

**UNIVERSITY OF EDUCATION, WINNEBA**

**CUSTOMER EXPERIENCES AND PERSPECTIVES ON MOBILE MONEY  
SERVICE FRAUD: A CASE STUDY OF UNIVERSITY OF EDUCATION,  
WINNEBA**



**MASTER OF ARTS**

**2023**

**UNIVERSITY OF EDUCATION, WINNEBA**

**CUSTOMER EXPERIENCES AND PERSPECTIVES ON MOBILE MONEY  
SERVICE FRAUD: A CASE STUDY OF UNIVERSITY OF EDUCATION,  
WINNEBA**



**A dissertation in the Department of Communication and Media Studies,  
Faculty of Foreign Languages and Communication, submitted to the school of  
Graduate Studies in partial fulfillment  
of the requirements for the award of the degree of  
Master of Arts  
(Communication Studies)  
in the University of Education, Winneba**

**JANUARY, 2023**

## DECLARATION

### Student's Declaration

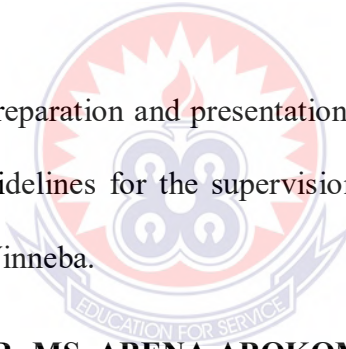
I, Mavis Ofosuah Asante, hereby declare that this thesis, with the exception of quotations and references contained in published works which had all been identified and acknowledged, is entirely my own original work and has not been submitted, either in part or whole, for another degree elsewhere.

**SIGNATURE:** .....

**DATE:** .....

### Supervisor's Declaration:

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



**NAME OF SUPERVISOR: MS. ABENA ABOKOMA ASEMANYI**

**SIGNATURE:** .....

**DATE:** .....

## **DEDICATION**

I dedicate this work to my dearest husband Mr. Isaac Asomah Beseh, my adorable children (Geoffrey, Lady-Geona and Ron-Schneider) and my entire family



## ACKNOWLEDGEMENTS

I am very fortunate to have done my graduate work at the University of Education, Winneba. Therefore, there are few people to appreciate for the success.

First, I give thanks to the Almighty God for giving me wisdom, knowledge and His endless mercies for this great success

I also could not have undertaken this journey without the support, guidance and encouragement from my supervisor, Ms. Abena Abokoma Asemanyi. Additionally, this endeavor would not have been possible without the generous support from the lecturers of the School of Communication and Media Studies, especially Prof. Andy Ofori Birikorang and Prof. Christiana Hammond. I am grateful to all of you for pushing me beyond my limits. Lastly, I say thank you to my supportive parents and siblings, my adorable children and my dearest husband. Their belief in me has kept my spirit and motivation high during this journey.

To God I give all the glory for great things He has done.

## TABLE OF CONTENTS

DECLARATION	iii
DEDICATION	iv
ACKNOWLEDGEMENTS	v
TABLE OF CONTENTS	vi
ABSTRACT	x
<b>CHAPTER ONE: BACKGROUND OF THE STUDY</b>	<b>1</b>
1.1 Introduction	1
1.2 Problem Statement	5
1.3 Objectives of the Study	8
1.4 Research Question	8
1.5 Significance of the Study	9
1.6 Organization of Study	11
<b>CHAPTER TWO: LITERATURE REVIEW</b>	<b>12</b>
2.0 Introduction	12
2.1 Conceptual Review	12
2.1.1 Mobile Money Services	12
2.1.2 Cash Withdrawal	17
2.1.3 Cash Transfer	18
2.1.4 Cash Deposits	19
2.1.5 Purchase of recharge card	20
2.1.6 Fraud	21
2.1.7 Mobile Money Fraud	22
2.1.8 Causes of Mobile Money Fraud	26

2.1.9 Mechanisms to combat mobile money fraud by the key stakeholders	28
2.1.10 Mobile Money Ecosystem	30
2.1.11 Impact of Fraud	31
2.2 Empirical Review of the Growth in Mobile Money Services: Global Perspective	32
2.3 Security threats to Mobile Phone and Mobile Money	34
2.3.1 Safeguards against Security Threats	36
2.4 Growth of Mobile Money Services in Ghana	38
2.5 Regulatory Environment of Mobile Money Services in Ghana	43
2.6 Drivers of the usage of MoMo Services	46
2.6.1 Gender	46
2.6.2 Age	47
2.6.3 Education	48
2.6.4 Income levels	49
2.7 Importance of MoMo Service	50
2.8 Challenges of MoMo usage	53
2.9 Theoretical Review of Pentagon Theory	54
2.9.1 Relevance of Theory to the study	56
<b>CHAPTER THREE: RESEARCH METHODOLOGY</b>	<b>57</b>
3.1 Introduction	57
3.2 Research Philosophy	57
3.3 Research Design	60
3.4 Research Approach	63
3.5 Sampling techniques adopted for the selection of the units of enquiry	64



3.6 Sources and methods of data collection	65
3.6.1 Secondary data sources and their collection	65
3.6.2 Primary sources of data and their collection	65
3.7 Data processing and analysis	66
3.8 Ethical considerations	68
<b>CHAPTER FOUR: RESULTS AND DISCUSSION</b>	<b>69</b>
4.1 Introduction	69
4.2 What are the forms of MoMo fraud strategies experienced by customers of MoMo in Ghana?	69
4.2.1 Understanding MoMo Fraud	69
4.2.3 Frequency of occurrence of MoMo Fraud	70
4.2.3 Strategies for committing MoMo Fraud	72
4.3 Who are the main perpetrators of the MoMo fraud in Ghana?	75
4.4 What are the framework for fraud detection put together by the Telco's and consumers?	79
4.4.1 Telecommunication framework for detecting MoMo Fraud	79
4.4.2 MoMo consumer tactics for fraud detection or prevention	84
<b>CHAPTER FIVE: SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS</b>	<b>87</b>
5.1 Introduction	87
5.2 Summary of Findings	87
5.2.1 Forms of MoMo fraud strategies experienced by customers of MoMo	87
5.2.2 Examining the main perpetrators of the MoMo fraud among UEW Students	88



5.2.3 Framework for fraud detection put together by the Telco's and MoMo consumers	88
5.3 Conclusion	89
5.4 Recommendations	90
<b>REFERENCES</b>	92



## ABSTRACT

The study examined mobile money service fraud experiences and perspectives on control practices at University of Education, Winneba. The objectives of the study included to examine the forms of MoMo fraud strategies experienced by customers of MoMo on UEW Campus, to examine and classify the main perpetrators of the MoMo fraud among UEW students as well as the framework for fraud detection put together by the Telco's and consumers on UEW Campus. The study adopted the case study research design. The purposive sampling technique was used to select the UEW Campus. Using the convenience sampling technique, five respondents were sampled for the study. The outcome of the in-depth interviews conducted revealed Mobile money fraud was committed in various forms such as anonymous calls and text messages from scammers, fraudsters calling to deceive subscribers that they are to deliver goods from abroad or from a close relative under false pretexts. Finally, fraudsters sending false cash-out messages to merchants for authorization of which the physical cash is issued by the merchant to the fraudster without the equivalent e-cash. Mobile money fraud has been perpetuated in diverse forms such as mobile money network systems fraud, false promotion fraud, and reversal of erroneous transactions, fortuitous scams, and mobile money agents' fraud. Finally, the frameworks that have been used to detect mobile money fraud include the display of national identifies cards for the transaction, digital identification systems, the use of firewall to protect mobile money accounts, effective information technology architecture for mobile money services, reporting of mobile money fraud to telecoms and the sanctioning of mobile money fraudsters. The study suggested there should be public education and awareness creation on the activities of mobile money fraudsters in Ghana by telecommunication companies in conjunction with the National Communications Authority and the Bank of Ghana. The study therefore, concluded that the menace of mobile money fraud threatens the integrity of the mobile money financial services.

## CHAPTER ONE

### BACKGROUND OF THE STUDY

#### 1.1 Introduction

In recent years, mobile phone users, mobile telecommunication networks, technological specialists, and academia have all grown accustomed to the idea of mobile money (Narteh *et al.*, 2017; Abor *et al.*, 2018). After the first two "Mobile Money Summits" in 2008 and 2009, it attracted considerable attention as a payment mechanism all across the world (Bongomin and Ntayi, 2019; Maurer, 2015; Alnes, 2017).

Mobile phones can be used to access the service (Yawson, 2022). Jenkins (2008) suggested that the mobile money platform should include services like transfers; these goods have recently been integrated into the service. Financial analysts place these extra features and services under the same heading of banking. The mobile money service also aids in payment for services like digital television, parking, power and water, among others. Many consumers, especially those in metropolitan areas, are becoming more interested in this trend.

Mobile gadget usage has ingrained itself into our daily lives (Munos *et al.*, 2016). We now significantly rely on mobile devices to carry out our daily operations. The way we make financial transactions are a crucial component of our interactions with mobile devices that cannot be overstated (Kryshtanovych *et al.*, 2022). Financial technology, often referred to as Fintech, is the use of innovations and technology that attempts to contend with the conventional way of undertaking financial transactions (Suryono *et al.*, 2022). Individuals have opportunities and capabilities to plan, save, and manage their financial lives when they have access to traditional financial services or are financially included. Since the infrastructure and services required for

formal financial inclusion do not exist in the majority of the developing world, access to formal financial services becomes almost impossible. Customers frequently have to travel a great distance to locations with these financial infrastructures in order to receive these services, which results in additional costs for those who are already poor (Nyaga, 2013). Financial exclusion has the consequence that people who do not have access to traditional financial services are more likely to be poor, and this is strikingly obvious in the majority of developing nations (Roessler, 2018).

Financial services provided by telecom companies known as mobile network operators (MNOs) called mobile money transactions (MMTs) make it possible to move money (cash). These financial transfers, also referred to as mobile money (MM), are made available over telecommunications channels between service subscribers (customers) and MNOs.

According to Demirgüç-Kunt *et al.* (2021) 12 percent of adults in sub-Saharan Africa, or one third of all account users, reported having a mobile money account. This is a comfort since it allows millions of individuals in developing economies to access financial services. Short Message Services (SMS) and Unstructured Supplementary Service Data (USSD) coding are the primary deployment methods for MMTs, making it simple to set up the service in remote locations with limited internet connectivity. Customers can also utilize feature phones, which are less expensive than their smart phone equivalent. However, utilizing specialized mobile software, Mobile Money Services can also be made available on smart phones (Roessler, 2018).

The use of mobile money has increased dramatically in emerging countries (Chauhan, 2015; Markovich and Snyder, 2017). Majority of the population in these countries like Uganda, India, Tanzania, Zambia, Nigeria, and, Ghana, Argentina are unbanked and

the emergence of mobile money has presented them with the greatest and easiest alternative to the traditional banks (Demirgüç-Kunt et al. 2021).

In Kenya, M-Pesa (the mobile money platform) processed 43% of the nation's gross domestic product in 2013, 45% in 2015, and 49% in 2016 (Deloitte, 2015; Markovich and Snyder, 2017). As of March 2015, there were 31,154,420 cellular/mobile voice subscribers in Ghana. Mobile Telecommunications Network (MTN) is in the lead with 17,790,123 subscribers, of the market, followed by Vodafone with 7,300,166 subscribers with AirtelTigo users being 3,497,303 subscribers of the market (National Communications Authority, 2022).

Mobile money is the use of telecommunication platforms or networks to perform banking services by mobile phone subscribers. In short, mobile money allows subscribers to bank directly from their phones without having to physically visit a financial institution to pay bills, receive money, and transact business using virtual mobile accounts known as mobile money wallets (The Economist, 2012). The use of mobile money for transactions has been steadily increasing across Africa, with the technology positioned as the next "big thing" to revolutionize Africa's cash-dominated economy (Fintech Africa, 2017).

According to The Economist (2012), there were 20 countries where more than 10% of adults used mobile money at some point in 2011, 15 of which are in Africa. In Sudan, Kenya, and Gabon, for example, more than half of adults used mobile money (The Economist, 2012). According to the results of this survey, mobile money has become one of the "must-have" services for African telecom companies. For example, Ghana's top three telecommunications companies, MTN, AirtelTigo and Vodafone all provide

mobile money services to their customers, and usage statistics are increasing on a daily basis (Akomea-Frimpong, 2017).

In Ghana, MTN, a telecom company, was first to launch mobile money in 2009. In 2011, Tigo and Airtel joined, and as of now, all telecommunication networks offer this service (Fintech Africa, 2017). Mobile money transactions were expected to be worth GHC11 billion in 2014 with 2.3 million active users; this increased to GHS31 billion in 2015 with 10.4 million active users; and as of July 2016, this amount has increased by 118% amounting to 17.2 million active users (Akomea-Frimpong, 2017). In Ghana, the following mobile phone providers are driving this service: AirtelTigo, Vodafone and MTN (Roberts, 2018).

Mobile money has been prone to some fraudulent activities leading to the loss of some funds particularly due to the activities of scammers (Chatain *et al.*, 2011). These scammers are endangering the mobile money service rendered by these telecommunication companies in Ghana (Botchey *et al.*, 2022). The scammers using mobile money have earmarked Ghana as their top destination for their dubious activities, as evidenced by the fact that as at the year 2022, mobile money fraud cases made up of more than 60% of all transactions cases across Ghana, 42% of all transactions in Tanzania, 42% of all transactions in Kenya, and 53% of all transactions in Uganda (National Communications Authority, 2022; Busuulwa, 2016).

The relatively high rates of mobile money fraud cases that are perpetuated by scammers are difficult to track down and successfully retrieve the money of the victims due to the weak enforcement of rules and regulations governing fraudulent activities in Ghana (Akomea-Frimpong, 2017). Consequently, most of the perpetrators of these fraudulent activities are not arrested and prosecuted fully by law

(Botchey et al., 2022). Although this is a significant economic issue, a detailed study of the literature reveals limited information on fraudulent activities about mobile money services is documented. This can be linked to the use of ineffective fraud indicators to identify, quantify, and curtail the threat. Additionally, few researches have ascertained and shed light on the problem encountered in using mobile money, with little or no solutions (Osei-Assibey, 2015; Markovich & Snyder, 2017).

According to the National Communications Authority (2022), depending on the transaction, some victims felt prey to fraudsters by using mobile money and lost between GHC200 (\$45) and GHC3, 500 (\$800) on the average as at the year 2021. Victims claimed that scammers call them and claim that they transferred money into their mobile money wallet by mistake and that they need to send it back to them. Later, it is discovered that this is a deliberate, untrue ploy to dupe them (Alhassan & Butler, 2021).

A report by Ghana Chamber of Telecommunications (2019) shows that, 388 fraud instances were reported in Ghana using mobile money services in 2016, up from 278 in 2015, including MTN Mobile Money, Tigo Cash, Airtel Money, and Vodafone Cash. It is against this background that the study sought to examine mobile money service fraud experiences and perspectives on control practices at University of Education, Winneba.

## **1.2 Problem Statement**

In recent years, the notion of mobile money has gained popularity among phone users, telecommunication networks, technological specialists, and academics (Enowbi *et al.*, 2021). Research, literature and academics has traced the origins of mobile money services to M-PESA, it started in Kenya and is now expanded rapidly to numerous

impoverished nations worldwide (Etim & Salem, 2014). The service is available via mobile phone (Etim, 2014). Mobile money is described as a digital financial service in which an individual accesses a financial service or initiates a financial transaction via a mobile phone handset (Yu & Ibtasam, 2018).

Irrespective of the importance of mobile money services, it is challenged with the activities of fraudsters in recent times (Akomea-Frimpong, 2017; Botchey et al., 2022). The activities of mobile money fraud does not only causes financial loss to consumers or mobile money providers, but it also harms the reputation of the mobile money service providers as a whole (Deloitte, 2015; Markovich & Snyder, 2017). As a result, limiting the risk of fraud is a fundamental goal of a solid risk management approach. In contrast to the preceding definition, fraud is a component of deceit by one person and it results in some purposeful falsehood against the victim (Akomea-frimpong *et al.*, 2019).

Also, in order to eliminate mobile money fraud, and optimize the security of the system, it is now more important than ever to conduct research into the security practices used by mobile network operators and users. Recent increases in fraud instances have caused certain mobile money service providers to lose millions of dollars in income. For instance, the CIO East Africa (2012) reported on a fraud case using MTN Uganda mobile money, in which corporate employees stole millions of dollars from customers of the service. Unfortunately, there is little research on mobile money theft in Africa; with some publications in CIO East Africa. Therefore, while it is anticipated that mobile money service will be immensely alluring to fraudsters, the exact amount and type of the fraud risks are yet to be clearly identified for MNOs and mobile customers (Enowbi et al., 2021).



However, the success of this service has come with a risk for the operators because unscrupulous individuals continue to use the mobile money service as a conduit to defraud others (Chatain et al., 2011). These fraudsters, who, if left unchecked, can put an end to operations in Ghana (Laryea, 2016), jeopardize the service's sustainability. The relatively high rates of mobile money fraud recorded are difficult to trace, and the devices and legislation available on mobile money operations are insufficient to apprehend the perpetrators. This can be attributed to the use of ineffective fraud indicators to detect, measure, and prevent the threat (Osei-Assibey, 2015).

In Ghana, some research has been conducted on mobile money fraud. Akomea-Frimpong et al. (2020) investigated fraud control on mobile money services in Ghana. The study investigated the main causes of fraud in Ghana's mobile money services, as well as the measures taken to combat the problem by key stakeholders involved in the mobile money services. The researcher used a qualitative research design. In total, 43 interviews were conducted with key stakeholders in Ghana's mobile money industry. According to the study, fraud in mobile money services is caused by weak internal controls and systems, a lack of sophisticated information technology tools to detect the threat, insufficient education and training, and poor employee remuneration. These factors impede growth and the smooth operation of services.

Botchey et al. (2020) studied mobile money fraud prediction in Ghana. The study looked at machine learning algorithms based on support vector machines (kernel-based), gradient boosted decision tree (tree-based) and Naïve Bayes (probabilistic based) algorithms, taking into consideration the imbalanced nature of the dataset. The outcome of study established that the use of gradient boosted decision tree holds a great potential in combating the problem of mobile money fraud as it was able to produce near perfect results.

Afanu and Mamattah (2013) investigated mobile money security in a comprehensive manner. The study was a case study of mobile money security in Ghana, and it used qualitative and quantitative data gathered through questionnaires and structured interviews with key mobile network operator personnel (MNO). The general perception that there is no direct link between mobile phone protection and mobile money security is one of the study's main findings. Personal identification number (PIN) sharing was also identified as a major cause of consumer-driven fraud. However, there is a dearth of literature on customer experiences and perspectives on mobile money service fraud. It is against this background that this study sought to explore customer experiences and perspectives on mobile money service fraud using the UEW Campus as a case.

### **1.3 Objectives of the Study**

The main aim of the study is to establish the occurrence of mobile money fraud among UEW students together with its accompanying experiences. However, specific objectives of the study include the following.

1. To examine the forms of MoMo fraud experienced by customers of MoMo.
2. To examine and classify the main perpetrators of the MoMo fraud.
3. To examine the framework for fraud detection put together by the Telco's and consumers.

### **1.4 Research Question**

The questions that underpins the study include the following.

1. What are the forms of MoMo fraud strategies experienced by customers of MoMo in Ghana?
2. Who are the main perpetrators of the MoMo fraud in Ghana?

3. What are the framework for fraud detection put together by the Telco's and consumers?

### **1.5 Significance of the Study**

With the increasing use of mobile money services and the emergence of new use cases, it is critical to conduct research into the security practices of mobile network operators and users in order to ensure mobile money is secure, to prevent fraud, and to understand user perceptions of the links between mobile phone protection and mobile money security. Recently, some mobile money service providers have seen an increase in fraud cases, resulting in the loss of millions of dollars in revenue.

Africa (2012) reports on a fraud case involving MTN Uganda mobile money, in which company employees stole millions of dollars from mobile money users. Unfortunately, research into mobile money fraud in Africa has been limited to newspapers such as the CIO East Africa, with little scientific research done on the subject. As a result, the true scope and nature of fraud issues for MNOs and mobile users have yet to be fully defined, despite the fact that mobile money services are expected to be extremely appealing to fraudsters.

By 2016, it is expected that global mobile payment transaction values will total \$617 billion, with 448 million users (Gartner, 2012). Based on this forecast, the increased use of mobile money services, and the various business use cases designed every day, it is critical to design a holistic approach to mobile money security that will reduce security exposures and prevent fraud.

The use of mobile money as an electronic payment system is gaining traction in Ghana and most African countries. MNO reliance on technology (mobile telecommunications and information systems) to deliver mobile money service comes

with some security risks and existing risks inherent in e-payment systems. The way these security risks are handled may influence mobile money users' perceptions of the service's security. Furthermore, the mobile money subscriber's awareness of their responsibility for the security of the service on their mobile phone may influence some of the actions they take to protect their mobile money wallet.

The relevance of this study rest on its probable contribution to knowledge, policymaking and the mobile service industry. Perhaps this study is the first comprehensive study to assess mobile money service fraud experience and perspectives on control practices among students of University of Education, Winneba. Thus, in terms of theoretical relevance, this present study advances knowledge and understanding of experiences of students concerning mobile fraud and its preventive controls.

Mobile money as an electronic payment technology is gaining traction in Ghana and most African nations. This is because the way these security threats are managed may have an impact on mobile money customers' perceptions of the service's security. This study gives some insight into the security controls and methods used by MNOs to safeguard the mobile money service, as well as mobile money customers' perceptions of the relationship between mobile money security and mobile phone protection. The project will aid the reduction of the intervention costs and allow new operators to gain insights from the older and more experienced ones. Understanding fraud allows for greater knowledge in the investment required in mobile financial services.

Further, successful completion of this study will be helpful to policymakers, regulatory authorities, mobile network operators, and other mobile money stakeholders and assist them in making wise decisions on mobile money services due

to the sheer volume of transactions and the amount involved, as well as the profound economic repercussions any failure in mobile money services and transactions will have for subscribers and the economy at large.

The study will also contribute to the literature by responding to calls from previous studies that argue for management researchers to move toward consensus on mobile money fraud, as this would help develop a cutting-edge approach that is suitable for most, if not all situations (Dartey-Baah, 2015). It also fills the gap in literature calling for knowledge expansion (Wang & Noe, 2010), on mobile money service fraud experiences and perspectives on control practices.

### **1.6 Organization of Study**

This work has been organized into five chapters. Chapter one covers the general introduction to the study grouped under the following headings; background of the study, statement of the problem, objectives of the study, research questions, significance of the study and the organization of the study.

Chapter two identifies and reviews previous and relevant work done on the topic. It also involves the definition of concepts. Thus, the chapter deals with the literature review. In chapter three, the research methodology was outlined including the research design, population, sample and sampling procedures, instrument, data collection procedure and data analyses. Chapter four deals the data analysis, presentation, and discussion. Chapter five covers the summary of findings, conclusions, recommendations, and suggested area for further studies.

## CHAPTER TWO

### LITERATURE REVIEW

#### 2.0 Introduction

This chapter discusses the relevant scholarly views and arguments on to assess mobile money service fraud experience and perspectives on control practices among students at the University of Education, Winneba in an attempt to draw readers' attention to what has already been done on the topic, and the gaps in the literature that need to be addressed. The literature review draws on the following sub-headings: conceptual review, theoretical framework, and empirical evidence. Details of the sub-headings are discussed in the sub-sections below.

#### 2.1 Conceptual Review

##### 2.1.1 *Mobile Money Services*

Mobile money is defined as the "monetary value that is made available to a user to conduct transactions through a mobile device and is accepted as payment by parties other than the issuer, issued on receipt of funds in an amount equal to the available monetary value, electronically recorded, mirrored by the value stored in an accounts typically open in one or more banks, and redeemable for cash," according to Di Castri (2013, p. 5). Mobile money is a type of electronic currency or financial service provided via a mobile phone (ACP Observatory on Migration, 2014).

According to Jack et al. (2010), mobile money is an SMS-based financial service designed for deposits and transfers from a mobile phone's virtual account that is typically distinct from the banking system. People who frequently use this service have access to savings, payments, and bank account transactions. Money deposited into a mobile phone-based account (a "mobile money account") reflects the account holder's possession of an item known as "e-money." They contended that mobile

money might be utilized as a medium of exchange and a means of transmitting purchasing power as long as value is maintained when e-money is sent over the phone.

According to Kendall et al. (2011), mobile money is a network tool that keeps and transfers money for the purpose of exchanging currency, payments, and digital value between major participants including financial institutions, companies, and customers. Customers can use mobile money services to exchange hard currency for e-money, transfer e-money, and turn e-money back into hard currency (Mbiti & Weil, 2014).

According to ACP Observatory on Migration (2014), mobile money falls within the categories of mobile transfers, mobile payments, and mobile banking (M-banking). At mobile money agents, customers deposit cash into their electronic accounts, commonly known as mobile wallets. When a transaction occurs, mobile wallets or accounts are credited or debited. By taking payments and disbursing funds, these agents serve as mediators in the financial system. Without a bank account, mobile transfer services are made available. A mobile money customer (sender) can send cash to another customer (receiver) through an agent, who can then redeem the cash from a different agent.

According to Lyons (2010), a mobile transfer service might be a Person to Person (P2P) transaction carried out from one mobile money account of a subscriber to another without the assistance of an intermediary. Usually, a mobile device is used for this electronic transfer. M-commerce, commonly referred to as mobile payments, refers to services that let customers exchange goods and services while also making payments remotely or at physical locations without the usage of currency.

Mobile money services have the potential to increase the stability, comprehensiveness, and efficiency of the financial system as well as the security of financial customers (Catri, 2013). Jenkins (2008) asserts that the ability of mobile money to promote financial sector inclusion unleashes enormous potential for development impact. Savings obtained through mobile money allow for wealth-building investments in future generations. In comparison to informal and semi-formal financial services and portfolios based on money, mobile money services offer a safer and more practical alternative.

By allowing digital payments through mobile devices, it not only reduces the need for real cash but also creates a platform for a far wider array of financial services. Financial organizations use the sophisticated infrastructure (mobile connectivity, cash in and cash out networks, and mobile money accounts) designed for transactions and electronically storing money.

Any payment made using a mobile device to initiate, authorize, and confirm an exchange of money in exchange for goods and services is referred to as a "m-payment" or "mobile payment" (Karnouskos, 2004). The term "mobile devices" in this context refers to any phone, tablet, or other device that can connect to a mobile network and accept payments (Herzberg, 2003).

E-money has been defined as a more general term that covers payments done with mobile devices, credit cards, prepaid cards, debit cards, near-field communication (NFC) contactless cards, and ATMs. A subcategory of electronic money known as "mobile money" refers to financial services and transactions carried out utilizing mobile phone-integrated technologies. These services could or might not be



connected directly to a personal account or to ATM, prepaid, debit, or credit cards (International Finance Corporation, 2011).

Mobile phone usage is expanding quickly, and most African countries lack access to traditional banking services, which has contributed to the rapid expansion and widespread adoption of mobile money services. In poor countries, more than a billion people have access to mobile phones but no formal bank accounts (GSMA, 2012). The widespread use of mobile phones in Africa offers the necessary platform for reaching out to the unbanked and rural poor with financial services.

In recent years, mobile phone users, mobile telecommunication networks, technological specialists, and academia have all grown accustomed to the idea of mobile money (Narteh *et al.*, 2017; Asongu & Asongu, 2018). After the first two "Mobile Money Summits" in 2008 and 2009, it attracted considerable attention as a payment mechanism all across the world (Suri & Jack, 2016; Maurer, 2015; Gosavi, 2017).

Some academics also claim that M-PESA, which started in Kenya and has since extended to many impoverished nations worldwide, is responsible for the development of the mobile money service (Markovich & Snyder, 2017). Mobile phones can be used to access the service (Etim, 2014). Jenkins (2008) suggested that the mobile money platform should include services like bill payment, salary payment, and local and international transfers; these goods have recently been integrated into the service.

Financial analysts place these extra features and services under the same heading of banking. The mobile money service also aids in paying other bills for services like digital television, parking, power and water, among others. Many consumers,

especially those in metropolitan areas, are becoming more interested in this trend. Rich urban mobile phone users frequently experience this scenario (Nyaga, 2013).

As usual, sending money to the families ends up being an expensive and challenging process. As a result, mobile money can be incredibly helpful and reasonably priced for the underprivileged (Pope *et al.*, 2011). Another option is for the user to transfer funds to a new individual or family, who will then get them via a different mobile money provider or agency (Aker & Mbiti, 2010).

Mobile money is simply defined as a currency that is kept on SIM cards for identification purposes, much like how an account is operated with a specific account number in a traditional banking system. Mobile money is essentially financial transactions carried out primarily through the use of a mobile phone, to put it another way. Mobile banking, mobile payments, and mobile payment transfer systems are the three separate services that make up the category of mobile money services (Lochan *et al.*, 2010). The performance and features of mobile money services can also be used to characterize them. These services include long-distance remittances, micropayments, and informal airtime that are aimed at bringing financial transactions to the doorsteps of the unbanked (Pope *et al.*, 2011).

Mobile money appears to be the most effective method for achieving the goal of financial inclusion for those who are below the poverty line. Mobile money was created as a platform for payments that allows both individuals and businesses to send and receive money. It was not only designed as a transfer mechanism (Aker & Mbiti, 2010). Even if mobile money services may not be able to give all the benefits offered by conventional banks and other financial institutions, such as services like interest on savings and loans (Donovan, 2012; Lochan *et al.*, 2010). Additionally, mobile money services increase productivity and efficiency by reducing wait times in banking

facilities. The majority of the countries in the African sub-region may be able to effectively experience growth in their trade, health care delivery, agriculture, and other economic sectors through the use of mobile money services, according to studies. Mobile money accessibility, where subscribers may quickly visit any mobile money office to complete any transaction, is one of the services that merchants offer to their potential subscribers. The ease with which mobile money users can conduct transactions without experiencing any issues or stress relates to the convenience of using mobile money (Oliver, 1997). Cash withdrawal, cash transfers, buying recharge cards, paying bills, and other services are provided by money mobile.

### ***2.1.2 Cash Withdrawal***

In recent years, mobile phone technology advancements have significantly changed economic life and raised the living standards of the masses through financial services including money transfers, cash deposits, and withdrawals in people's day-to-day commercial dealings (Oh, 1999). Mobile money providers and other networks to help those who do not have access to traditional banking services and to give them a way to keep money electronically as well have used the mobile money system.

Customers who do not use banks but who do have account numbers can use their mobile SIMs as accounts to make free deposits into their mobile wallets thanks to mobile financial services. The initial implementation of the transfer mechanisms was as an unofficial banking system using account numbers and electronic payments for goods and services (Oh, 1999). Remittances are typically moved from the informal route to a well-planned and formal route as a result of the system's provision of simple ways for people to transfer, pay, and receive payment for goods and services.

The usage of mobile money systems allows the informal cash economy to have a significant impact on regional economic growth through the local market with the diversification of commodities and manufacturing (Affla, 2012). While this is going on, users of mobile money services start to express satisfaction with the products and services, which further contributes to the expansion and sustainability of the mobile money industry (Oliver, 1997). Customers considered satisfaction to be their overall perception of a service provider or their response to what they expected, as well as the overall satisfaction they felt after having their specific goals, objectives, and wants fulfilling (Hansemark & Albinson 2004).

### ***2.1.3 Cash Transfer***

The term "mobile money cash transfer" primarily refers to a system for sending and receiving small amounts of money via a mobile device to and from other mobile users across the nation, in distant rural locations as well as internationally (Ivatury & Mas, 2008). Certain businesses regularly use mobile money services to improve their clients' traditional offerings. In comparison to real cash, both the sender and the recipient must pay a minimal or negligible cost. The mobile money system has emerged as the most affordable way for both the wealthy and the poor to conduct financial transactions, enabling people to send and receive money from friends and family in an efficient manner (Donovan, 2012).

Additionally, by avoiding the long lines in banking halls and lowering transaction costs as a result of minimizing leaks, and strengthening security, mobile money services increase productivity and efficiency (Donovan, 2012; Lochan et al., 2010). The majority of the countries in the African sub-region may be able to effectively experience growth in their trade, health care delivery, agriculture, and other economic sectors using mobile money services, according to studies. It has been determined that

mobile money does not give all of the benefits and services provided by the conventional banking system, including interest on savings, credit, and insurance on the value kept in the mobile account.

Since the advent of mobile money systems, internal migratory workers in cities have been able to transfer remittances to their far-flung and rural communities, which might otherwise struggle to find transportation and financial aid while relocating. The need to carry significant amounts of cash, especially during the time of expensive and long trips with the risks of this cash being easily stolen, is eliminated by using mobile money systems, according to research, which is safer and more secure than informal remittance channels (Omondi, 2013). Customer loyalty eventually results from financial transfers (Osei-Assibey, 2009).

#### ***2.1.4 Cash Deposits***

The majority of people stick to saving money in traditional banks instead of putting it into their mobile accounts when it comes to cash deposits. Other company models, which frequently accept mobile payments, developed as a result of the legislative environment, customer and consumer demographics, culture, and other relevant variables. Additionally, the majority of business models or activities are typically driven by partnerships, mobile carriers, or banks (Boer & de Boer 2010), in conjunction with increasingly sophisticated technology services that enable the operations for payment or service delivery.

Recently, a variety of mobile payment systems have been made available, giving full support to other large and important networks as methods of funding and payment between individuals. Most often, mobile payment companies and operators have found that users in less developed nations want to be able to pay for the operation of other phone accounts, notably those of friends and family members, between whom

remittances have been exchanged (Beccue 2009). The person receiving the talk time would typically like to cash it out to get the full value of the payment.

To manage liquidity and reduce risk, telecoms in global markets have primarily focused on offering prepaid services, especially in telecom-led models that do not rely on a bank partnership. This may be due to their lack of experience in managing credit risk associated with financial services. Most nations forbid nonbank payment service providers from taking client deposits or using money to finance payment activities, protecting consumers and reducing risk to the financial system (GSMA, 2009). Customers' levels of satisfaction and trust in the operation of mobile money services are much increased when they have access to ways of depositing their revenue.

#### **2.1.5 Purchase of recharge card**

The usage of the system to buy a recharge card from the mobile money service providers is another service provided recently by the mobile money operation. The purchase of traditional telecom cards for phone calls has substantially decreased since the launch of mobile money services, giving place to the purchase of recharge cards for calling credit renewals (Mantel, 2000). However, unexpected and creative uses of mobile money services have also evolved, including paying for social occasions like funerals and weddings, public transportation, taxi rides, and making informal loan repayments (Omwansa, 2009).

As a long-term success, the mobile money operation can significantly improve the amount of taxes and utilities collected, which can build the infrastructure and process of government as well as the economy's ability to grow and prosper (Scot et al., 2004). Due to the mobile system, where customers or subscribers can easily go and get the recharge cards for top-ups, buying recharge cards to activate the mobile

phones for calls and text messaging is normally done with great convenience these days.

Recent purchases of E.C.G prepayment credits, DSTv recharges, and other utility credits are easily paid for via the mobile money system, thereby minimizing the challenges involved in visiting the offices and premises of the utility provider. Convenience in accessing products and services enables organizations to have a competitive edge over their competitors, as such mobile money services assist customers in conveniently accessing the recharge cards as, and when the need arises (Baker 2002).

#### **2.1.6 Fraud**

Fraud is a purposeful error made by management or staff members of the organization. Fraud is harmful to others since it involves deceiving or tricking other people to benefit oneself or a group (ACFE, 2014). According to The Association of Certified Fraud Examiners (ACFE) (2014), there are three categories of fraud: asset theft or abuse of assets, fraudulent financial statements, and corruption. The first theory that can adequately explain the elements that lead to fraud is the fraud triangle theory. Cressey first put forth this notion in 1953. The three components of the fraud triangle are pressure, opportunity, and reasoning. Wells re-introduces the concept of the fraud triangle (2011).

According to Hunton et al. (2004), each of the three components—opportunity, incentive or pressure, and rationalization plays a separate role in the fraud. Later on, he goes on to explain that opportunity arises when internal controls are insufficient or when there is collusion, allowing the criminals to escape any kind of oversight. On the other side, pressure or incentive is what prompts someone to lie. Fraud, according to

Albrecht & Zimmerman (2012), is a result of a combination of pressure, opportunity, and rationalization. Fraud either occurs as a result of an immediate need for money or grows greater over time as fraud confidence rises. However, fraud was perpetrated because of external pressure, lax internal controls, and the characteristics of other honest people.

### ***2.1.7 Mobile Money Fraud***

Fraud involves mobile money's forms and causes. Since its launch, scammers have engaged in several fraudulent operations with the primary objective of undermining the value of the mobile money service to the general public. Mobile money fraud is an intentional act carried out by con artists or thieves to acquire an unfair advantage against mobile money customers, operators, and agents (Subex, 2017; Merritt, 2011). Scammers are well-trained in their use of the service's stakeholders as leverage. The con artists plot their schemes for a very long time, and they occasionally receive resources and technological support from cartels that make use of systemic flaws to their advantage (Maurer, 2012).

Mobile money fraud is an intentional act carried out by con artists or thieves to acquire an unfair advantage against mobile money customers, operators, and agents (Subex, 2017; Merritt, 2011). Scammers are well-trained in their use of the service's stakeholders as leverage. The con artists plot their schemes for a very long time, and they occasionally receive resources and technological support from cartels that take use of systemic flaws to their advantage (Maurer, 2012). Since its launch, scammers have engaged in a number of fraudulent operations with the primary objective of undermining the value of the mobile money service to the general public. Fraud in mobile money services has been categorized into three, namely:



1. **Fraud committed by users:** Before using mobile money services, subscribers must complete several steps, including registration. Unfortunately, some users sign up with the intent to do business using dubious methods and steal money from other users and mobile money providers. The activities of fraudulent subscribers affect unwary people with an estimated 50 percent of mobile money subscribers and mobile money operators being susceptible to the whims and caprices of the fraudulent subscribers. To advance and influence the transactions in their favour, they steal mobile money codes, SIM cards, PINs, and other pertinent information.
2. **Systems fraud:** System-related fraud encompasses all fraudulent activities that impact mobile money deployment via system flaws and processes. System-related fraud will affect a variety of stakeholders, including agents, businesses, and mobile money operators. System-related fraud is most prevalent when a platform lacks adequate controls to guide transaction processing. This fraud is prevalent during the transaction activation stage of the deployment and continues to grow into the value addition stage. Although numerous complex algorithms have been developed to assist telecommunications operators in achieving various goals, some of the operators lack some of this information technology (IT) systems specifically made for mobile money operations. Some of the systems are outdated and unable to keep up with the escalating difficulties posed by mobile money operations (Vlcek, 2011). These flaws allow con artists to go around the system and utilize it to defraud others for their money. Fraudulent IT professionals can also deceive others and hide their actions by manipulating the IT systems.

Mobile customers use mobile money services, and they must go through a lengthy registration process. Unfortunately, some users sign up with the intent to do business using dubious methods and steal money from other users and mobile money providers. Unwitting individuals are impacted by the actions of fraudulent subscribers, with an estimated 50% of mobile money subscribers and operators falling prey to the whims and caprices of the fraudulent subscribers. They steal SIM cards, PINs, mobile money codes, and other crucial data to advance and rig the transactions in their favour.

- 3. Employee and Agents' Fraud:** There are honest, ethical, reliable, and business-minded mobile money agents who are passionate about ensuring the success of the mobile money service. However, some people have set themselves up with the workers of the mobile money operators in order to deceive, manipulate, and benefit from the transaction procedures. To steal money from accounts and utilize it for their own gain, these con artists generate numerous fake accounts and passwords. For instance, in Ghana in 2017, 3,000 mobile money agents were punished after being discovered conspiring with mobile money users to defraud the mobile money companies (Khan & Bersudskaya, 2016).

Additionally, mobile money operators' staff members have been charged with assisting mobile money agents in stealing money from mobile money subscribers (Bersudskaya & Kuijpers, 2016). Common agent frauds include float loss in the agent's account due to illegal use, compromised PINs, and con games where fraudsters pretend to be MNO employees in order to get access to the agent's float account. Additionally, customers may defraud agents. For instance, fraudulent withdrawal reversals or phony monetary deposits. According to

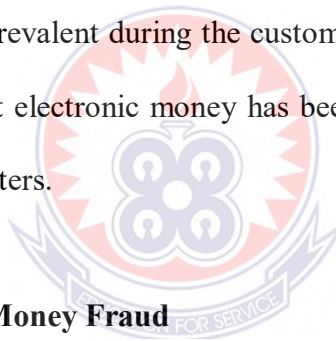
studies conducted by the Helix Institute in 2015, fraud is a major worry for many agents.

Agent-driven fraud is perpetuated from within the agent network. The fraud is initiated and carried out by agents or their employees. It includes agent employees defrauding agents, master agents defrauding their own sub-agents, agents defrauding customers, and agents defrauding the mobile financial service provider. Agent-driven fraud is most common at the start of a deployment, fueled by early pricing flaws. The fraud evolves over time, changing its form, victims, and impact on deployment.

4. **Consumer driven fraud:** Consumer-driven fraud is initiated by fraudsters impersonating customers. Agents, other consumers, businesses, and mobile financial service providers are all targets of consumer fraud. Consumer-driven fraud is the most common type of fraud in the market, and it occurs at all stages of deployment. It is more common during the transaction activation stage of the business, when consumers begin to trust the mobile financial service more, but do not yet understand many of the service's potential risks. Consumer education activities are the primary method of managing consumer-driven fraud, but there are numerous processes and system-based checks that can also help mitigate these challenges.
5. **Business partner related fraud:** Business partner-driven fraud refers to fraudulent activities carried out through the network of a business partner. Business partners include business-to-consumer (B2C), consumer-to-business (C2B), and merchants. Employees of the business organization, customers, and partner businesses of the mobile money operator may engage in fraudulent

activities. Business partner-related fraud is more common during the value addition stage of the deployment. This is primarily because business partnerships are developing at this stage. Because business transaction adoption is still in its early stages, this type of fraud is still in its early stages.

6. **Mobile financial service provider fraud:** This is a collection of fraudulent activities carried out by employees of mobile financial service providers. The fraudulent activities will be carried out without the business's permission. The most common types of fraud in this area are fraud on the mobile money operator and employees of mobile money operators defrauding agents, businesses, and consumers. Fraud in the ecosystem is less prevalent at the start of the deployment and becomes more prevalent during the customer activation and value stages. At this point, significant electronic money has been invested in the system, making it appealing to fraudsters.



### **2.1.8 Causes of Mobile Money Fraud**

**Poor employees' conditions of service:** the outcome of the key informant interview conducted revealed that poor conditions of service are the leading cause of mobile money fraud, especially employee and agent fraud. They complained that their salaries and commissions were insufficient, and to survive the economic downturn, they engaged in illegal activities to supplement what they were paid. Because of this condition, the cost of living in Ghana has risen, and financial crime has spread throughout the country.

Some mobile money agents and employees of mobile money operators deliberately conspire to defraud mobile money subscribers by diverting money or deducting money from accounts without the subscribers' approval. Some mobile money agents

and employees of mobile money operators provide fraudsters with insider information and security codes that allow them to manipulate the system and profit from it. They do all of this to supplement their meagre salaries from mobile money operators.

**Weak internal systems:** another cause of mobile money fraud is the weak internal systems of the mobile money service according to the key informant interview conducted. This is because some mobile money operators and their agents have very lax control systems that start at the top and work their way down. Employees and managers of mobile money operators can authorize transactions that have not been approved by their superiors, and some exceed transaction limits without seeking permission from the operator. Some agents send money to subscribers without keeping proper records. Some mobile money agents work in the open under trees and umbrellas, where thieves and robbers can easily attack them and steal their money. Some of the agents who work in the buildings have weak locks, no safes to keep the money, and no security devices; as a result, fraudsters have easy access to the buildings and steal physical cash from them.

**Outdated operating systems:** additionally, the outdated systems that are used to operationalize the mobile money service are another cause of mobile money fraud as revealed by the key informant interview conducted. According to the study's participants, mobile money fraud has thrived due to the outdated information technology systems used to provide mobile money services. Some IT fraudsters are skilled at hacking into systems and stealing money. This is due to inadequate system security. Employees have easy access to subscribers' passwords. There will be times when the IT systems will be down, jammed, or very slow, among other things.

**Weak enforcement of measures:** The National Communications Authority is responsible for ensuring that telecommunication companies in Ghana provide quality services to consumers, but they have little to do with the mobile money service. The Bank of Ghana has issued Electronic Money Issuers (EMI) guidelines to assist mobile money operators and agents, but these guidelines are limited and porous, allowing any fraudster to circumvent them. Proper legislative regulations with legal backing are lacking in the mobile money service. The EMIs are simply administrative regulations imposed by the Bank of Ghana, which is insufficient to detect and prevent illegal activity in the mobile money service. Some participants stated that the Central Bank has frequently failed to sanction mobile money operators for failing to comply with their regulations because the bank does not have the legal authority to control what the operators do.

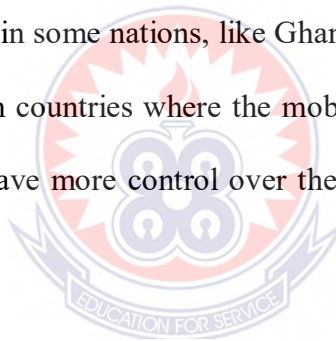
#### **2.1.9 Mechanisms to combat mobile money fraud by the key stakeholders**

Risk management strategies are being implemented for the mobile money service (Gilman & Joyce, 2012; Gilman & Singh, 2012; Merritt, 2011). The task of establishing policies to regulate the operations of the mobile money service falls on central banks (Maurer, 2012). The actions taken by central banks are based on comments made by different industry participants regarding some shortcomings in the rules that now govern the service. Before publishing a paper to help in formulating a policy statement, central banks request all of the major stakeholders' opinions on the service and thoroughly examine their opinions.

Over the years, mobile money carriers have contended that these policy guidelines are insufficient to support them in addressing the myriad risks connected to the service (Mas & Radcliffe, 2011). These challenges are clarified by central banks in their

yearly updates to the policy documents they create to help advance financial inclusion. Central banks provide training to mobile money providers on a variety of digital finance and e-commerce activities, as well as on money laundering, fraud involving mobile money, and the steps to be taken to stop it (Suárez, 2016). Additionally, central banks serve as a conduit between mobile money providers and the government and its different security organizations.

Banks have always served as financial intermediaries, managers of funds, and facilitators of financial transactions, among other functions (Bara, 2013). But there are several hazards involved in these trades. One of the financial innovation products that banks have added to their portfolio is the mobile money service (Markovich & Snyder, 2017). However, in some nations, like Ghana, banks act as fund managers for mobile money carriers. In countries where the mobile money service was created by the banks, they tend to have more control over the operations of the service (Singh, 2012).



These banks help MNOs diversify their revenue and investments to prevent having to handle their operations entirely in the future. Under the central bank's instructions, the banks administer the funds of the mobile money providers. The banks set strict criteria for mobile money carriers, train them, and provide them with instructions on how much cash their customers can withdraw. Banks maintain Know Your Customer (KYC) to eliminate fraudulent transactions. These days, banks have sophisticated software that can identify and protect payments from mobile money operators against scammers and cyberattacks (Narteh et al., 2017).

The central banks, beginning with Kenya (via M-PESA), have urged telecommunications companies to participate to promote financial inclusion and

entice the unbanked to join formal banking institutions (Merritt, 2011). Cooperation between telecommunications firms and their stakeholders is essential for chasing away fraudsters and maintaining the service (Klein & Mayer, 2011).

Gilman & Joyce (2012) state that the next crucial factor in regulating the service and catching fraudsters is the cooperation of mobile money carriers and their agents with security agencies. The establishment of efficient internal controls is a top concern for mobile money operators, who adhere fervently to industry norms and central bank directives. Regular internal training on mobile money services and better compensation plans are employed to increase employee and agent morale and reduce fraudulent activity. Mobile money providers also carefully adhere to KYC processes and routinely verify subscribers' accounts, passwords, and other data (Sorooshian, 2018).

#### **2.1.10 Mobile Money Ecosystem**

Safaricom, a Kenyan telecommunications company, launched M-Pesa, the country's first mobile money service, in 2007. (Botchey et al., 2020). Three (3) significant players dominate the mobile money ecosystem. The owner of a mobile money account, the telecommunications provider, the mobile money agents, and the mobile money employees. Users accumulate money in their wallets either through direct deposits or contributions from third parties (business associates, relatives, NGOs, etc.) (Botchey et al., 2020).

Peer-to-peer (P2P) accounts, mobile money agents, retail locations of telecommunications firms, and, more recently, a few chosen banks are the primary means of initiating deposits, withdrawals, and payments. A brief messaging service indicates when a transaction is accomplished (SMS). M-successful M-Pesa's rollout swiftly spread to more African nations and emerging market nations (Botchey et al.,



2020). In 2019, there will be two (2) billion US dollars' worth of transactions made by the more than 1.2 billion persons who currently have mobile money accounts worldwide. There were around fifty (50) million additional users from Sub-Saharan Africa (Botchey et al., 2020).

In comparison to the industrialized world, there are far more people without bank accounts in Africa and other developing nations. According to the World Bank Group, account ownership is almost ubiquitous in high-income economies, leaving almost no adult population in underdeveloped nations without a bank account (Botchey et al., 2020).

#### ***2.1.11 Impact of Fraud***

Fraud is not limited to mobile financial services; it occurs across the board. Nonetheless, because mobile financial services have a high potential for increasing financial inclusion and extending financial services to the mass market, fraud in this domain has far-reaching implications. In a variety of ways, fraud has a far-reaching impact on the mobile money ecosystem. If fraud is rampant and persistent, the service's credibility will suffer greatly.

When employees steal money from the system or agents have to pay to gain access to opportunities, the regulator may be forced to step in to protect consumers. Individual subscribers will be discouraged from using the services because they are afraid of losing money through fraudulent activities. Due to a fraud that occurred at the firm, the credibility of a leading Telco in East Africa's mobile money service was severely harmed.

Brand equity is essential for any company or organization. The values that define how an organization is perceived by the environment are represented by its brand. If fraud

has a negative impact on the organization's products, users will associate the brand with fraud, which may affect any other services or products offered by the organization. Fraud will, in some cases, lead to money laundering and associated criminal activities. This could include terrorism financing as a result of lax KYC in customer registration and the concealment of funds brought into the financial system by criminals using fictitious identities. Even though there is no evidence to suggest that this is occurring, mobile financial service providers should be aware of the risks.

Fraud also has a negative impact on innovation. Innovation includes opening up the platform to other systems / networks to increase the range of services. Because the entire ecosystem is concerned about the fraud that may result from innovation, providers will be less willing to take risks and innovate around mobile payments. In order to promote innovation, organizations may be forced to limit fraud within existing systems first, and then consider introducing new services.

The mobile financial system relies on agents to provide critical float and cash. This is the key that drives liquidity and, as a result, the availability of mobile financial services. Fear of loss will discourage agents from investing in float and cash if there is a high level of fraud in the system. Second, if fraudsters steal funds from their accounts and they are unable to reconcile any commissions earned against what the system shows, the agents will be unwilling to commit funds. Because it affects their ability to invest in the business, operators are increasingly collaborating with agents to manage fraud within their outlets.

## **2.2 Empirical Review of the Growth in Mobile Money Services: Global Perspective**

Mudiri (2013) undertook a study on mobile money services in India, Indonesia, the Philippines, Argentina, Kenya, Papua New Guinea, and Uganda. The study, which

used an exploratory research design involving interviews, concluded that financial education and capacity building were necessary components of a comprehensive strategy to address the dangers of mobile money fraud.

Rieke *et al.* (2013) evaluated the hazards in the industry of services that support electronic or mobile money service transactions. They specifically used a method for runtime predictive security analysis, which looks at process behaviour concerning transactions within a money transfer service and attempts to compare it to expected behaviour provided by a process model. They looked for abnormalities that would point to a probable abuse of the service for purposes of money laundering by analysing deviations from the specified behaviour. They assessed the practicality of the suggested strategy and supplied data on the computational and recognition capabilities of the predictive security analyser tool, which was developed using actual operational and simulated logs. The tests were designed to find abuse patterns indicative of a certain money laundering technique in synthetic process behaviour using attributes extracted from actual transaction events.

Adedoyin *et al.* (2017) put a better case-based reasoning (CBR) technique forth for identifying fraud in the mobile money service. They argued that utilizing machine learning to evaluate the sample size of instances leading to the detection of anomalous and fraudulent actions improves basic CBR capacity. Instead of using the conventional dimensions of time and transaction amounts, they divided subscriber behaviour into five contexts and then combined them into a single dimension. They also suggested that the CBR strategy might work better if simulation data were used. Their findings demonstrated that weighted and combined dimensions outperform those measured independently.

According to Kanobe et al. (2017), the development of mobile money services has aided the unbanked in emerging economies in their efforts to access formal financial services. They said that this situation was brought about by lax regulatory standards, which encouraged the growth of fraudulent transactions. They evaluated the administration of the mobile money service using an interpretive qualitative approach based on Activity Theory (AT) with a focus on information security rules, regulatory papers, and processes. Their findings illustrated the reasons why mobile money services in emerging economies have insufficient information security management. Additionally, they described the functions performed by mobile money operators' workers in maintaining the service's information security.

### **2.3 Security threats to Mobile Phone and Mobile Money**

Some of the factors affecting mobile device security are loss, theft, improper disposal, unauthorized access, and malware. Because mobile phones are small, the likelihood of them being lost, misplaced, or stolen is very high, making them an easy target for theft. To prevent exposure to sensitive data that may be stored on or accessible from mobile phones in the event of theft, proper measures must be put in place to restrict unauthorized access to mobile phone data.

According to a survey of taxi companies in Sweden, the United Kingdom, Australia, Denmark, France, Germany, Norway, Finland, and the United States, tens of thousands of digital devices (including mobile phones) were left behind (Checkpoint, 2005). Aside from the compromise of logical and physical data, a mobile phone with active service, such as mobile money service, could be accessed without authorization, resulting in money theft from mobile money wallets. Furthermore, even if the contents of the user stored on the phone are wiped away, the mobile phone itself

may have significant financial value, can be manually restored to its original settings, and reused easily.

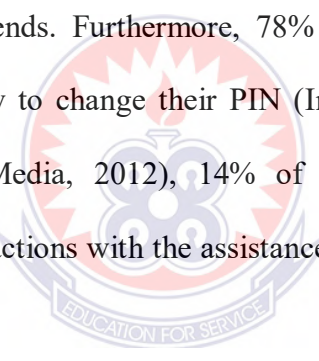
PINs, patterns, and passwords are the user authentication mechanisms available on mobile phones. While these authentication mechanisms are not perfect, they are the first line of defense against unauthorized mobile phone access. Access to mobile phones and their contents, on the other hand, can be gained by forging or guessing the authentication credentials or completely bypassing the authentication mechanism. Surprisingly, most mobile phone users rarely use the built-in security mechanisms, and when they do, they frequently use settings that are easily guessable, such as 1234 or 0000 (Knijff van der, 2002).

Another avenue that could be exploited is flaws in the authentication method. This is due to the fact that some devices have a master password built into the authentication mechanism that, when entered, allows unlimited access, including bypassing the security lock set by the user (Knijff van der, 2002). Some of the methods for obtaining master passwords are: calculating it directly from the equipment identifier (Jansen and Ayers, 2007), using a backdoor to bypass all or part of the control mechanism and forensic tools that can be used to bypass built-in security mechanisms in order to recover the contents of a mobile phone.

Malware is another threat to mobile device security. Mobile phones are sometimes infected with viruses and other types of malware via communication networks. Malware can spread in a variety of ways, including attachments to SMS messages, internet downloads, and Bluetooth messages. Malware can eavesdrop on user input and steal sensitive information stored on a mobile phone, as well as be used to grant an attacker unrestricted access.

Another study in Kenya (Githui, 2011) concluded that while mobile money operators had company and industry principles guiding them, they had not been implemented and fully adopted, leaving the possibility of technologically savvy people using their technologies to achieve their illegal targets of fraud and scam. For example, an average of 18% of respondents in a 2,980 household survey in Tanzania had money stolen from their m-money account because of fraud or a swindle (InterMedia, 2013).

According to the Tanzanian survey, 33% of households shared their mobile money PIN (password) with others. One-third said they shared their PIN "always," and another quarter said they shared it "very often. About 55% of those who shared their PINs did so with agents, while 45% shared them with close family members such as spouses, siblings, and friends. Furthermore, 78% of those who shared their PINs reported not knowing how to change their PIN (InterMedia, 2012). According to a Tanzanian survey (InterMedia, 2012), 14% of mobile money users may have conducted m-money transactions with the assistance of an agent and may have shared their PINs with the agent.

The logo of the University of Education, Winneba, is a circular emblem. It features a central shield with a book and a torch, surrounded by a sunburst pattern. Below the shield is a banner with the motto "EDUCATION FOR SERVICE". The entire emblem is set against a red and white background.

### **2.3.1 Safeguards against Security Threats**

The first safeguard is to use threat scenarios to identify and deal with potential threats. Mobile wallet applications designed for mobile money services must be thoroughly examined to identify threat scenarios such as spoofing, tampering, repudiation, and information disclosure. Protecting sensitive information stored on a mobile phone, such as account numbers or authentication data (passwords or PINs), is an important consideration (Hoseph & Anpalagan, 2007).

Furthermore, sensitive data exposure could be reduced by not storing sensitive information such as personal and financial account information on a mobile phone.

Sensitive data should be kept on removable memory cards and stored separately from the device. Another important safeguard is keeping control of a mobile phone that uses mobile money. It must be handled with care, just like a credit card, by maintaining control at all times and securely storing it if left unattended. In addition to the cost of the mobile phone, its loss or theft may expose confidential information stored on the phone to theft.

Preventive and detective mechanisms can also be used to defend against malware and other types of attacks. Most mobile phones already have a variety of these mechanisms that can improve phone security. It should be noted, however, that add-on security software may contain or introduce flaws and should be thoroughly tested before use (Fogie, 2006).

According to a research study on privacy and security concerns associated with mobile money in Africa, mobile money users play an important role in securing their mobile money. The failure to pay attention to basic security features on users' mobile phones exposes them to a variety of threats, the most serious of which is financial loss if an attacker gains physical control of the phone. Furthermore, security is a two-way street between the user and the service provider because a technically adept adversary may be able to exploit poor security design within mobile money apps or circumvent poorly implemented encryption (Harris et al., 2013).

A study conducted in Africa to identify the security concerns of mobile money users revealed that if the user does not pay attention to the security of the mobile phone, the user may be vulnerable to criminal activity (Harris et al., 2013). This was confirmed in a study of 2,000 Tanzanian adults, which also revealed that both users and nonusers

are concerned about the security of mobile money, fearing losing money from their mobile wallet if their phone is misplaced or stolen (InterMedia, 2012).

#### **2.4 Growth of Mobile Money Services in Ghana**

In July 2009, MTN, Ghana's largest telecommunications service provider, collaborated with nine banks to launch mobile money services in accordance with the Branchless Banking Guidelines (Nicco-Annan, 2021). According to the guidelines, it could only act as a bank's agent. All MTN mobile money accounts were linked to one of these nine banks. MTN spent a lot of money to raise awareness of the service by sending merchants to unbanked and underserved areas of the country to educate and market mobile money (GSMA, 2022).

All of the merchants who penetrated Ghana's unbanked geography were from partner banks with an interest in those areas. Each mobile money account opened by a merchant represented an account at the bank for which the merchant worked. However, registering customers and opening accounts presented another challenge. Customers were required to present a valid national ID in order to register, which slowed the registration process for many (GSMA, 2022). Registrations had to be a scheduled event rather than a service that could be performed immediately after a customer expressed interest (Nicco-Annan, 2021).

Despite this, some factors made mobile money accounts more appealing to the unbanked than traditional bank accounts. They required less Know-Your-Customer (KYC) and were less expensive to use (Nicco-Annan, 2021). Merchants were also more accessible to the unbanked, with some branches reaching rural areas. MTN had approximately 20,000 registered mobile money subscribers as of October 2009 (Nicco-Annan, 2021). However, MTN was unable to operate mobile money on the



scale and in the manner that it desired because the partner banks made the majority of operational decisions (Archie et al., 2021).

In 2015, the Bank of Ghana issued the Guidelines for E-Money Issuers and Agent Guidelines after reviewing the Branchless Banking Guidelines. The Branchless Banking Guidelines were replaced by these guidelines, which established new protocols for mobile money operations (Archie et al., 2021). The guidelines were issued by the Bank of Ghana (2022) as part of a larger strategy to create an enabling regulatory environment for efficient and safe digital payment and funds transfer mechanisms, as well as to "promote the availability and acceptance of electronic money as a retail payment medium with the potential to increase financial inclusion" (Archie et al., 2021).

The Dedicated Electronic Money Issuer (DEMI) status was introduced in the E-Money Issuer Guidelines, which an institution could obtain by obtaining a license to issue e-money alongside licensed financial institutions (Ifeanyi-Ajufo, 2022). This allowed telcos to gain the ability to issue money to customers for transactions without having to link each mobile money account to a bank account. The E-Money Issuer Guidelines establish system and control standards, as well as technology and security requirements for DEMIs.

It also established general operational provisions for DEMIs, such as mobile money account types, transaction limits, permissible transactions, KYC requirements, capital and liquid fund requirements, and consumer protection principles, among other things (Ifeanyi-Ajufo, 2022). Many of these requirements and operational rules are now part of the Payment Systems Act 2019 (Act 987), which governs digital financial service providers.

The Agent Guidelines essentially changed the definition of "agent" from the definition outlined in the Branchless Banking Guidelines and provided new operational guidelines to complement the Bank of Ghana's new e-money guidelines and payment systems structure (Ifeanyi-Ajufo, 2022). The 2015 guidelines had the practical effect of freeing telcos from the role of agents and giving them the option to be principals in the relationship. Although telcos are no longer required to act as bank agents, beneficial partnerships between telcos and some banks still exist to facilitate transactions between mobile money accounts and bank accounts, as well as payments for services (Ifeanyi-Ajufo, 2022).

MTN's success in entering the mobile money market, as well as the enabling regulatory environment, inspired other Ghanaian mobile network operators to follow suit. Tigo Cash debuted in October 2010, followed by Airtel Money in 2011 and Vodafone Cash in 2015. (Ifeanyi-Ajufo, 2022). Airtel and Tigo merged in 2017 to form AirtelTigo (Nicco-Annan, 2021). Because of mobile money and mobile banking, mobile phones officially became the most widely used medium of payment in Ghana by 2019. (GSMA, 2022). At the end of 2018, mobile money dominated the landscape, with 32.5 million registered accounts (up from 23.9 million in 2018) and 13 million active users (GSMA, 2022).

MTN Ghana also established Mobile Money Limited, a subsidiary in charge of mobile financial services. MTN has held a market share of more than 80% since 2017, and it continues to dominate the mobile money market to this day (Ifeanyi-Ajufo, 2022). In 2020, the Ministry of Communications and Digitalization (MOCD) revealed that MTN controlled 75% of the telecom market, classifying it as a significant market power (SMP) (Ifeanyi-Ajufo, 2022). The MOCD also revealed that MTN controlled

approximately 94 percent of the mobile money market share; this is because other telcos pay MTN interconnect fees (Ifeanyi-Ajufo, 2022).

MTN's SMP status allows the National Communications Authority (NCA) to enforce provisions of the Electronic Communications Act 2008, such as establishing a price floor or ceiling for associated mobile money costs in order to maintain a competitive market and level the playing field for all telcos (Ifeanyi-Ajufo, 2022). AirtelTigo, on the other hand, was formed through a merger to create a more powerful telecommunications network. However, in 2020, the entity's parent companies chose to sell their shares to the government (Henry, 2022). Since the sale was completed in November 2021, it remains to be seen whether operating under government management will benefit or harm AirtelTigo.

The government's previous failure to successfully manage Ghana Telecom, the country's first government-owned telco, resulted in the privatization of Ghana Telecom, which is now Vodafone Ghana. Since 2020, Vodafone Ghana has also made efforts to increase financial inclusion by allowing Vodafone Cash users to send and deposit money free of charge (Henry, 2022). This initiative was made possible by the interoperability of mobile money (Ifeanyi-Ajufo, 2022). Vodafone was the first company to launch a free peer-to-peer service in order to gain a competitive advantage and increase financial inclusion.

Like many other developing nations, the majority of the people in Ghana does not use any institutional financial services, such as banks or credit unions. Before MoMo entered the Ghanaian financial system, people sent money to their relatives via bus drivers, but they frequently had to pay exorbitant commission fees before the money

could be sent (Bampoe, 2015; Tobbin, 2012). Unfortunately, paying exorbitant fees did not necessarily ensure that the money would arrive safely at its intended location.

There were always numerous and various sources of disappointment, including frequent vehicle breakdowns, robbery attacks on moving targets, and the delayed transfer of monies, among others (Tobbin, 2012). Therefore, the MoMo payment system was used due to its benefits of easy, safe, and affordable transfers as opposed to the conventional way. The banks that issue the physical money to consumers in the current MoMo landscape, which is dominated by profit-maximizing mobile money operators (MMOs), hold the electronic money that the MMOs issue. As a result, the Central Banks hold the corresponding amount of physical money to back the electronic money that MMOs issue to their clients.

While the Bank of Ghana controls and regulates all MoMo activities, the National Communication Authority (NCA) is responsible for monitoring the security of the customer data that mobile network operators (MNOs) acquire as well as the reliability of the technologies those MNOs employ (Bank of Ghana, 2017). Customers can change cash to electronic money and vice versa with the assistance of MNOs. They have numerous agents all around the nation who help with this procedure. Currently, several banks have been successful in effectively connecting their clients' accounts to their MoMo wallets to improve how convenient the banking service is to use (Bank of Ghana, 2017).

The Bank of Ghana emphasized the need to promote mobile payment in its regulations to banks and savings and loan companies in 2008, claiming that it may be utilized to significantly improve financial services outreach to the unbanked groups in Ghana. The Bank of Ghana stated that "financial institutions cannot take on

branchless banking without the help of other market players like telecom companies, technology service providers, agents, etc." as part of its strategy to establish an enabling regulatory environment to promote MoMo payment systems in Ghana (Bank of Ghana, 2016).

As a result, financial institutions and the telecommunications sector can collaborate to offer branchless banking services to the unbanked. Following the Bank of Ghana's publication of these instructions, major players in the Ghanaian telecommunications market like MTN, Vodafone, and AirtelTigo have made deliberate attempts to roll out MoMo service to all Ghanaians, both in the official and informal sectors. Following the 2008 legislation, MTN introduced its MoMo service in the nation in July 2009. Airtel launched its MoMo service in March 2010, while Tigo followed suit in October with the launch of its "Tigo Money" service. With "Vodafone Cash," Vodafone entered the MoMo market in July 2015 (Saliu, 2015).

According to the Bank of Ghana, MoMo subscriptions and active users are rising steadily yearly. In a similar line, MoMo transaction volume and value are both rising. For instance, the number of registered MoMo consumers climbed from about 3.8 million to 24 million between 2012 and 2017. The information also showed that there were more active MoMo consumers overall (from 345,434 to 11.1 million). While the overall number of MoMo transactions climbed by roughly 5,340% during that time, their value increased by as much as 26,131%. The amount of the remaining float rose from GHC 19.6 million to GHC 2,321.1 million (Bank of Ghana, 2016).

## **2.5 Regulatory Environment of Mobile Money Services in Ghana**

The Bank of Ghana has supervisory and regulatory authority over banks and all other financial institutions, and it oversees their licensing and operation through various

acts of parliament relating to financial services (Ifeanyi-Ajufo, 2022). The Bank of Ghana's Banking Supervision Department oversees banks, while the Other Financial Institutions Supervision Department oversees financial institutions that are not banks. The Payments Systems Department oversees telcos' financial activities, particularly their mobile money operations (Ifeanyi-Ajufo, 2022).

The Payments Systems Department also handles payment system licensing, monitoring, and onboarding for telcos (Ifeanyi-Ajufo, 2022). The Fintech and Innovations Office oversee payment and financial technology service providers. Telecommunication services provided by telcos, on the other hand, are supervised and regulated by the NCA rather than the Bank of Ghana. The NCA regulates telecommunications companies by issuing operating licenses, ensuring fair competition among licensees, monitoring service quality, establishing equipment standards, and mandating safeguard mechanisms (Ifeanyi-Ajufo, 2022).

To maintain control over the rapidly evolving financial sector, new and improved legislation has been enacted to replace previous legislation deemed unsuitable for the current financial services industry. For example, the Payment Systems Act of 2003 (Act 662) was repealed and replaced by the Payment Systems and Services Act of 2019 (Act 987). (Henry, 2022). These acts, together with the Non-Bank Financial Institutions Act 2008 (Act 774), have given the Bank of Ghana the authority to license, regulate, and supervise financial sector developments. Under the Payment Systems Act (Act 987), telcos that offer mobile money services are considered payment system providers, and their licensing and regulation are the responsibility of the Bank of Ghana (Ifeanyi-Ajufo, 2022).

In Ghana, the Payment Systems Act governs DFS or payment system services. It unifies the laws governing payment systems and payment services and regulates institutions that provide payment services and electronic money. It is a criminal offense under the Payment Systems Act to operate a payment service business without a payment service license from the Bank of Ghana (Henry, 2022).

Ghana also passed the Banks and Specialised Deposit-Taking Institutions Act 2016 (Act 930) in 2016, which regulates deposit-taking institutions and consolidates deposit-related laws. While banks and nonbank institutions licensed under Act 930 are not required to obtain a license to operate a payment system, they must apply for and receive authorization from the Bank of Ghana to offer services (Ifeanyi-Ajufo, 2022).

Other legislation, such as the Data Protection Act 2012, governs payment service providers (PSPs) in addition to Act 987. (Act 843). To apply for a PSP license, you must first register with the Data Protection Commission and obtain a data protection certificate (which in turn is a requirement for businesses to acquire licenses or registration to operate in Ghana). In accordance with the Anti-Money Laundering Act 2020 (Act 1044), applicants for a PSP license must also submit an anti-money laundering policy as part of their application (Ifeanyi-Ajufo, 2022).

Nicco-Annan believes (2021). The policy outlined the KYC processes, internal reporting procedures, and compliance measures. PSPs must also submit a cybersecurity policy to the Bank of Ghana as part of their license application in order to comply with the Cybersecurity Act 2020. (Act 1038). The cybersecurity policy that is submitted must include key performance indicators or strategies that highlight cybersecurity awareness (Nicco-Annan, 2021).

The Cybersecurity Act 2020 also created the Cyber Security Authority to oversee cybersecurity in Ghana. The board of the authority is made up of the ministers of communication, defense, national security, and the interior. The authority is required to establish sectoral computer emergency response teams (CERTs), including for the banking and finance sector, to ensure good coordination in cybersecurity incidents (Nicco-Annan, 2021). The MOCD established the Ghana National Computer Emergency Response Team (CERT-GH) in August 2014, primarily to respond to cyber infractions on government networks, but it also serves the private sector (Ifeanyi-Ajufo, 2022).

## **2.6 Drivers of the usage of MoMo Services**

Most studies have discovered that the intention or actual adoption of MoMo services is influenced by a variety of factors, some of which have been predicted by technology adoption theories. In addition to these variables, studies have discovered that demographic characteristics such as age, gender, and education moderate adoption (Venkatesh et al., 2003; Maduku, 2013).

### **2.6.1 Gender**

Males, according to research, are more daring and likely to be early adopters of financial innovations than their female counterparts (Jambulingam, 2013). Males are also found to be more creative than females (Demirci & Ersoy, 2008). As a result, they are more likely than females to be early adopters of financial innovation.

Empirical studies have shown that women are more anxious/cautious about adopting and using new technologies, particularly in the early stages, and this affects their adoption attitude (Lee, Hsieh & Hsu, 2011). Gender was also found to be a significant moderator of technology adoption in China by (Wang et al. 2017). When examining



the relationship between perceived ease of use, enjoyment, and intention to use a printing technology, gender emerged as a significant moderator.

While many studies have found that gender is a significant moderator of technology adoption, others have found that gender has no significant moderating effect on financial innovation adoption and use. Hernández et al. (2011) and Lee et al. (2011) found no statistically significant moderating role for gender in determining attitudes toward technology adoption and use.

However, according to Chawla and Joshi (2018), culture has a significant impact on the level of involvement of females in financial decisions. Using India as a case study, they discovered that in most rural communities, males are encouraged to engage in financial activities from childhood, while females are pushed to the sidelines. As a result, males have a cultural advantage in adopting financial tools earlier than females.

### **2.6.2 Age**

According to the literature on technology adoption, attitudes toward technology adoption differ across three major age groups: youth, adults, and the elderly. According to Chawla and Joshi (2018), older people prefer traditional face-to-face financial transactions to adopting new technology for financial transactions. When compared to the youth, older people are more skeptical of financial innovations (Lee et al., 2011; Demirci & Ersoy, 2008).

The older generation's low adoption is primarily due to their lack of expertise in the use of mobile phones, computers, and the internet. Further research has revealed that, when compared to the youth, older people are more likely to feel unsure and uneasy about using technology-based financial services (Demirci & Ersoy, 2008). According to research, youth adoption of mobile financial services is high, owing to their high

use of mobile phones. Mobile phones are easily accessible, portable, and entertaining, with numerous multimedia features and information sharing applications that cater to the youth's lifestyle.

Empirical studies conducted in countries such as Botswana (Lesitaokana, 2016), Holland (Peters & Allouch, 2005) and Australia (Carroll et al. 2003) have all discovered an increasing rate of mobile phone adoption among the youth, primarily because it is affordable, portable, and attractive, and provides them with many options to perform many tasks at their own convenience.

Studies conducted in African countries such as Rwanda (Donner, 2005), and Burkina Faso discovered similar factors (Hahn & Kibora, 2008). This rising usage has a positive impact on the adoption of mobile phone-based applications, the most prominent of which is money financial services (MFS). Many empirical studies have found that age is a significant moderator of technology adoption (Yi et al. 2005). Age is a significant moderator of users' assessments of the usefulness, cost, and quality of MoMo services in terms of adoption.

### ***2.6.3 Education***

Increasing levels of education have been found to be positively correlated with increased chances of technology adoption. Higher education increases people's knowledge and confidence in using technology (Riddell & Song, 2017), so early adopters of technology are more likely to be highly knowledgeable.

Many empirical studies have supported Rogers' assertion, finding that early adopters of technological innovation tend to be people with more education and experience. People with low levels of education are typically restricted from using technology due to a lack of knowledge and expertise.

People with higher levels of formal education, according to Weijter et al. (2007), are typically exposed to certain technologies such as computers and the internet, whether as part of their learning process, work, or daily activities. According to empirical research conducted in Nigeria and Ghana, the higher one's educational level, the more likely one is to use MoMo services (Osei-Assibey, 2015).

#### ***2.6.4 Income levels***

Many studies in various fields have discovered a link between income and financial innovation adoption. In Jordan, AbuShanab and Pearson (2007) discovered that the likelihood of adopting e-banking was highly associated with higher income levels. Higher income quintiles are more likely to use e-banking, owing to their desire for easy access to their earnings. They discovered that those in the highest socioeconomic wealth quintile were more likely to use e-banking than those in the lower income quintile. The majority of those with higher incomes also had higher education. Thus, people with higher incomes are more likely to adopt financial innovation than those with lower incomes in South Africa.

Domeher et al. (2014) discovered no significant relationship between income and the likelihood of using a financial innovation in Ghana. They explained that the adoption of a financial innovation is dependent on a combination of income and other factors such as education. As a result, someone with a higher income but illiteracy may find it difficult to use financial innovations such as e-banking.

All of the above demographic characteristics are rarely evaluated in isolation. They are typically evaluated together. Individual demographic characteristics such as age, educational level, and income level have a significant moderating effect on the

adoption of mobile financial services, according to recent studies in Saudi Arabia and Tanzania.

Gender, on the other hand, had no significant moderating effect on mobile financial service adoption in either study (Alkhaldi & Kharma, 2018; Abdinoor & Mbamba, 2017). Some studies discovered a link between marital status and mobile phone-based applications, while others discovered none. According to some studies, married people are more likely to use mobile financial services than single people. Others have discovered no link between marital status and the use of mobile financial services (Gan et al. 2006).

Some empirical studies have discovered a positive relationship between residence location and MoMo adoption. According to McKay and Kaffenberger (2013), people living in cities are more likely to use MoMo than people living in rural areas. Balan et al. (2009) attributed the low rural adoption rate to structural and technical rigidities such as a lack of network coverage, which is one of the most important facilitating conditions required to influence adoption.

## **2.7 Importance of MoMo Service**

In terms of formal bank account use, few empirical studies on the effect of MoMo adoption on formal account use exist. Mbithi and Weil's study is the only one known to have attempted to investigate the effect of MoMo on people graduating to using formal accounts (2014). They discovered that in Kenya, the use of MoMo (M-Pesa) increases the likelihood of users becoming banked.

According to studies, there is at least one person in every four households in developed countries such as the United States who is either underbanked or unbanked. These families typically obtain some or all of their financial services outside of the

formal banking system. The majority of unbanked households have never opened a bank account. The most basic and common reason given for the absence of any bank account is a lack of funds to operate a bank account. They may also indicate that they do not require a bank account (Burhouse & Osaki, 2012).

Fanta and Mutsonziw (2016) discovered that even in countries with high rates of financial inclusion, there are still gender gaps in access to and use of formal financial services. This is primarily due to the fact that female-owned businesses face more financial constraints than male-owned businesses (Demirgüç-Kunt et al, 2015; Henderson et al. 2015).

Several studies have found that people with higher education have a higher probability of becoming financially included than people with lower education (Demirgüç-Kunt et al, 2018) in countries such as China (Fungáčová & Weill, 2015), Argentina (Tuesta, Sorensen, Haring, & Camara, 2015), India (Chithra & Selvam, 2013), and Peru (Camara & Tuesta, 2015). Higher education holders are considered to have the financial ability to hold bank accounts, and they can also provide personal guarantees and collaterals required by banks to access loans. Higher education is also linked to greater socioeconomic well-being (Lotto, 2018).

MoMo service meets the needs of the poor by providing a service that is compatible with their way of life, thereby increasing their ability to save (Ouma, Odongo & Were, 2017). Jack and Suri (2014) discovered that M-Pesa users can absorb relatively large income shocks without significantly reducing their household consumption by saving through their MoMo accounts. These shocks include, among other things, unexpected illness, job loss, livestock death, and unexpected harvest failure.

The study, on the other hand, discovered that when non-M-Pesa households experience unexpected shocks, their consumption drops by as much as 7% on average. Other research in Kenya has found that the use of banking products and services accessed via mobile phone (known as mobile banking) is largely limited to people in the top income quintile (Demombynes & Thegeya, 2012).

Demombynes and Thegeya (2012) discovered that the poor, who typically do not have any formal accounts, primarily use mobile phone savings. MoMo (M-Pesa) account holders were more likely to save than non-M-Pesa account holders. They discovered that M-Pesa increases the likelihood of saving and the amount saved, despite the fact that the service does not pay users interest on their savings. When compared to interest payments, users' savings motivations are driven by convenience and safety. Jack and Suri discovered these elements as well (2011).

According to Mbithi and Weil (2014)'s research, using MPesa reduces the likelihood of people using informal savings mechanisms. Informal savings groups in Nairobi move their savings into M-Pesa accounts primarily because funds in M-Pesa accounts are time and cost-effective to access at their leisure. According to Jack and Suri (2011), 90% of early M-Pesa users use the service as a savings tool, owing to its security, privacy, ease of use, and lower transactional costs.

Ouma et al. (2017) discovered that MoMo is a financial service that increases the likelihood of households saving as well as the amount saved in a recent study conducted in four Sub-Saharan African countries (Kenya, Uganda, Malawi, and Zambia). They attributed the growing volume of savings to the fact that MoMo users can deposit any amount of money they receive as many times as they want into their wallet, and transactions are convenient.

## 2.8 Challenges of MoMo usage

MoMo, like any other technology, is not without its difficulties. According to Hoofnagle, Urban, and Li (2012), the fundamental challenge is for MoMo operators to persuade both sellers and consumers of the utility of the service. The service providers must be able to persuade the service sellers to build and improve on their existing infrastructure so that product consumers can obtain the enabling environment or framework to use the MoMo. Adoption cannot occur until the seller is convinced that the system is profitable and the consumer is convinced that the system is useful to his or her livelihood.

Certain challenges have been discovered to have negative consequences for users and potential users after adoption. Network outages are one such challenge. Balan et al. (2009) discovered that adoption is very low in areas with no or unstable network coverage because the system requires network coverage to function. Stormy weather conditions, according to Balan et al. (2009), can disrupt the network system, causing transaction delays.

According to Bampoe (2015), the main challenge for MoMo users and potential users in Ghana is network failure. Delays in a MoMo payment system, particularly during network outages, can 'be disastrous, especially in case of an emergency that requires money immediately.' Otieno & Liyala (2018). In Kenya, Otieno & Liyala (2018) discovered that many traders still use cash for their transactions rather than relying on the MoMo payment system because they do not trust the system. Trust is still a major factor in MoMo adoption. They also discovered that some people have not adopted the system because they lack the necessary prerequisite (an ID card) to register for the service.

There are few or no agents in some areas, particularly in rural areas. Where there are agents, they usually do not have enough cash or float to serve the customers, primarily for security reasons. Because of the high illiteracy rates in many developing countries and communities, most people lack the necessary skills and even information to access and use the platforms' services. Some people are even unaware of the existence of such services or lack the necessary information to process the information and make a decision to use the service. Some people are also restricted from using the service, primarily due to language barriers (Otieno & Liyala, 2018).

According to an economic survey conducted by the Government of Kenya, the challenges confronting the adoption of MoMo and other technologically driven financial services include a lack of I.T. skills and infrastructure, as well as a lack of information. There are also limited or inadequate mechanisms for disseminating information, even when it is available (Government of Kenya, 2003).

## **2.9 Theoretical Review of Pentagon Theory**

In this study, the Pentagon Theory was adopted to explore the forms of MoMo fraud strategies experienced and framework for fraud detection put together by the Telco's and consumers of MTN mobile money services. The most recent theory, which complements the fraud triangle theory and fraud diamond theory, is the fraud pentagon theory.

The fraud pentagon hypothesis (also known as Crowe's fraud pentagon theory) is an updated theory that addresses the elements that cause fraud. The fraud pentagon idea, first put forth by Crowe in 2011, is an expansion of Cressey's fraud triangle theory from 1953. According to this idea, competence and arrogance are two more



components of deception. This fraud pentagon theory's definition of competence is equivalent to the definition of capability that was just provided.

According to Wolfe and Hermanson (2004), competence/capability refers to a worker's ability to disobey internal controls, devise a covert plan, and manipulate social circumstances for personal gain. Arrogance, on the other hand, is the attitude of superiority stemming from the possession of specific privileges and the conviction that one is exempt from business internal controls or policies. If the regulators are competent at applying the rules, fraud won't ever occur.

Employees, in particular, are motivated to commit and conceal the fraud by pressure from both financial and non-financial incentives. In 2012, Albrecht and Zimbelman categorized pressure into four major categories. These include pressure from money, vices, work-related pressure, and additional pressure. Financial considerations result from avarice, the desire to upgrade one's lifestyle, or economic demands brought on by the high standard of living. While non-financial reasons, such as injustice between coworkers, workplace annoyance, and cover-ups for subpar performance, result from demands at work.

Opportunity is a factor that will give people the chance to conduct fraud due to their lax controls. Lack of controls, inability to assess performance quality, failure to punish fraudsters, lack of information access, ignorance, indifference, inability, and absence of an audit trail are the six main reasons that create opportunity. There are opportunities because the offenders think their behavior won't be noticed, claims Aprillia (2017).

Companies with poor internal control systems, poor managerial oversight, lax sanctions, and ambiguous procedures are typically where opportunities arise. The

existence of thoughts that can lead someone to explain actions even when they are incorrect is known as rationalization. According to Aprillia (2017), fraudsters will seek out rational justifications for their behavior. An attitude that justifies fraudulent conduct has been used is rationalization. Fraud is committed based on the justification that the action was not unlawful. (Crowe, 2011).

### ***2.9.1 Relevance of Theory to the study***

The capacity for personnel to conduct fraud is known as competence. Therefore, mobile money fraud is allegedly committed by breaching corporate internal controls, creating embezzlement plans, and going ahead to commit fraud such as scamming mobile money users. According to Crowe (2011), competency in fraud is the ability of an employee to disobey internal rules, devise a concealment plan, and take note of the social circumstances that will best serve his interests.

According to Crowe (2011), arrogance is having a sense of superiority over others and believing that internal controls and business policy do not apply to her. A trait of superiority or arrogance and hence people who are arrogant and have a high level of confidence are convinced that internal rules did not apply to them are likely to commit mobile money fraud. This is because arrogant nature results from the offender believing that he has no control over his ability to perpetrate fraud and that he is therefore free to do so without fear of repercussions. This assumption is probably accountable for the scamming of UEW Students of their mobile money using MTN as a cover.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.1 Introduction**

The research approach presents the groundwork for gathering and evaluating data. This chapter explores the research design, methods, tools and techniques that aided in the selection of the study area, preparation of research instruments, data collection and analysis. First, the philosophical bearing that influence the chosen research model for data collection and analysis to address the various research questions as discussed.

It appraises the argument on qualitative and quantitative methods and provides validation for the combination of the two in this research (mixed method). The adopted research process and the sampling strategy, the researcher's role as well as the ethical considerations sustaining this research are also presented in this chapter.

#### **3.2 Research Philosophy**

Research philosophy is about the development of knowledge and the nature of that knowledge and the two fundamental philosophical assumptions that explain the nature of knowledge are epistemology and ontology. The philosophical basis in a research is vital because it communicates to the researcher about the method of data collection and analysis (Sanders et al., 2009). Bryman & Bell (2007) argue that epistemology holds the belief of what comprises satisfactory knowledge in a particular field of study. Positivism and interpretivism are two fundamental epistemological bases, which are considered as acceptable knowledge in social science (Bryman & Bell, 2007).

According to positivism, acceptable knowledge should be through observation and experiment carried out in a value-free approach by a researcher. Thus, the positivist

approach stress on a well-structured methodology that expedites the replication of further knowledge (Sanders et al., 2009; Collis & Hussey, 2009).

Positivism is supported by rigour, objectivity, and precision with the core objective of coming out with a largely accepted knowledge established on observable facts that are independent of the researchers' prior beliefs. Under positivism, theories provide the basis for explanation, permit the anticipation of the problem, predict the occurrence and allow them to be controlled (Collis & Hussey, 2009).

Therefore, positivism cannot be associated with people and the meanings they ascribe to social phenomena, which are dynamic and complex in nature (Kura & Sulaiman, 2012). Hence, there is the need for a different research philosophy for an interpretive understanding that will enable the researcher to appreciate the views of the social actors (Schwandt & Schwandt, 2001).

A paradigm to be a worldview, together with the various philosophical assumptions associated with that point of view." In the same way Creswell and Plano (2007, p21) refer to a paradigm as a worldview. It is "made up of the general theoretical assumptions and laws, and techniques for their application that the members of a particular scientific community. It is a comprehensive belief system, world view, or framework that guides research and practice in a field.

This school of thought about Paradigm is the philosophical orientations that guides the researcher in decision making in the process of social research. Four research philosophies that are used by researchers around the globe. These are the positivist research philosophy (this theory posits that; the social world can be understood in an objective way. In this case, the scientist becomes an objective analyst dissociating himself of personal values and works independently), the interpretivist research

philosophy (actually the opposite of positivists, it theorizes that, the social world can be understood from a subjective perspective).

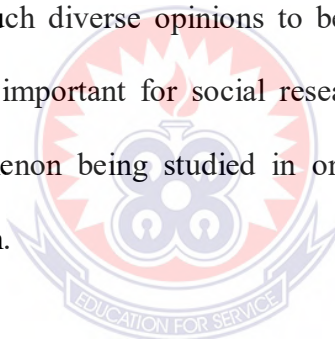
The ways through which people experience the social world is given great attention and the interpretivist plays a role in observing the social world), the pragmatist research philosophy (This theory deals with facts. The research philosophical choices are determined by the research problem. The pragmatist has a freedom to choose the method, design, procedure or technique of the research aim) and the realistic research philosophy (built on the ideologies of positivist and interpretivist research philosophies. Realistic research philosophy is based on assumptions that are necessary for the perception of subjective nature of the human).

The interpretivism research paradigm was adopted for the study. In considering the research objectives and questions, this research does orient itself towards the qualitative approaches. Hence, interpretivism seems as the finest paradigm to employ in this research such as to explore mobile money fraud experience among UEW Students.

Interpretive epistemology was employed as the philosophical base for this research. According to the interpretive epistemological approach, social reality is subjective since it is shaped by the view point of the survey partaker (Collis & Hussey, 2009). The social world of the phenomenon being studied is comprehended from the point of view of the respondents. Hence the social phenomenon is studied from the researcher's observation (Collis & Hussey, 2009). Therefore, mobile money fraud experience among UEW Students was studied from the perspective of the respondents.

The interpretive perspective is more suitable for gathering empirical evidence directly from UEW Students to examine the forms of MoMo fraud strategies experienced, to classify the main perpetrators of the MoMo fraud, and to examine the framework for fraud detection put together by the Telco's and consumers on UEW Campus. The interpretive approach permits the engagement of research subject in its natural environment in order to gain full knowledge of the phenomenon from their perspective.

Ontologically, the subjectivist approach is chosen for this research in order to gain an understanding mobile money fraud experience among UEW Students. Owing to the fact that there are different viewpoints mobile money fraudulent activities, it is imperative to consider such diverse opinions to better understand the phenomenon being studied. It is also important for social researcher to interact with the social world about the phenomenon being studied in order to understand the subjective reality of the phenomenon.



### **3.3 Research Design**

Survey research, cross-sectional studies, and longitudinal design are associated with the positivist approach on the other hand associated with case studies, ethnography, and grounded theory associated with the interpretive approach (Bryman, 2006; Collis & Hussey, 2009). Case study design is used in social sciences to explore a social phenomenon in its natural setting, using different methods to collect empirical evidence and can be a single-case or multiple cases depending on the total number of cases investigated (Yin, 2014; Yin, 2009). Case study design comes a number of advantages with respect to multiple data collection (Yin, 2009). Therefore, the different source of data leads to data triangulation since the researcher relies on multiple sources of data to validate empirical evidence. Case study research

methodology is associated with the interpretive approach (Bryman, 2006). According to Yin (2013), case study design is suitable for both explanatory and exploratory studies due to the need to understand complex social reality in details within a particular context (Yin, 2013). A researcher may decide to study more than one case thereby leading to multiple case studies.

The case study design was used for the research. Case study is one of the methodologies used in the social sciences to explore a social worldview in its natural setting, using different methods to obtain detailed knowledge. Case study is often steered at describing a phenomenon, to explain the processes within and between social institutions and to describe the relationships between variables.

Largely, case study research is directed at gaining a holistic and in-depth comprehension of social and behavioural phenomena, and to observe, interpret and analyse a social phenomenon. Therefore, case study research design was adopted for this research in order to gain an in-depth understanding on the experience of mobile money fraud among UEW Students. The case explored is mobile money fraud.

Yin (2013) case study strategy far surpasses other research designs in terms of providing a researcher the opportunity to use different procedures in the collection of information. Case study design was used to conduct this research because it permitted the use of multiple sources of evidence. Multiple sources of data provides the opportunity for data triangulation. In data triangulation, researchers adopt multiple sources of information, methods, cases and theories to validate evidence.

According to Yin (2009), some of the features of case study design include the following; case study permit an in-depth study of a small number of cases, frequently longitudinally; data are collected and analysed about a large number of features of

each case; cases are enquired in their natural setting making the researcher understand how the case influences and is influenced by its setting.

Case studies usually deal with qualitative research and data but can also be integrated with quantitative data where appropriate. further argues case study design possess the potential to study cases in-depth and to use multiple sources of evidence making it a useful tool for descriptive research studies in which the concentration is on a specific situation or context where generalization is less important.

Case study research design is adopted to conduct this research. A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not evident“ (Yin, 2014, p. 16). Case study method enables a researcher to closely examine the data within a specific context. In most cases, a case study method selects a small geographical area or a very limited number of individuals as the subjects of study.

Case studies, in their true essence, explore and investigate contemporary real-life phenomenon through detailed contextual analysis of a limited number of events or conditions, and their relationships. In other words, a case study is a unique way of observing any natural phenomenon which exists in a set of data. According to Yin (2014, p.10), the case study method is particularly appropriate when the research question starts with: “How?” or “Why questions?”

The merits associated with the use of case study design according to Yin (2009), is it has the ability to accommodate data from different sources, largely from the documentation, archival records, interviews, direct observations, and participant observation. Despite the advantages associated with the use of case study method in conducting research, critics of the case study method believe that the study of a small



number of cases offers no grounds for establishing reliability or generality of findings. Others feel that the intense exposure to the study of the case biases the findings with some dismissing case study research as useful only as an exploratory tool. Nonetheless, the case study method was adopted and used to conduct the research.

### **3.4 Research Approach**

According to Creswell (2013), the quantitative approach, qualitative approach, and mixed methodologies approach are the three basic approaches. In a research project, the distinction between quantitative and qualitative research methodologies can be seen in the collecting and analysis of primarily numerical data (quantitative) and primarily words (qualitative) (Creswell, 2013).

Furthermore, while quantitative methods aid in the testing of theories (Bryman and Bell, 2007; Collis & Hussey, 2009), qualitative methods aid in the development of theories by delving deeper into the complexities of a phenomenon in order to gain interpretative understanding (Collis & Hussey, 2009). The study was conducted using a qualitative technique. In order to address exploratory inquiries, the qualitative technique is preferable (what and how questions).

As an initial venture into the topic area aims to describe what is happening in the field, Creswell (1998) claimed that the qualitative technique is generally more suitable for answering what and how inquiries. As a result, this approach was used to examine the forms of MoMo fraud strategies experienced by customers of MoMo, examine and classify the main perpetrators of the MoMo fraud and examine the framework for fraud detection put together by the Telco's and consumers on UEW Campus. The reason for this is that qualitative research allows social scientists to investigate and

comprehend the meanings that research participants attach to societal and/or human problems (Creswell, 2013).

### **3.5 Sampling techniques adopted for the selection of the units of enquiry**

Non-probability sampling method was adopted for this study. The non-probability sampling method was adopted for this research because the sampling frame of the study was unknown. Hence, the sample size for the study cannot be determined scientifically. Therefore, purposive and convenience sampling techniques under the non-probability sampling were subsequently adopted to select the survey respondents for the study.

Purposive sampling technique was used to select the institutions such as the University of Education Winneba and Mobile Telecommunication Network Ghana (MTN), Winneba Branch. This technique entails the identification and choosing of individuals, groups of individuals or organization that are proficient and well-informed about a phenomenon of interest (Zhi, 2014). The disadvantages associated with purposive sampling technique are that estimates derived may not be a representative of the whole population and statistical analyses are not appropriate.

Convenience sampling technique was used to select UEW students purposely to explore their perspective on mobile money fraud. In all, five students were conveniently sampled and interviewed from the Winneba Campus. Also, the management of Mobile Telecommunication Network Ghana (MTN), Winneba Branch in charge of mobile money services and as well as the mobile money fraud cases were conveniently sampled and interviewed. These categories of associations were chosen for the study based on their availability and willingness to partake in the study. Thus, convenience sampling is a type of non-probability sampling in which members of

target population meet certain practical criteria, such as easy accessibility, geographical proximity, availability at a given time, or the willingness to participate or to be included for the purpose of the study.

### **3.6 Sources and methods of data collection**

The aim of data collection is to gather quality data with valid evidence. This will allow analysis to lead to the formulation of credible answers to the questions posed as well as achieve the objectives of the research. Data was collected from both primary and secondary sources for this research.

#### ***3.6.1 Secondary data sources and their collection***

Secondary information on mobile money fraud were obtained from relevant literature. The secondary information were extracted from published journals and books written on mobile money fraud and security.

#### ***3.6.2 Primary sources of data and their collection***

Primary data collection method included in-depth interviews. An interview is a focused conversation amongst several people on a subject or a structured conversation that usually involves one participant asking questions and the other answering them. They provide a researcher with information regarding to the area of enquiry. A semi-structured interview is a qualitative data collection strategy in which the researcher asks informants a series of predetermined but open-ended questions. The researcher has more control over the topics of the interview than in unstructured interviews.

Semi-structured interviews were used to collected relevant data on the forms of MoMo fraud strategies experienced by customers of MoMo on UEW Campus, the main perpetrators of the MoMo fraud among UEW students, and the framework for fraud detection put together by the Telco's and consumers on UEW Campus.

### **3.7 Data processing and analysis**

The notes made from each in-depth interview were read through a number of times, before they were formally transcribed and same as the notes from the other data collection processes. Detailed notes were made immediately after the discussions in addition to the notes made during each interview process.

*Developing themes:* the text segments in each code many times to extract the striking and significant themes. Themes were developed in line with the findings from existing literature and topics and issues emanating from the empirical data itself by reading through text segments in codes to identify relationships. Key themes such as mobile money fraud strategies, perpetrators of mobile money fraud, and framework for mobile money fraud detection.

The selected initial themes were then read through many times and refined further into a smaller number of themes. These themes were made to be specific enough to relate to the issue or idea or a topic in line with the research questions but also broad enough to cover different explanations related to the issues in the various text segments. A more hierarchical approach to themes development was adopted as the research moved towards the generation of explanations for the presentation of findings in line with the objectives of the study and the research questions.

*Interpretation of findings:* The researcher analysed the developed themes in line with the research questions. A detailed description of each case and themes was first presented in a case-by-case analysis (Collins & Hussey, 2009). This was followed by thematic analysis of the case study to reveal similar and contrasting findings with respect to the experiences of mobile money fraud among UEW Students. This enabled

the researcher to provide a comprehensive picture of how mobile money fraud is rampant among the UEW Students from the Winneba Campus.

### **3.8 Reliability and Validity**

According to Rowley (2002), reliability is the degree to which a test consistently measures what it is supposed to measure. Reliability refers to the extent to which a questionnaire, test, observation or any measurement procedure produces the same results on repeated trials. In short, it is the stability or consistency of scores over time or across ratters.

Reliability ensures that data gathered for research are consistent over time. The reliability measures the degree of consistency with which an instrument measures the attributes it is designed to measure, and the validity also measures the degree to which an instrument measures what it is intended to measure. The researcher will ensure that the physical and psychological environment where the data will be collected is comfortable, by ensuring that the respondents responded at their will and were assured of privacy, confidentiality, and anonymity.

Validity is the process that measures a test that is supposed to be measured. Gay & Mills (2015) stated that validity allows the form of test, the purpose of the test and the population for whom the test it is intended to be measured accurately. According to Rowley (2002), validity is defined as the extent to which the instrument measures what it purports to measure. For example, a test that is used to screen applicants for a job is valid if its scores are directly related to future job performance. With respect to this research, the researcher will ensure reliability by making sure that there is consistency in the data collected from each of the five selected respondents for the study.

### **3.8 Ethical considerations**

Ethical consideration was of importance in this research on the experience of mobile money fraud among UEW Students. Ethical considerations such as confidentiality and informed consent of participants were maintained. It promoted trust, accountability, and mutual respect among the researcher and the respondents. For instance, some respondents did not permit the recording of the interview conducted.

Additionally, trust was maintained during the data collection by recording only the proceedings as agreed by the respondents. Confidentiality was maintained by not disclosing the real identity of the respondent during the reporting of the research findings. The collected data were not falsified and neither was a different picture of the issues being studied painted.



## CHAPTER FOUR

### RESULTS AND DISCUSSION

#### 4.1 Introduction

This chapter present and discussed empirical evidence on the perspective of mobile money fraud victims on the UEW Campus. The analysis is structured into three sections. The first section examined the forms of MoMo fraud strategies experienced by customers of MoMo whereas the second section examined and classify the main perpetrators of the MoMo fraud. The third and final section examined the framework for fraud detection put together by the Telecoms and consumers.

#### 4.2 What are the forms of MoMo fraud strategies experienced by customers of MoMo in Ghana?

##### 4.2.1 Understanding MoMo Fraud

The outcome of the in-depth interviews conducted revealed that all the respondents were knowledgeable about the term mobile money fraud. This is because the term mobile money fraud has become a typical issue in recent times as it has dominated the airwaves and print media (Botsohey et al., 2020). Additionally, the respondents were knowledgeable about the term mobile money fraud because the study purposively sampled victims of MoMo fraud. A respondent stated the following;

*„Mobile money fraud is the act, which involves deceiving or tricking other people to benefit them from their money“.*

Respondent 1, Key Informant Interview, 15-10-2022.

The key informant interview conducted with MTN revealed that mobile money fraud cases are on the ascendancy across Ghana (MTN Ghana, 2022). This phenomenon was attributed to customers of MoMo not taking their security seriously in terms of securing their Identification Number (PIN) (Akomea-Frimpong et al. 2020). The

Management of Mobile Telecommunication Network (MTN) (2022) defined mobile money as the use of tricks to defraud customers of mobile money of their money’.

According to Subex, (2017), mobile money fraud is an intentional act carried out by con artists or thieves to acquire an unfair advantage against mobile money customers, operators, and agents. Scammers are well-trained in their use of the service's stakeholders as leverage. The con artists plot their schemes for a very long time, and they occasionally receive resources and technological support from cartels that make use of systemic flaws to their advantage (Maurer, 2012).

#### ***4.2.3 Frequency of occurrence of MoMo Fraud***

For the past years, mobile money fraud has become a common occurrence among MTN subscribers as well as Vodafone and AirtelTigo users (Owusu-Ansah, 2017). Some MTN agents and staff were themselves, accomplices, to the fraud (Mustapha, 2017). Some of the few fraud cases police successfully solved involved the arrest of telco employees.

According to Owusu-Ansah (2017), telecommunication companies in Ghana have been meticulous in ensuring employees or ex-employees who were caught defrauding or stealing from customers are not associated with them. For instance, some mobile money agents have been punished after being discovered conspiring with mobile money users to defraud mobile money companies (Khan & Bersudskaya, 2016).

The outcome of the participant interview conducted revealed that all the respondents have been conned with their mobile money. On average, the respondents stated that they have been swindled of their mobile money five times in the past three years by fraudsters. The rate at which the respondents were defrauded of their mobile money



in the past years underscores the ascendancy of mobile money fraud across the country.

The situation is worsened by the total amount of money the respondents swindled over the past three years. On average, the respondents were defrauded of a total of GH¢4,000.00. Generally, depending on the transaction, some victims fell prey to fraudsters by using mobile money and lost between GH¢200 and GH¢3,500. The factor accountable for the above phenomenon was the victims (respondents) did not keep their PIN secured, which was used to defraud them. In addition, they were gullible and hence swindled off their money. Finally, the victims of mobile money fraud were not abreast with the operations of mobile money fraudsters thereby falling into their con trap.

The above findings were corroborated by the outcome of the participant interview conducted with the Management of MTN Ghana. According to the Management of MTN Ghana, about 500 mobile money users are successfully defrauded of their mobile money daily on average. Moreover, on average, mobile money fraud victims were defrauded of a whopping sum of GH¢10,000.00 daily; this data is based on the total number of reported mobile money fraud cases that have been reported to the company by customers. The data comprised victims of mobile money fraud on the UEW Campus.

The findings resonate with the findings of the Ghana Chamber of Telecommunications (2018) which established that about 388 mobile money fraud instances were reported in Ghana using mobile money services in 2016, up from 278 in 2015, including MTN Mobile Money, Tigo Cash, Airtel Money, and Vodafone

Cash. In April 2021, the Ghana Chamber of Telecommunications (2021) stated that more than 4,000 cases of mobile money fraud were under investigation.

#### ***4.2.3 Strategies for committing MoMo Fraud***

Following the introduction of mobile money services, scammers have engaged in several fraudulent operations with the primary objective of undermining the value of mobile money services to customers and telecommunication companies. According to Alhassan & Butler (2021), the victims of mobile money claim that scammers call them and claim that they transferred money into their mobile money wallet by mistake and that they need to send it back to them. Later, it is discovered that this is a deliberate, untrue ploy to dupe them (Alhassan & Butler, 2021). The outcome of the key informant interview conducted revealed that mobile money fraud was committed in various forms and including the following.

**Anonymous calls and text messages from scammers:** one of the strategies used to defraud MoMo users was the use of anonymous calls and text messages from scammers. Here, scammers call users of mobile money claiming that they have mistakenly deposited into their account and hence should be resent back to him or them. These messages and phone calls are often detected as false claims after the subscriber has checked the mobile money wallet to check account balance. Interestingly, some of the messages contains discrepancies with respect to the total amount compared to available balance of the MoMo user. Usually, the supposed amount mistakenly deposited by the anonymous caller is more than available balance. Below is a typical example of fraudulent text message to a subscriber.

*„Payment received for GHS1, 500 from Kofi Amoah. Current Balance: GHS200.00.  
Available Balance: GHS200.00“*

Respondent 2, Key Informant Interview, 15-10-2022.

**Scam by false pretense:** Fraudsters call to deceive subscribers that they are to deliver goods from abroad or from a close relative under false pretenses. Some fraudsters call and ask for specified amounts to be deposited into a mobile money account in exchange for goods from relatives or friends from abroad. A respondent stated the following.

*„I received a call from my supposed aunt who was in the USA that she has sent goods to the family so I should pay for the delivery with amount of GHS 2,000. I replied the caller that I do not have any aunt residing in the USA“.*

Respondent 3, Key Informant Interview, 15-10-2022.

**False cash-out SMS:** Fraudsters send false cash-out messages to merchants for authorization of which the physical cash is issued by the merchant to the fraudster without the equivalent e-cash. A respondent stated the following,

*„I was once called by a man who send he has wrongly transferred money into my MoMo account so I should resend it back to you. When I checked my MoMo Wallet, there was no money inside then I realized it was a fraud.“*

Respondent 4, Key Informant Interview, 20-10-2022.

**False Promotion:** Some mobile money subscribers are duped into transferring money to fraudsters after being told to authorize cash out transactions because of winning a mobile money promotion. Fraudulent mobile money subscribers either send fake messages to their agents from their handsets or receive genuine messages generated by computers; they pay the money fraudsters but later discover that they were fake.

According to the assumption of Fraud Pentagon Theory, competence and arrogance are two more components of deception (Oressey, 1953). This is the case in this study since the respondents stated that most of the fraudster demonstrated competence and arrogance in their attempts to scam them of their sums of money from their mobile money wallet. Fraudsters often demonstrated their competence using the above-described strategies for their fraudulent activities.

According to Wolfe & Hermanson (2004), competence/capability refers to a worker's ability to disobey internal controls, devise a covert plan, and manipulate social circumstances for personal gain. Arrogance, on the other hand, is the attitude of superiority stemming from the possession of specific privileges and the conviction that one is exempt from business internal controls or policies. Employees, in particular, are motivated to commit and conceal the fraud by pressure from both financial and non-financial incentives. These include pressure from money, vices, work-related pressure, and additional pressure. Financial considerations result from avarice, the desire to upgrade one's lifestyle, or economic demands brought on by the high standard of living. While non-financial reasons, such as injustice between coworkers, workplace annoyance, and cover-ups for subpar performance, result from demands at work.

This finding is consistent with the finding of Vlček (2011) and Khan & Bersudskaya (2016) categorized mobile money fraud into the following. Fraud is committed by stealing mobile money codes, SIM cards, PINs, and other pertinent information of other subscribers during registration to access their mobile money wallet without their authorization.

Another fraud is system fraud. System fraud occurs because the mobile money system is outdated and unable to keep up with the escalating difficulties posed by mobile money operations. These flaws allow con artists to go around the system and utilize it to defraud others for their money. Fraudulent information technology professionals also deceive others and hide their actions by manipulating information technology systems. Mobile network operator fraud happens when workers of telecommunication companies steal from customers' mobile money wallets, transfer customers' money unauthorized, and collude with other fraudsters to swap SIM cards among others. It usually involves a telco employee manipulating a customer's account without authorization.

False promotion fraud occurs when false prompts are sent under the guise of a telco promotion and the recipient is asked to input their identification number (PIN) as a verification measure to claim their prize. The fraudster gains access to the recipient's mobile money account with the PIN that is inputted. In addition, fraud messages are sent that indicate a deposit into a customer's account. The fraudster then calls the customer to tell them the deposit was a mistake and to send that amount back. Finally, another type of fraud is fortuitous fraud, where fraudsters pose as delivery companies and call customers under the pretext of delivering goods to them from relatives abroad.

#### **4.3 Who are the main perpetrators of the MoMo fraud in Ghana?**

According to Merritt (2011), following the launch of the mobile money services by the various telecommunication companies in Ghana, scammers have engaged in several fraudulent operations with the primary objective of undermining the value of the mobile money service to the public as well as the telecoms.

The outcome of the participant interview conducted revealed that mobile money fraud has been perpetuated in diverse forms such as mobile money network systems fraudster, false promotion fraudster, reversal of erroneous transactions fraudsters, fortuitous scammers, and mobile money agents' fraudsters. Each of these MoMo fraud perpetrators are discussed below.

***Mobile money network systems fraudster:*** the employees of the telecommunication companies such as Vodafone, AirtelTigo, and Mobile Telecommunication Company (MTN) commit this type of fraud. This type of fraud is often perpetuated in the form of mobile money employees as in the case of MTN stealing from customers' mobile money wallets, transferring customers' money from their mobile money wallets without authorization as well as colluding with other fraudsters to change the SIM cards of customers without their knowledge. Generally, this kind of fraud is comprised of an employee of a telecommunication company manipulating customers' accounts without their knowledge.

The reason accountable for this kind of fraud is that even though complicated algorithms have been developed to assist telecommunications operators to safeguard the account of customers, some of the systems are outdated and unable to keep up with the escalating difficulties posed by mobile money operations. Consequently, scammers are to manipulate the system and utilize it to defraud customers of their mobile money. This finding is consistent with the findings of Mustapha (2017) who established that for the past years, employees of telecommunication companies have been involved in mobile money fraud. Consequently, about 3000 employees of MTN suspected to be engaged in mobile money fraud have been sanctioned.

***False promotion fraudster:*** this is the most common type of mobile money fraud that is on the ascendancy currently particularly, with MTN mobile money users. This kind of fraud is committed in the form of false prize promotions being sent to customers of mobile money. The recipient of the false promotion is requested to input their identification number as a verification code to claim their supposed won prize. The fraudster who sent the message ended up gaining access to the recipient's mobile money account including the PIN and transferring money into their wallet without their knowledge. The Pentagon Theory of Fraud postulated that companies with poor internal control systems, poor managerial oversight, lax sanctions, and ambiguous procedures are typically where opportunities arise (Crowe, 2011). This finding resonates with the finding of Frickenstein (2019) who established that fraud by false promotion has been used to defraud thousands of mobile money users of their money particularly, MTN mobile money users.

***Reversal of erroneous transactions fraudster:*** the outcome of the participant interview conducted revealed that the reversal of erroneous transactions is a common fraud scheme that has been devised by mobile money fraudsters in Ghana. Scammers send fake short message services to mobile money users indicating that an amount of money has been mistakenly deposited into their mobile money accounts perpetuate this fraud scheme. The fraudster then calls the customer to tell them that the deposit was a mistake and to send that amount back. According to the Management of MTN Ghana (2022), the users of mobile money daily receive more than 500 reversals of erroneous transaction messages. However, more than 45% of the users of mobile money fall prey to these erroneous messages. Consequently, more than 100 mobile money users are scammed of their money daily.

**Fortuitous scammer:** this is the type of fraud that involves fraudsters posing as delivery companies and calling customers to inform them that there are delivering goods sent to them by their relatives abroad. Customers are subsequently instructed to deposit an amount of money into a particular mobile money account for the supposed goods to be delivered. The outcome of the key informant interview further revealed that this kind of fraud is not directed at only customers of mobile money. However, more than 60% of mobile money users have been swindled using this ploy. This finding resonates with the finding of Ifeanyi-Ajufo (2022) who established that fortuitous scam is accountable for more than 30% of mobile money fraud cases in Ghana.

**Mobile money agent fraudster:** To steal money from accounts and utilize it for their gain, some mobile money agents generate numerous fake accounts and passwords to swindle users of mobile money. Additionally, mobile money operators' staff members have been charged with assisting mobile money agents in stealing money from mobile money subscribers. Common agent frauds include float loss in the agent's account due to illegal use, compromised PINs, and con games where fraudsters pretend to be MNO employees to get access to the agent's float account. Additionally, there are fraudulent withdrawal reversals or phony monetary deposits into customers of mobile money with the intent of defrauding them.

According to Pentagon Theory of Fraud, opportunity is a factor that give people the chance to conduct fraud due to their lax controls. Lack of controls, inability to assess performance quality, failure to punish fraudsters, lack of information access, ignorance, indifference, inability, and absence of an audit trail are the six main



reasons that create opportunity. There are opportunities because the offenders think their behavior will not be noticed (Aprilia, 2017).

This finding resonates with the finding of the study conducted by Helix Institute (2015) which established that, in Ghana in 2014, 1,000 mobile money agents were punished after being discovered conspiring with mobile money users to scam the mobile money companies (Helix Institute, 2015).

#### **4.4 What are the framework for fraud detection put together by the Telco's and consumers?**

According to Helix Institute (2015), to curb the menace of mobile money fraud among others, telecommunication companies rendering mobile money services must invest massively in cybersecurity towards safeguarding the accounts of their customers. To control the menace of mobile money fraud, both telecommunication companies and consumers of mobile money services across Ghana have put in place some frameworks or mechanisms to ensure individualistic digital security efforts and individualistic digital security efforts to safeguard the mobile money accounts of customers. These mechanisms have been discussed below.

##### ***4.4.1 Telecommunication framework for detecting MoMo Fraud***

**Display of national identifies cards for the transaction:** following the disturbing cases of mobile money fraud, one of the key measures that have been implemented to control it is the display of national identity cards such as voter identity cards, Ghana Card, and passports before transacting business at any mobile money agents. For instance, the Mobile Telecommunication Network made it mandatory for customers to display a national ID before transacting with any of its agents or merchants. Similarly, the remaining telecommunications such as Vodafone and AirtelTigo

followed suit. This policy or directive was implemented in the year 2021 purposely to help to curb mobile money fraud. According to the Management of MTN, the implementation of the policy helped controlled the fraud committed by agents or employees of the telecommunication companies. For instance, the respondent stated the following;

*„When it was made compulsory for customers to display their ID card at the point of transactions, it reduced the unauthorized withdrawal of money from the wallet of customers without their consent“.*

Key informant interview (Manager of Mobile Money Service), 20/10/2022.

**Digital identification systems:** another mechanism that was introduced is the digital identification systems by the Government of Ghana. This measure required the re-registration of all SIM Cards by mobile phone users. Before this re-registration exercise, which is still ongoing, the National Communications Authority introduced the Ghana Card. The Ghana Card starting from 1<sup>st</sup> July 2022 was recognized as the only ID document required for all financial transactions as authorized by the Bank of Ghana. To strengthen the digital identification of mobile money accounts, the government also required all telecommunication companies to use the Ghana Card for the SIM re-registration exercise.

Consequently, telecommunication companies have also directed their employees and mobile money agents to require proof of identity before conducting transactions with valid forms of identity cards such as driver's license, voter ID, passport, driver's license, Social Security and National Insurance Trust ID, National Health Insurance Card or the Ghana Card. According to Karombo (2022), the implementation of the

digital identification systems policy by the Government of Ghana will help reduce mobile money fraud by 80% if all SIM card reregistration is completed.

**Firewall to protect mobile money accounts:** another mechanism that is used to curb mobile money fraud is a complicated firewall to protect mobile money accounts, especially the password of customers. A firewall is a network security device that monitors and filters incoming and outgoing network traffic following the security policies that have been previously established by an organization. A firewall, at its most basic, is the barrier that exists between a private internal network and the public Internet. The main purpose of a firewall is to allow non-threatening traffic in while keeping dangerous traffic out.

A firewall is an essential component of any security architecture because it removes the guesswork from host-level protections and transfers them to your network security device. Firewalls, particularly Next Generation Firewalls, are focused on blocking malware and application-layer attacks. When combined with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can detect and respond to outside attacks across the entire network quickly and seamlessly. They can set policies to better defend your network and perform quick assessments to detect and shut down invasive or suspicious activity, such as malware.

These Next Generation Firewalls, when combined with an integrated intrusion prevention system (IPS), can detect and combat attacks across the entire network in real-time. Firewalls can act on previously defined policies to better protect your network and can perform quick assessments to detect invasive or suspicious activity, such as malware, and shut it down.

When you use a firewall as part of your security infrastructure, you configure your network with specific policies that allow or block incoming and outgoing traffic. Firewalls are network security systems that guard against unauthorized network access. In general, a software unit filters incoming and outgoing traffic within a private network based on a set of rules to detect and prevent cyber-attacks. A respondent stated the following;

*"The firewall used to protect the accounts of mobile money is complicated. It is not easy to hack. We are not the mobile money department that monitors transactions, both in-flow and out-flow*

*of cash but cannot see the password of customers. It is a difficult system to hack".*

Key informant interview (Manager of Mobile Money Service), 20/10/2022.

**Effective information technology architecture:** According to the findings of the key informant interview, the Bank of Ghana has assigned its Payment Systems Department (PSD) to handle all issues about mobile money supervision. The Payment Systems Department is equipped with tools to function, but it was discovered that these tools are insufficient to assist the department in conducting extensive oversight of the mobile money service. Partner banks have divided their treasury divisions into sub-departments to manage the mobile money operators' funds.

Mobile money operators have departments that handle the transfer and distribution of electronic money to mobile money subscribers. This department works to ensure that mobile money operators' accounts are reconciled daily with the operators' branches and partner banks. This department also monitors bill payments, money transfers, account deposits, and savings from mobile money operators and agents.

This department ensures that mobile money operators follow the Bank of Ghana's rules and regulations for managing funds on mobile money services. They follow the rules, and employees who refuse to follow these directives are punished. Routine testing of the IT systems' functionality has become a top priority for all operators. Some operators have invested in sophisticated software to improve the service they provide to subscribers. MTN Ghana, for example, has announced the return of the "Allow Cash-Out" feature on its mobile money platform to improve customer security for withdrawal transactions.

**Sanctioning of mobile money fraudsters:** moreover, the key informant interview conducted revealed that stiffer punishment needs to be meted out to mobile money fraudsters. This punitive punishment can be in the form of long prison sentences with hard labor. In addition, mobile money agents who are caught engaging in mobile money fraud need to be sanctioned in the form of losing their license in addition to fines and penalties.

**Transaction limits:** furthermore, transaction limits are used by telcos to detect and or prevent mobile money fraud. Here, the amount that agents can receive or withdraw from a bank on a daily, weekly, and monthly basis is subject to transaction limits. To limit the amount of money subscribers and agents can access, telecommunication companies implemented these limits with assistance from partner banks and the Bank of Ghana. The limits are used for control and to monitor the activities of fraudsters. The amount that agents can issue to subscribers is governed by these limits. According to a respondent,

*„The daily limit for my MoMo transaction is GHS2, 000.00. However, the monthly limit is GHS20, 000.00. My MoMo transactions beyond the set limit are not permitted.*

*This has enabled me to keep track of my MoMo transaction to detect fraudulent activities by scammers”:*

Respondent 5, Key Informant Interview, 20-10-2022.

**Blocking the SIM card fraudsters:** finally, blocking the SIM cards of fraudster is another approach used to detect and prevent mobile money fraud. The Ghana Chamber of Telecommunications in the year 2020 stated that telecommunication companies in Ghana collectively blacklisted 28,000 SIMs and 17,000 identities as part of their joint program to reduce mobile money fraud. The blacklisted fraudsters were detected through their activities such as the sending of false SMS among other fraudulent activities. According to Akomea-Frimpong (2017), blacklisting the SIM cards of fraudsters is a welcome to preventing or reducing the menace of mobile money fraud across Ghana.

#### ***4.4.2 MoMo consumer tactics for fraud detection or prevention***

**Reporting of mobile money fraud to telecoms:** moreover, the reporting of mobile money fraud to telecommunication companies. Consequently, mobile money operators and their agents use three methods to report their activities and transactions to the Bank of Ghana and the partner banks via the Reporting Portal provided by the Bank of Ghana. Payment Systems Data Submission Module is a pre-determined format for data submission authorized by the Bank of Ghana to aid in timely reporting to the bank and various security agencies in Ghana. These reporting systems aid the state security apparatus and the Central Bank in detecting and punishing fraudsters per Ghanaian laws.

**Protecting Personal Identification Number (PIN):** According to the key informant interview, another way MoMo users can prevent mobile money fraud is to protect

their PIN at all costs. This is due to the fact that mobile money fraudsters have recently developed a new scamming scheme known as "Cash Out" fraud, in which subscribers to the Mobile Money service are pushed payment approval prompts and enticed to enter their PIN Code in order to receive a prize or for a specific service, such as phone book backup or job alerts, to be enabled on their phone. This action authorizes the transfer of funds from the consumers' wallet to the wallet of the fraudster. As a result, mobile money subscribers are expected to protect their personal information from unknown sources. As a result, whenever a person's personal identification number is in the wrong hands, it needs to be changed quickly. According to Laryea (2016), mobile money users' ability to secure their PIN will reduce the occurrence of MoMo fraud in Ghana.

Being aware of unsolicited messages: Furthermore, as revealed by the key informant interview, subscribers of mobile money fraud should be aware of fraudulent messages intended to defraud MoMo users. This is due to the fact that fraudsters create convincing messages in order to capture the attention of MoMo users. Most of these messages promise unexpected money that one has won or is likely to win, or imported goods sent by a relative that the person must pay to redeem. MoMo users are expected to think twice before providing personal information in response to these messages. Thus, MoMo users should be aware that they will not receive any unexpected funds and are unlikely to win any lottery by giving out their PIN. According to Provencal (2017), about 90% of mobile money fraud is committed through unsolicited messages.

**Checking the authenticity of payment application before using them:**

Cybercriminals create mobile applications that look exactly like the ones developed by banks and other financial institutions in order to steal your personal information

and money. Other payment service providers have apps that allow transactions from banks to mobile wallets and vice versa. To avoid becoming a victim, MoMo users should always check the authenticity or originality of these apps before downloading and installing them. When in doubt, they should check with the service provider for specific security features and links to the original apps. In the view of Mudiri (2013), fraudsters commit fraud using clone applications of financial services organization.

**Being aware of anonymous calls from fraudsters:** One of the many tricks that these crooks employ is calling unsuspecting mobile money subscribers and asking them to revert money sent to them by mistake. Scammers perpetuate this fraud scheme by sending fake short message services to mobile money users, indicating that money has been mistakenly deposited into their mobile money accounts. The fraudster then calls the customer to inform them that the deposit was a mistake and that they should return the money. Subscribers to mobile money should always check their balance to see if it matches the amount they want you to resend. This finding is consistent with the finding of Akomea-Frimpong et al. (2022) who established that the use of anonymous call is the current innovative way of defrauding mobile money users across Ghana.



## CHAPTER FIVE

### SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

#### 5.1 Introduction

This chapter presented and discussed empirical evidence from the perspective of mobile money fraud victims on the UEW Campus. The analysis was structured into three sections. The first section examined the forms of MoMo fraud strategies experienced by customers of MoMo on the UEW Campus whereas the second section examined and classify the main perpetrators of the MoMo fraud among UEW students. The third and final section examined the framework for fraud detection put together by the Telecoms and consumers on UEW Campus.

This chapter summarized and presented the key findings of the study. Following that, the study was concluded with workable recommendation (s) suggested based on the outcome of the study. This chapter is structured into three sections. The first covered the summary of findings whereas the second section covered the conclusion. Finally, the third and final section covered the recommendation (s) of the study.

#### 5.2 Summary of Findings

##### *5.2.1 Forms of MoMo fraud strategies experienced by customers of MoMo*

**Understanding Mobile Money Fraud:** The outcome of the in-depth interviews conducted revealed that all the respondents were knowledgeable about the term mobile money fraud. This is because the term mobile money fraud has become a topical issue in recent times as it has dominated airwaves and print media.

**Frequency of occurrence of Mobile Money Fraud:** The outcome of the participant interview conducted revealed that all the respondents have been conned with their mobile money. On average, the respondents stated that they have been swindled of

their mobile money five times in the past three years by fraudsters. The respondents were defrauded of a total of GH¢4,000.00 averagely. Generally, depending on the transaction, some victims fell prey to fraudsters by using mobile money and lost between GH¢200 and GH¢3,500.

**Strategies for committing MoMo Fraud:** The outcome of the participant interview conducted revealed that mobile money fraud was committed in various forms such as anonymous calls and text messages from scammers, fraudsters calling to deceive subscribers that they are to deliver goods from abroad or from a close relative under false pretexts as well as fraudsters send false cash-out messages to merchants for authorization of which the physical cash is issued by the merchant to the fraudster without the equivalent e-cash.

### *5.2.2 Examining the main perpetrators of the MoMo fraud among UEW Students*

**Main perpetrators of the MoMo fraud among UEW Students:** The outcome of the participant interview conducted revealed that the perpetrators of mobile money fraud included mobile money systems fraudster, false promotion fraudster, reversal of erroneous transactions fraudster, fortuitous scammer, and mobile money agents' fraudster.

### **5.2.3 Framework for fraud detection put together by the Telco's and MoMo consumers**

The measures or frameworks used to detect mobile money fraud include the display of national identity cards for the transaction, digital identification systems, and the use of firewall to protect mobile money accounts. Other measures included information technology architecture for mobile money services, reporting of mobile money fraud to telecoms, sanctioning of mobile money fraudsters and transaction limit for MoMo users. Finally, other measures included blocking the sim card fraudsters, protecting

personal identification number, being aware of unsolicited messages, checking the authenticity of payment application before using them and Being aware of anonymous calls from fraudsters.

### **5.3 Conclusion**

The study examined mobile money service fraud experiences and perspectives on control practices at University of Education, Winneba. The objectives of the study included to examine the forms of MoMo fraud strategies experienced by customers of MoMo on UEW Campus, to examine and classify the main perpetrators of the MoMo fraud among UEW students as well as the framework for fraud detection put together by the Telco's and consumers on UEW Campus.

The outcome of the in-depth interviews conducted revealed that all the respondents were knowledgeable about the term mobile money fraud. In addition, all the respondents stated that have been conned with their mobile money. The respondents stated that they have been swindled of their mobile money five times in the past three years by fraudsters. The respondents were defrauded of a total of GH¢4,000.00. Mobile money fraud was committed in various forms such as anonymous calls and text messages from scammers, fraudsters calling to deceive subscribers that they are to deliver goods from abroad or from a close relative under false pretexts. Finally, fraudsters sending false cash-out messages to merchants for authorization of which the physical cash is issued by the merchant to the fraudster without the equivalent e-cash.

The outcome of the participant interview conducted revealed that mobile money fraud perpetrators include mobile money systems fraudster, false promotion fraudster,

reversal of erroneous transactions fraudster, fortuitous scammer, and mobile money agents' fraudster.

Finally, the frameworks that have been used to detect mobile money fraud include the display of national identifies cards for the transaction, digital identification systems, the use of firewall to protect mobile money accounts. Other measures include effective information technology architecture for mobile money services, reporting of mobile money fraud to telecoms, sanctioning of mobile money fraudsters and setting transaction limits for MoMo users. Finally, other measures included blocking the sim card fraudsters, protecting personal identification number, being aware of unsolicited messages, checking the authenticity of payment application before using them and Being aware of anonymous calls from fraudsters.

#### **5.4 Recommendations**

Based on the outcome of the study, the following are suggested.

**Public education and awareness creation:** there should be public education and awareness creation on the activities of mobile money fraudsters in Ghana by telecommunication companies in conjunction with the National Communications Authority and the Bank of Ghana. Subscribers should be educated on the importance of verifying any banking app they use. They should be assisted in setting up a strong password and a SIM card PIN that cannot be used in another device to protect their phones or tablets. The public should be cautious when returning a call from an unknown number.

**Robust identification systems before transaction:** Prior to transactions, strict rules for merchant identification should be in place to ensure that obstinate merchants can be easily tracked down and arrested when they commit fraud. Furthermore,

subscribers must provide a valid form of identification before they can deposit or withdraw funds from their mobile money wallet. This will help to reduce the threat of mobile money fraud.

**Strict enforcement of legislation on fraud:** A legislative instrument or an Act of Parliament should be enacted specifically to guide the mobile money service, distinguishing it from laws that govern other cashless electronic financial services. This should be accomplished by soliciting input from all stakeholders in the mobile money industry. To assist telecommunication companies, information and knowledge sharing among cross-functional departments at the Bank of Ghana should be encouraged.



## REFERENCES

- Abdinoor, A., & Mbamba, U.O.L. (2017). Factors influencing consumers' adoption of mobile financial services in Tanzania. *Cogent Business and Management*, 4(1), 1-19.
- AbuShanab, E., & Pearson, J.M. (2007). Internet banking in Jordan: The unified theory of acceptance and use of technology (STAUT) perspective. *Journal of Systems and Information Technology*, 9(1), 71–97.
- ACP Observatory on Migration (2014). *Mobile money services: "A bank in your pocket": An overview of trends and opportunities*. International Organization for Migration.
- Adedoyin, A., Kapetanakis, S., Samakovitis, G. & Petridis, M. (2017), –Predicting fraud in mobile money transfer using case-based reasoning. *International Conference on Innovative Techniques and Applications of Artificial Intelligence*, Springer, Cham, pp. 325-337.
- Akomea-Frimpong, I. (2017). *How mobile money operators can minimize fraud*. Assembly Press.
- Alanezi, F. & Brooks, L. (2014), –*Combating online fraud in Saudi Arabia using general deterrence theory (GDT)*". Willey and Sons.
- Alkhalidi, A.N., & Kharma, Q.M. (2018). Customer's Intention to Adopt Mobile Banking Services: The Moderating Influence of Demographic Factors. *International Journal of Innovation and Technology Management*.
- Archie, H., Akpaka, B., & Williams, K (2021). *A History of Mobile Money in Ghana*. Decode Fintech, podcast, MP3 audio, 33:20.
- Asongu, S. and Asongu, N. (2018), –The comparative exploration of mobile money services in inclusive development. *International Journal of Social Economics*, Vol. 45 No. 1, pp. 124-139.
- Balan, R. K., Ramasubbu, N., Prakobphol, K., Christin, N., & Hong, J. (2009). mFerio: the design and evaluation of a peer-to-peer mobile payment system. *MobiSys '09 Proceedings of the 7<sup>th</sup> International Conference on Mobile Systems, Applications and Services*.
- Bampoe, H.S. (2015). *Mobile Money Adoption in Emerging Markets: a case of Ghana (MPhil Thesis)*. Accra, Ghana: University of Ghana, Legon.
- Bank of Ghana (2016). *Payment Systems Oversight Annual Report, 2016*. Ghana: IDPS Department, Bank of Ghana.
- Bank of Ghana (2017). *Payment Systems Oversight Annual Report, 2017*. Ghana: IDPS Department, Bank of Ghana.

- Bara, A. (2013), –Mobile money for financial inclusion: policy and regulatory perspective in Zimbabwe. *African Journal of Science, Technology, Innovation and Development*, Vol. 5 No. 5, pp. 345-354.
- Bell, E., & Bryman, A. (2007). The ethics of management research: an exploratory content analysis. *British Journal of Management*, 18(1), 63-77.
- Bersudskaya, V., & Kuijpers, D. (2016). *Agent network accelerator survey: Uganda Country Report 2015*. Helix, Kampala Uganda.
- Botchey, F.E., Qin,Z., & Hughes-Lartey, K (2020). Mobile Money fraud prediction-a cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and naïve bayes algorithms. *Information* 2020, 11, 383.
- Braun, V., Clarke, V. & Weate, P. (2016), –Using thematic analysis in sport and exercise research”, in *Routledge Handbook of Qualitative Research in Sport and Exercise*. Routledge, pp. 213-227.
- Braun, V., Clarke, V., Hayfield, N. & Terry, G. (2019), “Thematic analysis. Handbook of Research Methods in Health Social Sciences, pp. 843-860.
- Bryman, A. (2006) \_integrating quantitative and qualitative research: how it is done? *Qualitative Research*, Vol. 6, No. 1, pp. 97-113.
- Burhouse, S., & Osaki, Y. (2012). 2011 FDIC National Survey of Unbanked and Underbanked Households: Executive Summary.
- Busuulwa, B. (2016), –Mobile money fraud, crime rate increase in Uganda”, available at: [www. theeastafrican.co.ke/business/Mobile-money-fraud-and-crime-rate-increase-in-Uganda-/2560-3415786-quaydf/index.html/](http://www.theeastafrican.co.ke/business/Mobile-money-fraud-and-crime-rate-increase-in-Uganda-/2560-3415786-quaydf/index.html/) (accessed 12 June 2017).
- Camara, N., & Tuesta, D. (2015). Factors that Matter for Financial Inclusion: Evidence from Peru. *The IEB International Journal of Finance*, 10, 8-29.
- Carroll, J., Howard, S., Peck, J., & Murphy, J. (2003). From adoption to use: The process of appropriating a mobile phone. *Aust. J. Inform. Syst.*, 10(2), 38-48.
- Castri, S. D (2013). Mobile Money: Enabling regulatory solution.
- Chatain, P.L., Zerzan, A., Noor, W., Dannaoui, N. & De Koker, L. (2011), –Protecting Mobile Money against Financial Crimes: Global Policy Challenges and Solutions. World Bank Publications, New York, NY.
- Chauhan, S. (2015), –Acceptance of mobile money by poor citizens of India: integrating trust into the technology acceptance model. *Information*, Vol. 17 No. 3, pp. 58-68.

- Chawla, D., & Joshi, H. (2018). The Moderating Effect of Demographic Variables on Mobile Banking Adoption: An Empirical Investigation. *Global Business Review*, 19, S90-S113.
- Checkpoint (2005). Taxis hailed as black hole for lost cell phones and PDAs, as confidential data is taken for a ride. Accessed from <http://www.checkpoint.com/press/pointsec/2005/01-24a.html>.
- Chithra, N., & Selvam, M. (2013). *Determinants of financial inclusion: An empirical study on the inter-state variations in India*. SAGE Publication.
- Collis, J., & Hussey, R. (2009). *Business Research*: Palgrave Macmillan.
- Cressey, D.R. (1986), –Why managers commit fraud. *Australian and New Zealand Journal of Criminology*, Vol. 19 No. 4, pp. 195-209.
- Creswell, J. W. (1998). *A concise introduction to mixed methods research*. Sage Publications.
- Creswell, J.W., & Clark, P (2011). *Designing and Conducting Mixed Methods Research, 2<sup>nd</sup> edition*. Thousand Oaks: Sage.
- Creswell, John W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches. Third edition*. Washington DC: Sage.
- Creswell. J. W. (2009). *Research Design: Qualitative, Quantitative and Mixed Approaches (3rd Ed.)*. Thousand Oaks, CA: Sage
- D'Arcy, J., Hovav, A. & Galletta, D. (2009), –User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.
- Darrat, A. (1999). Are Financial Deepening And Economic Growth Causally Related? Another Look at the Evidence. *International Economic Journal*, 13(3).
- Demirci, A.E., & Ersoy, N.F. (2008). Technology Readiness for Innovative High-Tech Products: How Consumers Perceive and Adopt New Technologies. *Business Review*, 10(2), ss. 302-308.
- Demirguc-Kunt, A., Klapper, L., Singer, D., & Van Oudheusden, P. (2015). The Global Findex Database 2014: Measuring Financial Inclusion around the World. *World Bank Policy Research Working Paper 7255*. Washington, DC: World Bank.
- Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*. Washington, DC: World Bank.
- Demombynes, G. & Thegeya, A. (2012). Kenya's Mobile Revolution and the Promise of Mobile Savings. *World Bank Policy Research Working Paper*, No. 5988.



- Domeher, D., Frimpong, J.M., & Appiah, T. (2014). Adoption of financial innovation in the Ghanaian banking industry. *African Review of Economics and Finance*, 6(2), 88-114.
- Donner, J. (2005). The social and economic implications of mobile telephony in Rwanda: An ownership/access topology. In: P. Glotz, S. Bertschi, and C. Locke (Eds.), *Thumb culture: The meaning of mobile phones for society* (pp. 37-51). New Brunswick, NJ: Transactions.
- Etim, A.S. (2014), "Mobile banking and mobile money adoption for financial inclusion", *Research in Business and Economics Journal*, Vol. 9, p. 1.
- Fanta, A., & Mutsonziw, K. (2016). Gender and Financial Inclusion: Analysis of financial inclusion of women in the SADC region. *FinMark Trust Policy Research Paper No. 01/2016*.
- Fogie, S (2006). Air scanner vulnerability summary: Windows mobile security software fails the test, informIT.
- Fungáčová, Z. & Weill, L. (2015). Understanding financial inclusion in China. *China Econ. Rev.* 34, 196–206.
- Gan, C., Clemens, M., Limsombunchai, V., & Weng, A. (2006). A logit analysis of electronic banking in New Zealand. *International Journal of Bank Marketing*, 24 (6), 360-383.
- Gay, S & Mills, K (2015). The collagens: An overview and update. *Methods in Enzymology*, 144, 3-41.
- Gilman, L. & Joyce, M. (2012), "Managing the risk of fraud in mobile money", *GSMA: Mobile Money for Unbanked (MMU)*. Available at: [www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012\\_MMU\\_Managing-the-risk-of-fraud-in-mobile-money.pdf](http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf)
- Githui, D.M (2011). Mobile money transfer in Kenya: an ethical perspective, *Research Journal of Finance and Accounting*; Vol 2, No 2.
- Gosavi, A. (2017), "Can mobile money help firms mitigate the problem of access to finance in Eastern sub-Saharan Africa? *Journal of African Business*, Vol. 19, pp. 1-18.
- Government of Kenya (2003). *Economic Survey 2003*. Nairobi: Central Bureau of Statistics Government Printers.
- GSMA (2022). MTN MoMo Pay Merchant Payments: Expanding Women's Mobile Money Use in Ghana. Accessed from <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/MTN-MoMo-Pay-Merchant-Payments-Expanding-Female-Mobile-Money-Usage-in-Ghana.pdf>.

- GSMA Mobile Money Tracker (2012). Global Mobile Money Deployment Tracker. Retrieved from <http://www.wirelessintelligence.com/mobile-money>.
- Hahn, H.P., & Kibora, L. (2008). The domestication of the mobile phone: oral society and new ICT in Burkina Faso. *J. Mod. Afr. Stud.*, 46(01), 87-109.
- Harris, A, Goodman, S, & Traynor, P (2013). Privacy and security concerns associated with mobile money applications in Africa. *Journal of Law, & Arts* 245.
- Henderson, L., Herring, C., Horton, H. D., & Thomas, M. (2015). Credit Where Credit is Due? Race, Gender, and Discrimination in the Credit Scores of Business Startups. *The Review of Black Political Economy*, 42(4).
- Henry, L (2022). Ghana Telecoms Market Report: Telcoms, Mobile and Broadband – Statistics and Analyses. Accessed from <https://www.budde.com.au/Research/Ghana-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses>
- Herzberg, A (2003). Payments and banking with mobile personal devices. *Communications of the ACM* 46 (5), 53-58.
- Hoseph, L. & Anpalagan, A (2007). Trends and challenges in handheld wireless application development. *IEEE Canadian Review*, No. 55.
- InterMedia (2012). Tanzania mobile money tracker study. From <http://www.audiencescapes.org/sites/default/files/Tanzania%20Mobile%20MoneyQ3.pdf>
- InterMedia (2013). Mobile money in Tanzania use, barriers and opportunities, The Financial Inclusion Tracker Surveys Project. From [http://www.intermedia.org/wp-content/uploads/FITS\\_Tanzania\\_FullReport\\_final.pdf](http://www.intermedia.org/wp-content/uploads/FITS_Tanzania_FullReport_final.pdf)
- International Finance Corporation (2011). *Mobile Money Study 2011*. Washington, DC.
- Jack, W., & Suri, T. (2014). Risk Sharing and Transactions Costs: Evidence from Kenya's Mobile Money Revolution. *American Economic Review*, 104(1), 183-223.
- Jack, W., Suri, T., & Townsend, R. (2010). Monetary Theory and Electronic Money: Reflections on the Kenyan Experience. *Federal Reserve Bank of Richmond Economic Quarterly*, 96, 83-122.
- Jambulingam, M. (2013). Behavioural Intention to Adopt Mobile Technology among Tertiary Students. *World Applied Sciences Journal*, 22(9), 1262-1271.
- Jansen, W & Ayers, R (2007). Guidelines on cell phone forensics. *NIST Special Publication*.

- Jenkins, B. (2008), *Developing Mobile Money Ecosystems*. Harvard Kennedy School, Washington, DC.
- Jenkins, B. (2008). *Developing mobile money ecosystems*. Washington, DC: International Finance Corporation and Harvard Kennedy School.
- Kanobe, F., Alexander, P.M. & 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.
- Karnouskos, S (2004). Mobile payment: a journey through existing procedures and standardization initiatives. *IEEE Communications Surveys and Tutorials*, pp. 44-66.
- Karombo, T (2022). Ghana’s process for adding banking to its biometric card is a flawed one. Retrieved from <https://qz.com/africa/2117872/ghana-card-being-linked-to-banking-is-frustrating-ghanaians>.
- Kassem, R. & Higson, A. (2012), –The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, Vol. 3 No. 3, pp. 191-195.
- Kendall, J., Maurer, B., Machoka, P., & Veniard, C. (2011). An Emerging Platform: From Money Transfer System to Mobile Money Ecosystem. *Innovations: Technology, Governance, Globalization*, 6(4), 49-64.
- Khan, M., & Vera, B (2016). Working Together to Fight DFS Fraud. <http://www.helixinstitute.com/blog/working-together-fight-dfs-fraud>
- Kithaka, E. (2014). The Effect of Mobile Banking on Financial Performance of Commercial Banks in Kenya. *International Journal of Business and Social Research*, 2(1), 36-40.
- Klein, M. & Mayer, C. (2011), –*Mobile banking and financial inclusion: the regulatory lessons*. The World Bank.
- Knijff van der, R (2002). Embedded systems analysis, handbook of computer crime investigation, Edited by Eoghan Casey, Academic Press, 2002
- Krugel, G. T. (2007). *Mobile banking technology options: an overview of the different mobile banking technology options, and their impact on the mobile banking market*. FinMark Trust.
- Kura, B., & Sulaiman, Y. (2012). Qualitative and quantitative approaches to the study of poverty: Taming the tensions and appreciating the complementarities. *The Qualitative Report*, 17(20), 1-19.

- Laryea, D. (2016). *Mobile money fraudsters" very cunning-Telcos Chamber warns*. available at: <http://ghananewsonline.com.gh/mobile-money-fraudsters-very-cunning-telcos-chamber-warns/>
- Lee, k. S., Lee, H. S., & Kim, S. Y. (2007). Factors influencing the adoption behaviour of mobile banking: A South Korean perspective. *Journal of Internet Banking and Commerce*, 12(2).
- Lesitaokana, W. (2016). Influencing factors to mobile phone adoption among urban youth in Botswana. *Journal of Media and Communication Studies*, 8(1), 8-14.
- Li, Y. (2012). Perceived Risks as Barriers to Internet and Ecommerce usage. *Qualitative Market Research*, 5(4), 291-300.
- Lotto, J. (2018). Examination of the Status of Financial Inclusion and its Determinants in Tanzania. *Sustainability*, 10(2873), 1-15.
- Lyons, P. (2010). A Financial Analysis of Mobile Money Services. *Communications and Strategies*, 79(3), 29-40.
- Maduku, D.K. (2013). Predicting retail-banking customers' attitude towards Internet banking in South Africa. *Southern Africa Business Review*, 17 (3), 96-100.
- Markovich, S. & Snyder, C. (2017), *M-Pesa and mobile money in Kenya: pricing for success*. *Kellogg School of Management Cases*, Vol. 1, pp. 1-17.
- Marks, J. (2009), *Playing Offense in a High-Risk Environment*. Crowe Horwath, New York, NY.
- Mas, I. & Radcliffe, D. (2011), *Scaling mobile money*. *Journal of Payments Strategy & Systems*, Vol. 5 No. 3, pp. 298-315.
- Maurer, B. (2012), *Mobile money: communication, consumption and change in the payments Space*. *Journal of Development Studies*, Vol. 48 No. 5, pp. 589-604.
- Maurer, B. (2015). *How would you like to pay? How technology is changing the future of money*. Duke University Press, Durham.
- Mbiti, I., & Weil, D. (2014). *Mobile Banking: the impact of M-Pesa in Kenya*. African Successes, Volume III: Modernization and Development.
- McKay, C., & Kaffenberger, M. (2013). Rural versus urban mobile money use: Insights from demand-side data. Consultative Group to Assist the Poor.
- Merritt, C. (2011), *Mobile money transfer services: the next phase in the evolution of person-to- person payments*. *Journal of Payments Strategy & Systems*, Vol. 5 No. 2, pp. 143-160.

- Mobile Telecommunications Network Ghana (MTN Ghana) (2019). *Mobile money fraud in Ghana*. Mobile Telecommunications Network Ghana, Winneba Branch.
- Morawczynski, O (2015). Fraud in Uganda: how millions were lost to internal collusion. From <http://www.cgap.org/blog/fraud-Uganda-how-millions-were-lost-internal-collusion>.
- Mudiri, J.L. (2013), –Fraud in mobile financial services. *Rapport Technique, MicroSave*, Vol. 30
- Mugisha, I.R. (2014). Two Men Arrested for allegedly defrauding Ks495m from Tigo. From <http://www.newtimes.co.rw/section/article/2014-11-20/183244/>.
- Myers, M.D. (2013), *Qualitative Research in Business and Management*, Sage.
- Narteh, B., Mahmoud, M.A. & Amoh, S. (2017), –Customer behavioural intentions towards mobile money services adoption in Ghana. *The Service Industries Journal*, Vol. 37 Nos 7/8, pp. 426-447.
- National Communications Authority (2021). *Mobile money fraud in Ghana*. National Communications Authority, Accra Ghana.
- Nicco-Annan, J (2021). That’s MoMo like It: everything you need to know about mobile money in Ghana,” World Remit. Accessed from <https://www.worldremit.com/en/blog/money-transfer/mobile-money-ghana>.
- Nyaga, K.M. (2013), –The impact of mobile money services on the performance of small and medium enterprises in an urban town in Kenya”, Unpublished MBA Project work. University of Nairobi.
- Osei-Assibey, E. (2015), –What drives behavioural intention of mobile money adoption? The case of ancient susu saving operations in Ghana. *International Journal of Social Economics*, Vol. 42 No. 11, pp. 962-979.
- Otieno, O.C., & Liyala, S. (2018). Mobile Money Users' Functioning’s and Freedoms: Amartya Sen's Capability Approach. *World Journal of Computer Application and Technology*, 6(1), 14-22.
- Ouma, S. A., Odongo, T. M., & Were, M. (2017). Mobile financial services and financial inclusion: Is it a boon for savings mobilization? *Review of Development Finance*, 7, 29-35.
- Owusu-Ansah, V (2017). MTN Mobile Money Fraud, An Inside Job?” retrieved from <https://www.ghanaweb.com/GhanaHomePage/NewsArchive/MTN-Mobile-Money-fraud-an-inside-job-593205>.

- Peters, O., & Allouch, S.B. (2005). Always connected: a longitudinal field study of mobile communication. *Telematics Inform*, 22(3), 239-256.
- Provencal, R.O. (2017). *Mobile money fraud on the rise in Ghana: victims share their stories*. Available at: <http://rainbowradioonline.com/index.php/general-news/item/9324-mobile-money-fraud-on-the-rise-in-ghana-victims-shares-their-stories>.
- Riddell, W.C., & Song, X. (2017). The Role of Education in Technology Use and Adoption: Evidence from the Canadian Workplace and Employee Survey. *ILR Review*, 70(5), 1219-1253.
- Rieke, R., Zhdanova, M., Repp, J., Giot, R. & Gaber, C. (2013), –Fraud detection in mobile payments utilizing process behavior analysis. *Availability, Reliability and Security (ARES), Vol. 1, pp. 662-669*.
- Rowley, M. J (2002). *Qualitative researching (2nd edition)*. London: Sage.
- Saliu, I. (2015). *Assessing the Impact of Mobile Money Transfer Service on the Socioeconomic Status of the Mobile Money Vendors: Case of Kumasi Metropolis*. Kumasi, Ghana: Kwame Nkrumah University of Science and Technology.
- Saunders, M.; Lewis, P. & Thornhill, A. (2009). *Research Methods for Business Students*. Pearson Education Limited, 5th Ed.
- Schwandt, T. A., & Schwandt, T. A. (2001). Dictionary of qualitative inquiry. *SAGE Publication*.
- Singh, A.B. (2012). Mobile banking based money order for India post: feasible model and assessing demand potential. *Procedia-Social and Behavioral Sciences*, Vol. 37, pp. 466-481.
- Sorooshian, S. (2018), –Business ethics for mobile network operators. *Science and Engineering Ethics, Vol. 24 No. 1, pp. 333-334*.
- Straub, D.W. & Welke, R.J. (1998), –Coping with systems risk: security planning models for management decision making. *MIS Quarterly, Vol. 22 No. 4, pp. 441-469*.
- Suárez, S.L. (2016), –Poor people’s money: the politics of mobile money in Mexico and Kenya. *Telecommunications Policy, Vol. 40 Nos 10/11, pp. 945-955*.
- Subex (2017). *Service providers combat mobile money frauds*. Available at: [www.subex.com/subexhelps-service-providers-combat-mobile-money-frauds/](http://www.subex.com/subexhelps-service-providers-combat-mobile-money-frauds/)
- Suri, T. & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science, Vol. 354 No. 6317, pp. 1288-1292*.
- Tobbin, P. (2012). Towards a model of adoption in mobile banking by the unbanked: A Qualitative Study. *Information, 14(5), 74-88*.

- Tuesta, D.; Sorensen, G.; Haring, A., & Camara, N. (2015). Financial Inclusion and Its Determinants: The Case of Argentina. *BBVA Working Paper No. 1503. 2015.*
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27, 425-478.
- Vlcek, W. (2011), –Global anti-money laundering standards and developing economies: the regulation of mobile money. *Development Policy Review*, Vol. 29 No. 4, pp. 415-431.
- Wang, K., Chen, G., & Chen, H. (2017). A model of technology adoption by older adults. *Social Behavior and Personality: An international Journal*, 45, 563-572.
- Weijters, B., Rangarajan, D., Falk, T., & Schillewaert, N. (2007). Determinants and outcomes of customer use of self-service technology in a retail setting. *J. Serv. Res.*, 10(1), 3-21.
- Wolfe, D.T. & Hermanson, D.R. (2004), –The fraud diamond: considering the four elements of fraud. *The CPA Journal*, Vol. 74 No. 12, pp. 38.
- Yi, Y. D., Wu, Z., & Tung, L.L. (2005). How individual differences influence technology usage behaviour. Toward an integrated framework. *Journal of Computer Information Systems*; 46 (2), 52-63.
- Yin, R. K. (2009). *Doing a case study research design and methods. 4th ed.* Thousand Oaks, CA: Sage.
- Yin, R. K. (2013). Antecedents and consequences of service quality in a higher education context: a qualitative research approach. *Quality Assurance in Education*, 21(1), 70-95.
- Yin, R. K. (2014). *Case Study Research: Design and Methods, 5th edition.* Sage, Los Angeles.
- Zhi, H. L. (2014). A comparison of convenience sampling and purposive sampling. *PubMed*, 105-11.