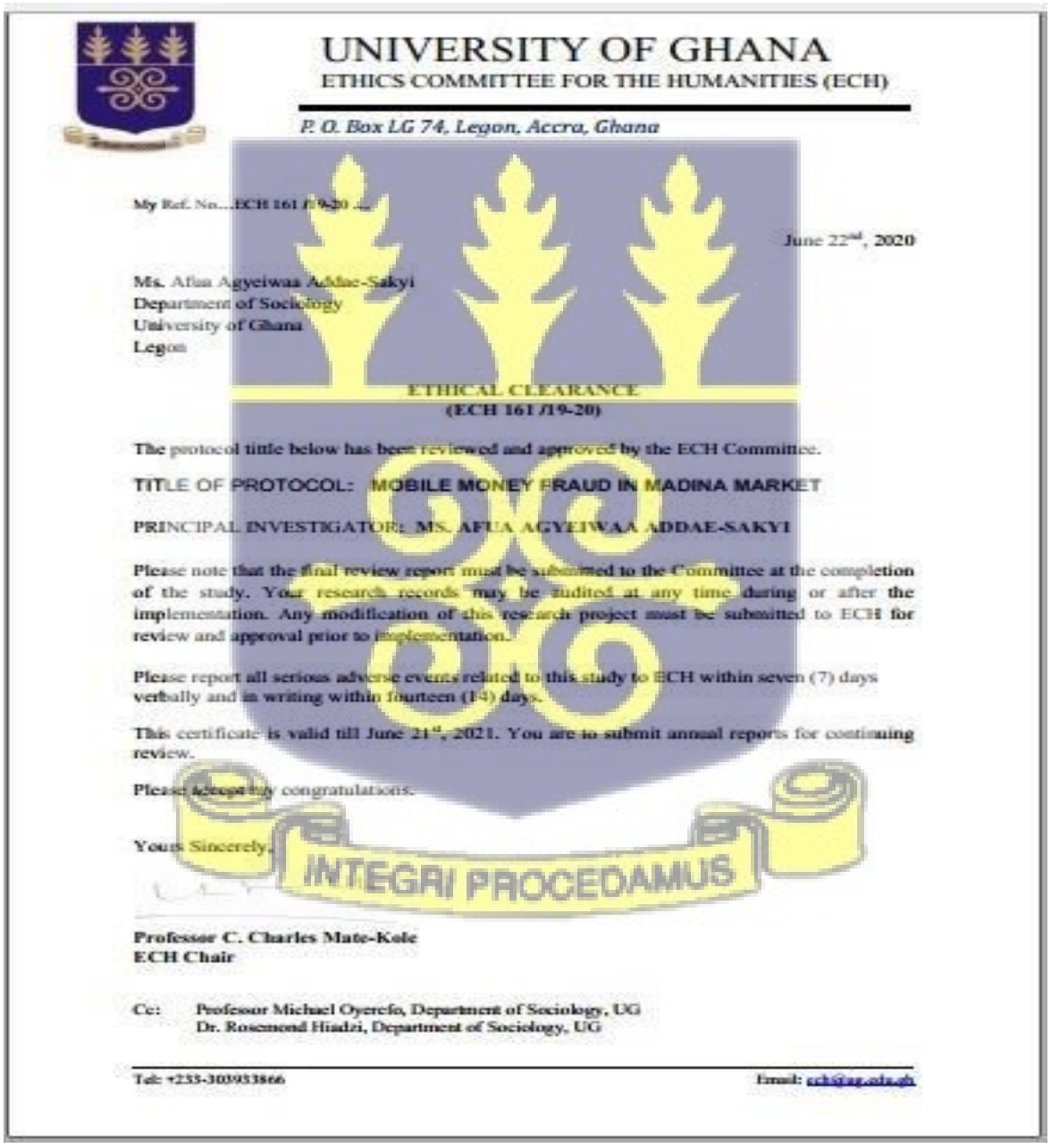
17. Do you still use mobile money after being defrauded?

18. What are some of the things you have done to ensure you do not get defrauded again?

19. Do you think your network provider has put in place measures to ensure you do not get defrauded again?

20. Do you think the police has done enough to ensure you do not get defrauded again?

APPENDIX 3- ETHICAL CLEARANCE FORM



UNIVERSITY OF GHANA
ETHICS COMMITTEE FOR THE HUMANITIES (ECH)

P. O. Box LG 74, Legon, Accra, Ghana

My Ref. No....ECH 161 /19-20 ...

June 22nd, 2020

Ms. Afua Agyeiwaa Addae-Sakyi
Department of Sociology
University of Ghana
Legon

ETHICAL CLEARANCE
(ECH 161 /19-20)

The protocol title below has been reviewed and approved by the ECH Committee.

TITLE OF PROTOCOL: MOBILE MONEY FRAUD IN MADINA MARKET

PRINCIPAL INVESTIGATOR: MS. AFUA AGYEIWAA ADDAE-SAKYI

Please note that the final review report must be submitted to the Committee at the completion of the study. Your research records may be audited at any time during or after the implementation. Any modification of this research project must be submitted to ECH for review and approval prior to implementation.

Please report all serious adverse events related to this study to ECH within seven (7) days verbally and in writing within fourteen (14) days.

This certificate is valid till June 21st, 2021. You are to submit annual reports for continuing review.

Please accept my congratulations.

Yours Sincerely,

INTEGRI PROCEDAMUS

Professor C. Charles Mate-Kole
ECH Chair

Cc: Professor Michael Oyerefo, Department of Sociology, UG
Dr. Rosemond Hiadzi, Department of Sociology, UG

Tel: +233-30933866 Email: ech@ug.edu.gh