UNIVERSITY OF EDUCATION, WINNEBA

AN INVESTIGATION OF MOBILE MONEY FRAUD IN THE KASOA TOWNSHIP

SAMUEL AMOABENG

MASTER OF PHILOSOPHY

2022

UNIVERSITY OF EDUCATION, WINNEBA

AN INVESTIGATION OF MOBILE MONEY FRAUD IN THE KASOA TOWNSHIP

SAMUEL AMOABENG
(200026582)

A thesis in the Department of Social Studies Education, Faculty of Social Sciences Education, Submitted to the School of Graduate Studies in Partial fulfillment of the requirement for the award of the degree of Master of Philosophy (Social Studies Education) in the University of Education, Winneba

July, 2022

DECLARATION

Student's Declaration

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

Signature:……

Date:……

Supervisor's Declaration

I hereby declare that the preparation and presentation of this work were supervised in accordance with guidance for supervision of thesis as laid down by School of Graduate Studies, University of Education, Winneba.

Name of Supervisor: Dr. Joseph Ignatius Obeng

Signature:…….

Date:…….

DEDICATION

This work is dedicated to my wife, Mrs. Catherine N. A. Amoabeng, my daughter, Alexia Maame Kwaaba Amoabeng and staff of School of Graduate Studies, University of Education, Winneba.

ACKNOWLEDGEMENTS

I am most grateful to God for taking me through my studies up to this level. The contribution, advice and direction of my supervisor, Dr. Joseph Ignatius Obeng is much appreciated. I also thank Prof. George Kankam, Prof. Samuel K. Asiedu-Addo, and Dr. Akwasi K. Amoako-Gyampah, for their encouragement and support towards the completion of this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURE

ABSTRACT

For many years, efforts to make financial products and services accessible and affordable to all individuals and businesses, regardless of their personal net worth or company size, (financial inclusion) was a major challenge, globally, due to the high costs involved. In light of this, mobile banking service that allows users to store and transfer money through their mobile phones, has increased the appetite for mobile financial service deployments, especially in developing countries. Mobile money, which is a type of mobile banking, has become extremely popular around the world and most especially in countries where most of its population do not use banks. However, as more businesses and customers launch their money into cyberspace, opportunities for 21st century, tech-savvy thieves also increase. With continuous losses to fraud indicating that fraud is an issue which requires continuous attention, it is important to explore mobile money fraud. This work explored mobile money fraud in the Kasoa Township. Using mixed method approach and stratified and purposive sampling technique, a total of 394 respondents were involved in the study. Data collected were analysed quantitatively and qualitatively. Results from the study revealed that, anonymous calls from fraudsters were the most prevalent type of mobile money fraud. Also, majority of the respondent said they trusted the fraudster as their reason of being defrauded while those who could not be defrauded stated awareness as their reason. Furthermore, loss of customer and business trust, destroying business relationships, clean-up cost, collapse of business, market distortion were major effects of mobile money fraud on mobile money operations. Based on the outcome of the study, it was recommended that; Both merchants and individual subscribers in Kasoa are encouraged to save contact of their Mobile Network Operators on their phones in order to detect fake calls claiming to have come from the Service Provider's Office to help curb anonymous call related fraud in Kasoa. In addition, mobile money operators/service providers need to intensify customer awareness on mobile money fraud by using local language such as Fante, Ewe, Nzema, Hausa and Ga, with the help of local information centres in the Kasoa Township.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

For many years, efforts to make financial products and services accessible and affordable to all individuals and businesses, regardless of their personal net worth or company size, was a major challenge, globally due to the high costs involved. To offer financial services, premises had to be constructed, employees recruited and significant capital investments had to be made. Financial institutions concentrated on the high value consumers that yielded larger revenues and largely excluded the majority of the population (Mudiri, 2012).

Banking and financial institutions have been playing important role in the economic development of all the countries in the world. They contribute in different ways to ensure the efficient operation of economic activities. Thus, there is no exaggeration in saying that the banking business is the 'life blood' of industry and business in modern times. If we study the evolution and development of modern banking institutions, we will see that there were three predecessors namely merchants, money lenders and gold smiths (Arya, 2019).

It can be said that the development of modern banking has been the outcome of money exchanges in the beginning, and later as the credit creator in the economy. The seventeenth century is considered as the real development in modern banking. This can be attributed to the Industrial Revolution in the United Kingdom and its after effects in

the world, leading to increased and expanded economic activities for which adequate financial arrangement could not be made (Arya, 2019).

The banking industry is one of the areas of business that has been influenced the most by technology. Banking operations have evolved from the mere exchange of cash, cheques and other negotiable instruments to the application of information and communications technology (ICT) to banking transactions. Through technology, banks are now able to offer convenient services to their customers. According to Molla (2005), information and communications technologies (ICTs) have changed the way of conducting business transactions to meet the growing demands of customers for most organisations. The importance of information and communications technologies in the banking sector has been seen, in terms of its potential to increase customer base; reduce transaction costs; improve the quality and timeliness of responses; enhance opportunities for advertising and branding; facilitate self-service and service customisation; and improve customer communication and relationship.

Business, via the internet or electronic commerce, provides a competitive advantage for banks, by lowering their operational costs, and providing the best satisfaction of customer needs. A strong banking industry is important for every country, and can have significant effects in supporting economic development, through efficient financial services. In the world of electronic commerce, it is very important that banks provide electronic banking services in order to experience survival in the long-term (Burnham, 1996). Consequently, most banks in both developed and developing countries are now offering electronic banking services with various levels of sophistication. It is expected that banks that do

not offer electronic banking services may lose their customers to their competitors (Orr, 1999).

With the help of the internet, banks are providing benefits to their customers. From the customers' point of view, electronic banking provides convenient and valuable source to deal with funding because, it is convenient to have 24hour access to account (Applegate, Holsapple, Kalkota, Radermacher & Whinston, 1996). Customers can use these services anywhere, including their homes and offices at any time, without visiting the banks, physically. The banks, thus can use the electronic commerce technology, for meeting the competitive advantage and gaining the best level of profitability while providing best services to its customers.

The banking system in developing countries is significantly different from those in developed countries such as the United State of America. As with most developing countries, Ghana has been undergoing a process of financial sector restructuring and transformation as an integral part of a comprehensive strategy (Acquah, 2006). According to Bawumia (2007), banks in Ghana will need to re-invest in this new conducive, but challenging environment. This is important because electronic transactions will continue to grow, and only countries that make a move towards embracing electronic business will participate in this revenue generation (Akoh, 2001).

However, Kadleck (2005) contends that, as more businesses and customers launch their money into cyberspace, opportunities for 21st century, tech-savvy thieves also increase. For instance, the introduction of mobile telecommunications, and later, the adoption of mobile phones to provide financial services have changed the dynamics of the banking

sector, and this has brought financial services closer to the public, through existing merchant infrastructure within local communities. The success of M-PESA (Mobile banking service that allows users to store and transfer money through their mobile phones), since its launch in Kenya in 2007, has increased the appetite for mobile financial service deployments, especially in developing countries. Financial institutions such as banks and micro-finance institutions are also investing in the provision of mobile financial services.

Mobile money is a type of electronic banking which enables subscribers to bank directly from their mobile phones, without being physically present in a financial premise to pay bills, receive money, and transact other businesses, all through virtual mobile accounts known as the mobile money wallets (Afanu & Mamattah, 2013). Mobile money service has become extremely popular in emerging markets around the world (Chauhan, 2015; Osei-Assibey, 2015; Markovich & Snyder, 2017). In countries such as India, Uganda, Argentina, Tanzania, Zambia, Nigeria, Ghana and Kenya, where the majority of the population do not use banks, mobile money is the most convenient and easy-to-use alternative for financial transactions, instead of traditional banks (Deloitte, 2015; Markovich & Snyder, 2017).

In 2018, the mobile money industry added 143 million registered customers, globally with the total number of accounts reaching 866 million a 20 percent year-on-year increase. As at 2017, most of this growth came from Asia, where 90 million new accounts were opened. East Asia and the Pacific experienced the highest year-on-year account growth at 38 percent, and the region now accounts for 11 percent of registered accounts globally. Activity rates are stable at the global level: 34.5 percent of the world's

registered accounts are now active, up from 33.9 percent in 2017. Activity rates are once again highest in Latin America and the Caribbean (48.5 percent), while the biggest increases are in Asia (East Asia and Pacific and South Asia), where activity rates in several countries increased by more than 10 percent (GSM 2018 Report). While activity rates in sub-Saharan Africa remain stable at 36.8 percent, largely unchanged from 2017, the region added over 17.5 million new active accounts in 2018.

According to a survey conducted by the Gates Foundation, the World Bank and Gallup World Poll, out of the top 20 countries in the world for mobile money usage, 15 are in Africa. Kenya has 80 percent of the world's mobile money transactions. In addition, Kenya's M-pesa has nearly two million users registered with the system in a year of its nationwide rollout (Ivantury & Mas, 2008; Vaughan, 2007). M-pesa also provides services to 15 million Kenyans (more than a third of the country's population) and serves as a channel for a fifth of the country's GDP and processes more transactions domestically within Kenya than Western Union does globally, providing more banking facilities to more than 70 percent of the country's adult population (Bampoe, 2015). In 13 African countries, over a third of adults are active mobile money users. Transaction values also increased by 17 percent in 2018, with 272 live deployments in 90 countries transacting $40.8 billion in the month of December, 2018. The industry is, therefore, now processing over $1.3 billion per day, and while cash-in and cash-out transactions still represent, the majority of mobile money flows, digital transactions grew at more than twice the rate, driven largely by bill payments and bulk disbursements. For the average active mobile money customer, this equates to 12 transactions a month and worth $206 (Bampoe, 2015)

A report on QuartzAfrica in 2019 by Selin Ozyurt (Economist, Agencefrançaise de Dévelopment AFD) indicated that the unprecedented growth of mobile financial services in sub-Saharan Africa has defied all expectations. While Kenya is often cited as a leading example of digital transformation, Ghana has recently become the fastest-growing mobile money market in Africa, with registered accounts increasing six-fold between 2012 and 2017. The country's experience provides a fresh perspective on its digital transformation and demonstrates that technology can help modernize the financial system as well as also support greater financial inclusion (Ozyurt, 2019).

PricewaterhouseCoopers (2011) states that, over 80 percent of the adult population in Ghana do not have account in the recognised financial institutions. The number of Ghana's population keeps on increasing with an increasing number of mobile phone users hence, many Ghanaians are not part of the formal banking systems. The mobile money operation is seen as the channel through which many unbanked in Ghana can join the formal banking systems (Akomea-Frimpong, 2017).

In Ghana, mobile financial services are mostly used by those poorly served by the traditional financial sector (Ozyurt, 2019). The 2017 GlobalFindex database indicates that, access to formal financial services rose from 41 percent to adults in 2014 to 58 percent in 2017. This is largely attributable to mobile accounts, with 20 percent of digital-wallet users being previously unbanked. These represent about 40 percent of all account holders, compared to 13 percent in 2014.

The adoption of E-banking services has revolutionised how financial transactions are carried out globally. The increasing popularity and accessibility of the internet has been

an important factor as it provides the backbone for e-banking services to take place. Poong, Eze and Talha (2009) highlighted that, the internet enables people worldwide to carry out commercial activities whenever and wherever they desire. The scope of e-banking services includes Online Banking, Automated Teller Machines (ATM), Mobile Banking, and Short Messaging Service banking (Kavitha, 2017).

Ghanaians have so far used mobile wallets, principally for transferring money to a person (Peer-to-peer, P2P). According to the Bank of Ghana Annual Report (2017), the total value of all mobile money transactions reached GHS156 billion ($29 billion) in 2017, compared to GHS35 billion ($6.5 billion) in 2015. Gradually, the range of mobile accessible goods and services has successfully expanded to the purchase of mobile communication credits, payment of public service bills or salaries.

Many factors explain the rapid progress of mobile money use in Ghana. First, the strong penetration rate of mobile phones (about 128% of the population) makes the widespread use of mobile-money services possible, particularly in rural areas. Second, and more importantly, the Ghanaian success is the product of a right mix of consumer-driven practices and a favourable regulatory environment for the industry, built on the back of early infrastructure investments.

The mobile money service was first introduced in Ghana by the telecom company, MTN in 2009, and it was followed by Tigo and Airtel in 2011, and today, all the mobile money operators are involved in this service (Fintech Africa, 2017). The estimated value of mobile money transactions in 2014 was GHC11bn with 2.3 million active users. It shot up to GHC31 million in 2015 with 10.4 million active users, and as at July 2016, the

estimated value was GHC37.07bn, representing 118 percent growth over the previous year's figures with active users of 17.2 million (Akomea-Frimpong, 2017). Airtel, MTN, TIGO and Vodafone are the mobile phone operators that are driving this service in Ghana (Roberts, 2016). This momentum looks set to continue, with the mobile money market estimated to be worth of $129.29bn by 2021 all over the world (Deloitte, 2015). For instance, citinewsroom reported that, 'cheques' popularity as a means of payment declined in the first quarter of 2019, data from the Payment Systems Department of the Bank of Ghana has shown. According to the central bank's data, which excludes in house cheques, the total number of cheques cleared in the first three months of 2019 went down by nearly 121,000 compared to the same period last year representing a more than 6.7 percent decline. Also, the value of cheques transactions in the period under review went down by almost GHS5 billion, which represents more than 10 percent decline in the transactions recorded same period last year. The 2017 World Payments Report highlights the declining role of cheques as a means of payment given the rise of other efficient electronic payments methods' (citinewsroom.com).

Since its inception, mobile money service has been saddled with many fraudulent activities by scammers, with the aim of derailing the good of the service to the populace. Mobile money fraud is an intentional act perpetuated by scammers or fraudsters to gain undue advantage over mobile money subscribers, mobile money operators and mobile money agents (Subex, 2017; Merritt, 2011).

1.2 Statement of the Problem

With the growing patronage of e-banking services, some of the known factors capable of hindering the growth of mobile money must be addressed. Security concerns are of greatest importance for the adoption of e-banking services (Angelakopoulos & Mihiotis, 2011). Roberds (1998) contends that, the incentives for fraud increase in scenarios where transactions can be made in large amounts, cannot be effectively verified at the point of sale and when issuers of payment claims bear the costs of fraud. Tsai, Huang, Liu, Tsaur and Lin (2010) also explain that, the dynamic nature of technology and e-banking presents unique security challenges that require novel solutions. More recently, researchers highlight the frequency and sophistication of cyber-attacks as one of the challenges in securing e-banking services (Camillo, 2017). Therefore, there is te need for telecommunication companies, banks and other service providers to continually ensure that their e-banking channels are secured taking into consideration the dynamic nature of technology and threats. The Eurostat 2010 Information and Communication Technology survey undeniably confirmed that e-banking frauds have become the most rampant type of acquisitive fraud in both developed and underdeveloped economies (Anderson, Barton, Boehme, Clayton, Levi, Moore & Savage. 2012).

Fraud can have severe negative consequences for consumers who fall victim to it, including loss of money, insecure and at-risk accounts, and more interactions with parties attempting to defraud them (Chalwe-Mulenga et al, 2022). According to the International Public Sector Fraud Forum, (2020) study on guide to understanding total impact of fraud, it was revealed that, fraud of which mobile money fraud is no exception affects individuals, the family, the community and the government at large. The Commonwealth

Fraud Prevention Centre, (2023) supported this in their study on the total impacts of fraud. It was found from their study that, victims of fraud place burden on community health services and charity. Fraud breaks down relationships be it business, friendship or family and increases victim's debt where victims are left to either go for loans, sell his/her assets to pay debt or fail to pay his/her wards school fees if any. A victim's information could also be used to further defraud others and MNO's and governmental bodies use funds that could have been used for social infrastructure in communities for clean-up and maintenance cost.

Mobile money with its numerous benefits such as payments for goods and services, payments of insurance and loan disbursement, among others has, however, been saddled with fraud. This is because unscrupulous persons continue to use the service as a conduit to scam others (Chatain et al., 2011). Fraud not only results in financial loss to customers or the service providers, but it also damages the reputation of the service to the customer and risks the reputation of the industry as a whole (Gilman & Joyce 2006). For instance, a report by Banking, Specialised Deposit-taking Institutions (SDI) and Electronic Money Issuers (EMI) fraud in 2021 trends and statistics, EMI recorded 12,350 mobile money related fraud incidents which were valued at GH12.8million (Banking, SDI & EMI, report 2021).

A report by Mustapha on graphic.com in 2017 indicated that, one telecommunication company reportedly received about 365 complaints of fraud monthly from its subscribers while blocking more than 400.000 scammed messages daily. Estimates of analysts suggest that, about 50 percent of all mobile money subscribers have either been targeted or have experienced one form of fraud or another (Mustapha, 2017). In addition to this,

the assertion in an article in Microsave brought to bare that, an average of, at least, hundred mobile money users lose money every week resulting in mental and physical trauma for victims, increase in vulnerability, collapse of businesses and destroying business trust, among others (Mustapha, 2017).

This is a salient economic problem, but a careful review of literature indicates that priority has been placed on mobile money fraud with respect to network operators, customers' adoption of mobile money, electronic banking fraud as a whole and factors influencing electronic fraud. Arhin, (2018) conducted a similar study on mobile money fraud where he looked at the impact of fraud on the financial performance of mobile payment companies in Ghana. However, Arhin, (2018) concentrated on the impact of mobile money fraud on telecommunication companies in Ghana. More so, a study by Afanu and Mamathah, (2013) looked at mobile money security as a whole and limited their study to only one mobile telecommunication network, and the link between mobile phone security and mobile money service security. These studies focused mainly on service providers and MNO's in the mobile money service sector and did not pay attention to individual subscribers in general. This study therefore sought to fill knowledge gap by focusing on the most prevalent mobile money fraud type, factors promoting mobile money fraud and the effects of mobile money fraud all from the view point of mobile money customers.

1.3 Purpose of the Study

The purpose of this study was to investigate mobile money fraud in the Kasoa Township in order to contribute to the understanding and solution to a problem that has gotten worse over the years.

1.4 Objectives of the Study

The objectives of the study were to:

1. identify the type of mobile money fraud that is prevalent in the Kasoa Township.
2. determine the factors that promote mobile money fraud in the Kasoa Township.
3. explore how mobile money fraud affects the inhabitants in the Kasoa Township.

1.5 Research Questions

The study was based on the following research questions:

1. What type of mobile money fraud is prevalent in the Kasoa Township?
2. What factors promote mobile money fraud in the Kasoa Township?
3. How does mobile money fraud affect the inhabitants in the Kasoa Township?

1.6 Significance of the study

The study would be beneficial to mobile network operators, mobile financial institutions, software development companies, policymakers and other stakeholders. The study would serve as a guide or resource material for Mobile Network Operators, Software Development Companies, policymakers and other stakeholders in the mobile financial services industry when developing a framework for mobile banking products. It would help to create awareness of the possible effects of mobile money fraud on mobile network operators.

Also, the study would help stakeholders to identify and understand the most prevalent type of mobile money fraud in the telecommunication and mobile banking industry as a whole in order to employ the necessary steps to curtail it. In addition, this research would provide recommendations on how mobile money fraud affects the mobile money operations and the economy. It would also add to existing literature on mobile money fraud to assist other researchers.

1.7 Delimitation

The study was designed to investigate mobile money fraud in the Kasoa Township, and was limited to mobile money subscribers (e.g. Mtn mobile money, Vodafone cash and AirtelTigo cash) and mobile money agents/merchants (mobile money agents) in the Kasoa Township. Conceptually, the study focused on types of mobile money fraud, factors that promote mobile money fraud and the effects of mobile money fraud.

1.8 Limitations of the study

The study could have involved the whole municipality. However, it was conducted in Kasoa Township only with a small sample size due to limited resources. The researcher's use of the modified kish grid which recognised and sampled only people present as of the time of visit could be bias. The data collected is based on retrospective questioning and dependent upon the participants' ability to recall incidents accurately. The data could suffer from recall bias and self-serving distortions in memories. The use of questionnaire for individual subscribers restricted them from providing detailed information. Similarly, the data can be impacted by social desirability bias, as the participants could report instances to show innocence or hide their lapse in judgment. The researcher reported the

incidences as reported by the participants and did not try to authenticate the factual or technological feasibility of these attacks and claims.

1.9 Definition of Terms

Electronic banking: It is a channel whereby the customer interacts with a bank via a mobile device, such as a mobile phone or personal digital assistant (PDA). The emphasis is on data communication, and in its strictest form m-banking does not include telephone banking, either in its traditional form of voice dial-up, or through the form of dial-up to a service based on touch tone phones.

Mobile money: It is a service for transferring money that is mobile phone-based. It is the IT tools and channels that are non-banking for extending financial services to subscribers who cannot be reached by banks (Upadhyay & Jahanyan, 2016).

M-PESA: This means mobile banking service that allows users to store and transfer money through their mobile phones. In simple terms, it means Mobile Money.

Mobile money agent/merchant: A person or business that is contracted to facilitate transactions for users. The most important of these are cash-in and cash-out (i.e. loading value into the mobile money system, and then converting it back out again).

Mobile Telecommunication: Mobile Telecommunication is a type of telecommunication network with a collection of terminals, entities, and nodes connected to each other through links that enable telecommunication between the users of the terminals.

Financial Institution: Financial Institution otherwise known as banking institutions, are institutions that provide services as intermediaries of financial markets.

Mobile Financial Service: Mobile Financial Service is the use of a mobile phone to access financial services and execute financial transactions. This includes both transactional and non-transactional services, such as viewing financial information on a user's mobile phone.

Fraud: Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim.

Electronic fraud: Electronic fraud is a type of cybercrime fraud or deception which makes use of the internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.

Mobile money fraud: Mobile money fraud is an intentional act perpetuated by scammers or fraudsters to gain undue advantage over the mobile money subscribers, mobile money operators and mobile money agents (Subex, 2017; Merritt, 2011). It is a well-taught through act by the scammers to take advantage of the stakeholders of the service.

1.10 Organisation of the Study

The study is organised into five chapters. Chapter One concentrates on the introduction and it discusses the background to the study, statement of the problem, purpose of the study, research objectives, research questions, significance of the study, delimitation of the study as well as the limitations of the research. Chapter Two focuses on a review of literature relevant to the study. Chapter Three discusses the methodology adopted for the study, and it looks at the research paradigm, research approach, research design, population, sample and sampling procedures, data collection instrumentations, validity and reliability, trustworthiness, data collection procedure, method of data analysis and

ethical consideration. Chapter Four contains the findings and discussion of results, while Chapter Five highlights the major findings, conclusions and recommendations of the research work.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

2.1 Introduction

In this chapter, relevant literature that is related and consistent with the objectives of the study is reviewed. Important issues and practical problems are brought out and critically examined so as to determine the current facts. This section is vital as it determines the information that link the current study with past studies and what future studies will still need to explore so as to improve knowledge. Literature was reviewed on the following;

(i) Theoretical Framework

a) The Theory of Planned Behaviour

b) The Fraud Triangle Theory

(ii) Conceptual Review

a) Definitions

b) Types of mobile money fraud in Ghana

c) Reasons why fraudsters succeed in defrauding people

d) The effects of fraud

e) Measures implemented to combat mobile money fraud

2.2 Theoretical Framework

Although there are different fraud theories that could have been used for this study, the researcher adopted the Theory of Planned Behaviour and the Theory of Fraud Triangle.

2.2.1 The Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) is an extension of The Theory of Reasoned Action (TRA). TPB explains the factors influencing a person to behave. In this theory, there are three important factors that influence a person to have the intention before becoming a behaviour, namely attitude toward, subjective norms, and perceived behavioural control. Intentions are assumed to capture motivational factors that influence a behaviour. They are indications of how hard people are willing to try, how much people's effort are to perform the behaviour (Ajzen, 1991).

The Theory of Planned Behaviour is rooted in the notion that, actions are reasoned and planned prior to enactment (Fishbein & Ajzen, 1975; Ajzen, 1991). Attitude toward the behaviour refers to the degree to which a person has a favourable or unfavourable evaluation or appraisal to perform or not perform the behaviour (Ajzen, 1991). Bailey (2006) adds that, the attitude towards the behaviour is determined by a person's beliefs that the behaviour leads to a certain outcome and the person's evaluation of those outcomes as favourable or unfavourable. According to the TRA model, if people evaluate the suggested behaviour as positive (attitude) and if they think others want them to perform the behaviour (subjective norm), this results in a higher intention (motivation) and they are more likely to perform the behaviour (Ajzen & Fishbein, as cited in Mimiaga, 2009). Belief links the behaviour to a certain outcome or other attribute (such as cost to performing behaviour) and since the attitudes to be linked to the behaviour, a person already valued positively or negatively to perform the behaviour (Ajzen, 1991).

A subjective norm is a social factor, and it refers to a person's perception about important individuals or groups that influence the behaviour. It is a person's perception of social

pressure that influences the decision to do or not to do a behavior. It is derived from belief in norms (beliefs about what others think about our behavior) and motivation to fulfill these beliefs which is called the Normative Belief. Perceived behavioural control refers to a person's perception of the eases or difficulties of performing behaviour that assumed reflect past experience or information from others such as friend's experience. The more favourable the attitude and subjective norms, and the greater perceived behavioural control, should be an intention to perform the behaviour (Ajzen, 1991). This research uses TPB to identify the intention to commit fraud. It does not include behaviour. It is assumed that a person has the intention, thus he has willingness to make intention become the behaviour as stated by most previous studies (Ajzen 1991; Granberg & Holmberg, 1990).

2.2.2 The Fraud Triangle Theory

The Fraud Triangle Theory emerged from the criminology and sociology domains (Albrecht et al., 1982; Cressey, 1953, Sutherland, 1949; Sutherland, 1983; Morales, 2014). The Fraud Triangle Theory describes why people engaged in fraudulent activities. Cressey (1950) propounded the Fraud Triangle Theory with three elements, and they are pressure, opportunity and rationalisation. These elements are necessary for fraud to occur, and most previous adaptations of the fraud triangle have assumed that, these elements are independent of one another. A perpetrator must be motivated by some financial or social pressure to act dishonestly, perceive an opportunity to exploit another individual for his or her own gain, and has the ability to rationalise, and thus justify in his or her own mind, immoral or criminal act. A fourth element representing the perceived capability of the

perpetrator to commit a fraudulent misrepresentation has been advocated as an extension to the fraud triangle (Rittenberg et al., 2010; Wolfe & Hermanson, 2004).

Firstly, the pressure to commit fraud is the result of greed, ego, perceived financial necessity or poor judgment (Albrecht et al., 2009). Social normative influences are typically assumed to influence people to avoid immoral actions, but strong pressures to be perceived as successful, powerful or affluent have also become motivating factors for individuals to commit fraud (Dilla et al., 2011). Lister (2007) identifies pressure as one of the most significant factors to commit fraud. Pressure works as a catalyst behind every fraud perpetrator while committing unethical behaviour (Abdullahi & Mansor, 2015). Chen and Elder (2007) categorised pressure into the following, transgression of obligations, problems originated from individual problems, corporate inversion, position achievement and relationship between employees.

Secondly, opportunities are often manifest as weak controls and procedures that may mask or obscure the perpetrator's fraudulent actions (Cohen et al., 2010). The anonymity of individuals engaged in many transactions occurring on the Internet is one example of a weak control system (Zahra et al., 2005). The concept of perceived opportunity suggests that, people will take advantage of circumstances available to them (Kelly & Hartley, 2010). Kenyon and Tilton (2006) mention some factors like weak internal control, lack of supervision and inadequate segregation of duties may create opportunities to commit fraud. Wilks and Zimbelman (2004) indicate that, when the perception of management's attitude regarding risk of fraud is low, the level of sensitivity of auditors to opportunity and incentive is higher.

In addition, individuals must be willing to rationalise their actions, despite their actions deviating from common social norms against lying, cheating or stealing (Albrecht et al., 2009; Rittenberg et al., 2010). Ironically, this rationalisation may also be the result of emphasising a greater sense of social duty, such as providing for one's family or helping others through a period of crisis (Choo & Tan, 2007; Cohen, Ding, Lesage & Stolowy, 2010).

Finally, the communication, technical, financial or economic capabilities individuals possess can influence their ability to commit fraud. Charm, charisma and the ability to communicate well with others are useful for committing fraud and masking cues to deception. Fraud participators try to rationalise their fraud activities in different ways. Sometimes, many fraud participants try to rationalise by stating what manipulation they have done is just for short time period. WorldCom's point of rationalisation was that it was a one-time matter and company would make it up in future (Kennedy, 2012). Lehman Brothers also put similar rationalisation that they needed to do it to keep business alive and to protect its stakeholders (Jeffrey et al., 2011).

However, the Fraud Triangle Theory was criticised by researchers such as Kassem and Higson (2012) who argued that the model alone is an inadequate tool for deterring, preventing and detecting fraud. Kassem and Higson continued that two sides of the triangle (pressure and rationalisation) cannot be observed and factors like fraudsters' capabilities are ignored. A fraudster must be capable of successfully deceiving the other party in an exchange (Wolfe & Hermanson, 2004). Therefore, he or she must possess a set of capabilities that fits the requirements needed to successfully defraud a victim.

Fraudsters and social engineers use their abilities to influence others and develop a false sense of trust in others in order to gain some advantage (Ramamoorti, 2008).

Despite the fact that the authors did not offer a theoretical justification for linking the elements in the fraud triangle (Cressey, 1953; Albrecht et al., 1982), it has been successfully integrated with other structured behavioural models such as the Theory of Planned Behaviour, and these models have been used to describe managerial and financial statement fraud (Buchan, 2005; Carpenter & Reimers, 2005; Cohen et al., 2010).

Existing literature on corporate fraud suggests that, combining a structured behavioural approach with the fraud triangle is a useful and appropriate extension. However, there is currently no widely used structured behavioural model for describing interpersonal fraud (Carpenter & Reimers, 2005; Cohen et al., 2010; Grazioli & Jarvenpaa, 2000; Rofiq & Mula, 2010).

In furtherance to this, although the Planned Behaviour and Fraud Triangle theories fit this work, the Fraud Triangle with a fourth component being the fraudster's capabilities is more appropriate for the this study.

2.3 Conceptual Review

2.3.1 Definitions

The Concept of Electronic Banking

Electronic banking (e-banking) was born out of globalisation, competition and rapid growth of Information Technology systems. It has become the self-service delivery channel that allows banks to provide information and offer services to their customers,

with more convenience via several technology services, such as the Internet and mobile phone (Kurnia, Peng & Liu, 2010). This new technology was adopted by many organisations to enhance customer service quality and delivery, and reduce costs compared to the traditional approach. Electronic banking is an inexpensive way to conduct banking business, exchange information, and buy and sell goods or services from any place at any time. Also, it is a way to keep the existing customers and attract others to the bank (Chaimaa, Najib & Rachid, 2021).

E-banking allows the user to access services virtually thanks to the different forms of e-banking such as home banking, personal computer (PC) banking, Internet banking and mobile banking. Therefore, several benefits are offered, including convenience, ease to use, low cost, time factor, fast delivery and on-line bill payment. Electronic banking is the designated term for the new age banking system, and it is based on the automated delivery of banking products and services to customers through electronic delivery channels (Kurnia, Peng & Liu 2010). A common definition for e-banking is provided by the Basel Committee on Banking Supervision which says that, e-banking includes the provision of retail and small value banking products and services through electronic channels as well as large vale electronic payments and other wholesale banking services delivered electronically (BCBS, 1998; Drig & Isac, 2014). Previously, customers accessed e-banking services using automatic teller machines (ATMs) or touch tone telephone. Actually, several intelligent electronic devices are used, including a personal computer (PC) and personal digital assistant (PDA) (Chavan, 2013).

E-banking concept allows customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a

public or private network, including the internet (Kurnia, Peng & Liu, 2010). The basic services associated with e-banking are viewing, checking and savings account balances, paying bills, transferring funds between accounts, requesting credit card advances, and ordering checks for faster services (Singhal & Padhmanabhan, 2009). Therefore, it is obvious that, e-banking has a major impact on increasing the efficiency and convenience of the banking operations and services for customers. Without any physical contact, customers can transact from one corner of the country to another corner (Singhal & Padhmanabhan, 2009).

Mobile Banking

Mobile banking plays a key role in our modern economy, and has become an integral part of people's lives. Today, mobile users can conduct basic banking transactions such as checking balances, paying bills and transferring money from anywhere, anytime. Mobile phones are not only used for communication purposes, but are also used for banking transactions (Tembely & Musa, 2017).

Mobile banking (or m-banking) is an emerging branch of electronic or online banking. It is an application of mobile commerce based on wireless networks and mobile devices. It consists of banks, telecommunication companies and mobile devices, and uses software called an app, which can be downloaded to a mobile device. Since apps handle sensitive personal information, their safety is important (Matthew, Tembely, Musa & Momoh, 2017).

The mobile user is connected to a mobile network through a SIM card. Mobile banking has a unique competitive edge over traditional banking because, it allows customers to

perform banking transactions, irrespective of place and time. The advantages of mobile banking for both banks and customers include easy access anywhere, control over one's money, availability on 24-hour basis, and reduction in the cost of handling banking transactions. One does not need to have Internet connection; a mobile connection is all that is required. Right now, banks are not charging customers for their mobile banking services. But wireless carriers do charge some fees (Matthew et al, 2017).

M-banking can be defined as a channel whereby the customer interacts with a bank via a mobile device, such as a mobile phone or personal digital assistant (PDA). The emphasis is on data communication, and in its strictest form, m-banking does not include telephone banking, either in its traditional form of voice dial-up, or through the form of dial-up to a service, based on touch tone phones (Barnes & Corbitt, 2003).

Mobile banking via smart phones and tablets is one of the technological wonders of recent times. It uses cell phones and PDAs to access banking services via a wireless application protocol. It is growing rapidly and it has come to stay. It allows customers to take advantage of the latest advanced technologies. Mobile money has the potential of increasing the wealth of its users. Mobile banking is inevitable for the banks to stay competitive, though it has not been adopted to its full potential, leaving plenty of room for improvement (Tembely & Musa, 2017).

Fraud

Fraud is usually understood as dishonesty calculated for an advantage—a deception deliberately practiced so as to secure unfair or unlawful gain. Fraud within the context of mobile cash is that, the intentional and deliberate action undertaken by players within the

mobile money services scheme geared toward derivation gain (in money or e-money), and/or denying different players revenue and/or damaging the name of the opposite stakeholders (Mudiri, 2012). Fraud refers to crimes within which deceptive or false acts are committed for private, usually money, gained through falsehood of self and/ or guarantees of products, services, or money advantages that do not exist, were never supposed to be provided, or were disingenuous (OVC 2019a; OVC 2019b).

Electronic Fraud

Internet or cyber area has, in recent times, been a 'carrier of load' on people, businesses and nations. This can be as a result of the internet that has expedited communication, business transactions and education. Despite the myriad advantages of the employment of the internet, it's conjointly been a straightforward platform for criminals to commit fraud, harass or bully individuals, transfer smuggled and sexy materials to violate national security. These crimes area unit is referred to as cybercrime. Cybercrimes area unit classified as cyber act of terrorism, cyber erotica, cyber bullying, Spam and internet fraud. Internet fraud could be a sub to law-breaking. It is usually referred notably as "419" scams or ''sakawa'' in geographic area, specifically in several African nations (Ninson, 2017). Several students have consented to share data on these platforms, and these have been a means of internet fraud. Its practices, however, have raised some vital new considerations regarding the potential of destabilising socio-economic progress of states (Burell, 2008). The Bureau of Justice Statistics explains internet fraud as the intentional falsehood of knowledge or identity to deceive others (Rantala, 2004). Similarly, the Department of Justice outlines internet fraud as a fraud that uses any

element of the internet to accomplish the supposed fallacious activity (National White Collar Crime Center, 2008).

The Australian Federal Police (2016) conceptualises internet fraud, typically as any sort of fraud theme that uses one or additional on-line services such as chat rooms, e-mail, message boards, or internet sites to gift fallacious solicitations to prospective victims, to conduct fallacious transactions, or to transmit the issue of fraud to money establishments or to others connected with the theme (Ninson, 2017). Another scholar shared a concept on net fraud, contending that, it is any fallacious activity that involves the employment of electronic computer or different sort of ICT as a target supply (Pati ,n.b). Presumably, these definitions may be tailored in conceptualising net fraud because the use of net resource to commission fallacious act. Parker, 2000 contends that, the functions of the net in net fraud are classified into four-folds. That is, it is associated with nursing object for crime, as a subject matter for crime, as a tool for crime and as a logo for crime.

The Concept of Mobile Money

The use of mobile money has become well-known among mobile phone users, mobile telecommunication networks, technology experts and academia, in recent years (Narteh, Mahmoud, Amoh, 2017; Asongu & Asongu, 2018). It gained much attention across the world as a payment system after the first two "Mobile Money Summits" in 2008 and 2009 (Suri & Jack, 2016; Maurer, 2015; Gosavi, 2017). Some scholars also attribute the genesis of the mobile money service to M-PESA, which originated from Kenya, and it has spread to many developing countries across the earth (Markovich & Snyder, 2017). The service can be accessed via mobile phone (Etim, 2014). Jenkins (2008) proposes that, services such as bill payment, salary payment and local and international remittances

should be added to the mobile money platform, and these products have been embedded into the service recently. These added features and services are equated in the same category of banking by financial analysts. The mobile money service also helps in paying other bills on electricity and water, digital television, parking fees and several other services. This is a rising trend among many consumers, especially those in urban settings but this phenomenon is rampant among wealthy urban mobile phone users (Nyaga, 2013).

A report by the Yale School of Management (2017) asserts that, there are over a billion people in the world, today, who do not have bank account, but own a cell phone. This can be attributed largely to banks finding it too much expensive to retail locations and ATMs in poorer and most rural areas, and as a result, the people at the base of the pyramid are often left with only informal networks to transfer and save money (Yale School of Management, 2017). Mobile money fills this gap by providing a variety of financial services from simple transfer and savings to other more complicated products. The introduction of mobile money in Africa was driven by two factors, namely the strong penetration of mobile phone which is expected to grow to 80 percent in the next two years and about 41 percent of population in developing countries having access to financial services (Ibid).

In July 2009, MTN Ghana launched a mobile money cash management service called MTN Mobile Money. It took a while to gain as much attraction as in other African countries, due to the Bank of Ghana's restrictive 2008 Branchless Banking Guidelines. Five years later, however, the Bank of Ghana revised the regulations, and eventually released new agent and e-money guidelines. These new regulations permitted mobile

network operators (MNOs) to own and operate mobile money services under the supervision of the Central Bank. Shortly after that, players such as telecommunication giant, MTN invested heavily in creating awareness, educating customers and recruiting agents and merchants (Yale School of Management, 2017). MTN Mobile Money is a collaborative effort between MTN Ghana, authorised merchants, and ten banks in Ghana: Ecobank, Fidelity Bank, GT Bank, CAL Bank, Stanbic Bank, Zenith Bank, UBA, Merchant Bank, Intercontinental (Access) Bank, and Agriculture Development Bank (MTN Ghana2, n.d.). After few years, available MNOs such as Vodafone, Airtel, Tigo now AirtelTigo all began mobile money service in Ghana. Most of the mobile money services are mobile phone enabled (MTN Ghana2, n.d.). Some of the services offered under mobile money are also available to non-mobile users, and can be used over other internet-enabled devices other than the mobile phone, or facilitated at MNO Ghana Service Centres, Partner Bank Branches, or at authorised mobile money merchant locations throughout Ghana (MTN Ghana, 2012; MTN Ghana, n.d.).

Mobile money is projected to have significant impact on various money-related practices at the personal and business levels. Mobile money is marketed in Ghana as a means of pre-paying for mobile phone units (for oneself and others) without having to purchase a phone card, as a mechanism for money transfer (for personal use, person to person transfer, and purchases (www.mtn.com.gh; www. Airtel.com). In addition, market-wide adoption and use of mobile money in Ghana would eliminate the current challenges faced by Ghanaian consumers including lack of access to the formal banking sector by the poor (Mensah & Dzokoto, 2011), hassles involved with dealing with the banking sector (including queuing for long periods of time to use existing banking services for those

who have bank accounts); the need for carrying large sums of cash for large purchases (since credit cards where available and checks are accepted only from trusted customers that vendors have a long term relationship with), and the recurring problem of lack of change for small purchases (e.g. from street vendors).

Mobile Money Fraud

Fraud, in the context of mobile money, can be said to be the intentional and deliberate actions undertaken by players in the mobile financial services ecosystem, aimed at deriving financial gains, denying other players revenue or damaging the reputation of other stakeholders. The occurrence and prevalence of fraud is dependent on the stage of implementation of the mobile money service. Thus, as deployment evolves, the types of fraud evolve with it (Mudiri, 2012; Gilman & Joyce, 2012). Key enablers of mobile money fraud include maturity of the mobile money services, weak or non-standard processes, cultural issues, lack of compliance monitoring (Mudiri, 2012) and any new value added services not thought through properly, for example, the post-paid scheme in which the transaction is applied to the user's phone bill to be paid later (Merritt, 2010).

Mobile phones are by nature small in size, and the possibility of them being lost or misplaced or stolen is very high, hence it becomes an easy target for theft. Proper measures, therefore, must be put in place to restrict unauthorised access to mobile phone data in order to prevent exposure to sensitive data that may be stored on them, or accessible from them in the event of theft (NIST SP800-124, 2008). A survey of taxi companies in Sweden, Great Britain, Australia, Denmark, France, Germany, Norway, Finland, and the U.S. revealed that, tens of thousands of digital devices (including mobile

phones) were mistakenly left behind (Checkpoint, 2005). In addition to the compromise of logical and physical data, a mobile phone with active service, such as mobile money service could be accessed without authorisation, leading to theft of money from mobile money wallets.

Furthermore, the mobile phone itself could have significant financial value, and can be restored to its original settings, manually and reused easily, even if the contents of the user stored on the phone are wiped away (NIST SP800-124, 2008). Available user authentication mechanisms on mobile phones are PINs, patterns and passwords. While these modes of authentication mechanisms are not fool-proof, they are the first line of defence to prevent unauthorised access to mobile phones. However, access to mobile phones and its contents can be gained by forging or guessing the authentication credentials or bypassing the authentication mechanism entirely (NIST SP800-124, 2008). Interestingly, most mobile phone users hardly employ security mechanisms built into the mobile phone, and even if they do, often they use settings that could easily be guessed such as using 1234 or 0000 (Knijff, 2002).

Arguably, weaknesses in the authentication method are another avenue that could be exploited. This is because some devices have a master password built into the authentication mechanism, which allows unlimited access when entered, including bypassing the security lock set by the user (Knijff, 2002; NIST SP800-124, 2008). Jansen and Ayers (2007) opine that, the mechanisms available to acquire master passwords include calculating it directly from the equipment identifier (Jansen & Ayers, 2007), the use of backdoor to bypass all or part of the control mechanism (Withers, 2008), and forensic tools also exist that could be used to bypass built-in security mechanisms to

recover the contents stored on the mobile phone (Ayers, Jansen, Moenner & Delaitre, 2007; Breeuwsma et al., 2007 & Troy, 2008). Malware is another threat to the security of mobile devices. Communication networks are, sometimes used to deliver viruses and other forms of malware to mobile phones. Malware can spread in a variety of ways, such as being attached to SMS received, internet downloads and bluetooth messages received. Malware can eavesdrop on user's input and steal sensitive information stored on the mobile phone, and can also be used to allow an attacker to gain access at will (NIST SP800-124, 2008).

Mobile money recorded 53 percent of fraud cases of the entire mobile money transactions in Uganda, 42 percent in Tanzania, 12 percent in Kenya and 23 percent in Ghana, in 2015 (Busuulwa, 2016; Laryea, 2016). A report by Mustapha in graphic.com.gh, noted that in 2017, one of the telecommunication companies in Ghana reported that, it received about 365 complaints of fraud monthly from its subscribers. The scale of attempts at fraud is staggering as the telecommunication operator also indicated that it filtered all SMS messages that passed through its platforms and blocked more than 400,000 scammed messages on a daily basis from reaching the recipients. Analysts suggest that, about 50 percent of all mobile money subscribers have either been targeted or have experienced one form of fraud or another (Mustapha, 2017). This is evident in a study by Weber (2010), who revealed that reliability and security are the two major drawbacks of the mobile money payment system.

Mobile money transactions were mainly meant to make transactions within the mobile or online platforms rather than cash payments, which have now become the norm. This has resulted in reported attacks, and even murder of mobile money agents. In addition,

mobile money has come to be associated with a number of fraudulent activities, and this has led to loss of money and stealing of passwords, among others. Most often, criminals use a lot of strategies to defraud mobile money agents, consumers and financial service providers.

2.3.2 Types of Mobile Money Fraud in Ghana

Key enablers of mobile money fraud include maturity of the mobile money services, weak or non-standard processes, cultural issues, lack of compliance monitoring (Mudiri, 2012) and any new value added services not thought through properly, for example, the post-paid scheme in which the transaction is applied to the user's phone bill to be paid later (Merritt, 2010).

A study by Mudiri (2012) on fraud in mobile financial services outlined the following major categories of fraud and provides types under each category:

Consumer-driven fraud: Consumer-driven fraud is fraud that is initiated by fraudsters posing as customers. Consumer fraud targets agents, other consumers, businesses and mobile financial service providers. This type of fraud is the most common fraud on the market and transcends the different stages of the deployment. It is more prevalent during the transaction activation stage of the business when consumers begin to trust the mobile financial service better, but are yet to understand many of the potential risks of the service. The key method of managing consumer-driven fraud is consumer education activities, although there are many processes and system-based checks that can also help mitigate these challenges (Mudiri, 2012). The most common types of consumer driven fraud include the following:

(i) Counterfeit (fake) money – Fraudulent customers deposit counterfeit currency with agents and receive electronic money. They immediately withdraw the electronic money at other agent outlets, ATM devices or point of sale devices.

(ii) Phishing – Fraudulent consumers send fake SMS to agents either from their own handsets or generated from computers but the SMS may looks genuine to the recipient.

(iii) Customers conning agents after creating a relationship with the agent employee – Fraudulent customers develop a relationship with agent employees and con the employees of cash or electronic money.

Agent-driven fraud: It is perpetuated from within the agent network. The fraud is initiated and operated 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 prevalent at the beginning of the deployment, catalysed by early loopholes in product pricing. The fraud evolves over time, changing form, victims and impact on the deployment (Mudiri, 2012). The key types of agent-driven fraud include the following:

(i) Employees defrauding agents

(ii) Split deposits and

(iii) Master agents defrauding agents.

Business partner-related fraud: It describes the fraudulent activities perpetrated from the business partners' network. Business partners include business to consumer (B2C), consumer to business (C2B) and merchants. The fraudulent activities may be perpetrated by employees on the business organisation, employees on customers and partner

businesses on the mobile money operator. Business partner related frauds are more prevalent during the value addition stage of the deployment. This is mainly because business partnerships grow at this stage. This type of fraud is still in its early stages because the adoption of business transactions is still in its nascent stages (Mudiri, 2012). The most common types of business partner fraud include:

(i) Employees of businesses defrauding customers; and

(ii) Employees of businesses defrauding the businesses.

Mobile financial service provider fraud: This is a range of fraudulent activities perpetrated by the mobile financial service providers' employees. The fraudulent activities would be carried without authorisation of the business. The key types of fraud in this area include fraud on the mobile money operator, mobile money operators' employees defrauding agents, businesses and consumers. Fraud in the ecosystem is less prevalent at the beginning of the deployment and becomes common during the customer activation and value stages of the deployment. At this stage, substantial electronic money has been invested in the system and it therefore becomes attractive to fraudsters. Mudiri (2012) provides some examples such as:

(i) Mobile operators' employees stealing funds from the business;

(ii) Collusion between fraudulent mobile money employees and other fraudsters to carry out unauthorised SIM swaps;

(iii) Unauthorisediiaccess of financial records for personal gain; and

(iv) Unauthorised transfer of funds from customers' accounts.

System-related fraud: System-related fraud covers all fraud activities that affect the mobile money deployment through system weaknesses and processes. System-related

fraud cuts across different stakeholders, including agents, businesses, and mobile money operators. System-related fraud is highest when a platform has inadequate controls to guide in transaction processing. This fraud is prevalent during transaction activation stage of the deployment, and continues to grow into the value addition stage (Ibid). Under system related fraud, Mudiri (2012) identifies the following:

(i) Password/PIN sharing;

(ii) Weak password and transaction PIN strength;

(iii) Creation of fake and non-existent users on the mobile financial services platform;

(iv) Individual users with multiple rights; and

(v) Fraud on multiple access channels.

However, in the INTERPOL (2020) report, the major categories of fraud mentioned by Mudiri (2012) namely consumer-driven fraud, agent-driven fraud, business partner-related fraud, mobile financial service provider fraud and system related fraud were described as the types of mobile money fraud instead.

In an article published by the Ghana News Agency edition of September 3, 2021, Dr. Herbert Gustav Yankson, the Director Cybercrime Unit of the Criminal Investigations Department (CID), Ghana Police Service, revealed that cyber fraud makes up 45 percent of all cybercrime cases, making it the topmost. Dr. Yankson explained that, MoMo fraud involves fraudulent acts perpetrated against MoMo users through the use of deceit for unsuspecting victims to part with money.

Dr. Yankson said that, some of the schemes used by MoMo fraudsters include the Raffle Scheme (one receives a call that he or she has won a raffle and to claim the prize, some

amount of money would have to be paid); Long service award (one receives a call that he or she has been a long serving customer and is eligible for an award. The fraudsters then request for money as part of requirements for the award). Another scheme is the false SMS (a false SMS is sent to your number claiming that money was mistakenly sent to you, and that you should send it back. If an unsuspecting victim fails to crosscheck from his or her account balance, he or she may end up sending their own money to the fraudsters).

Dr. Yankson also mentioned the sick child scheme (the fraudsters manage to gather intelligence on their target victim, call with the information that his or her child is sick, and has been admitted at the hospital. They would then request for some amount of money urgently needed to settle some bills of the victim's child, otherwise the hospital staff would not attend to the child). Others are; police arrest scheme, romance scheme (mostly carried out on social media), transaction reversal scheme, spiritual schemes (someone calls claiming that he has been asked to kill you through spiritual means but then he wants to spare your life so send him some money as compensation) and fraudulent SIM swap scheme (the fraudsters are able to convince the Tele-Communications Company (TelCos) to change someone's SIM and re-register it using their details so that they can have control and use it) (Ghana News Agency, 2021).

However, an article by Annan (2018) published in the Business and Financial Times came out with the types of mobile money fraud as: scam messages/reversal of erroneous transfer, emotional scam, anonymous calls from fraudsters, cash-out fraud, vender pin fraud, false promotion, fortuitous scam and MNO fraud, and they are explained below:

With scam messages/reversal of erroneous transactions, fraudsters often resort to sending fake SMS messages to subscribers' phones (smishing) or email (phishing), alerting the customer of a cash in transaction on his mobile money wallet. Shortly, thereafter, the fraudster calls the customer claiming to have erroneously sent money to a wrong customer number. Innocently and before checking the balance on his or her mobile money wallet, the subscriber makes a transaction to reverse the "erroneously sent money" from his or her account, thus losing money. This fraud is also perpetrated in the form of cooked messages from fraudsters bearing a supposed source from the service provider requesting one to change one's PIN and reply by texting the old PIN and desired new PIN to the sender from whence the fraudsters use one's PIN at their discretion to make unauthorised withdrawals (Annan, 2018).

According to Annan (2018), emotional delusional SMS is where the fraudster sends an SMS seeming to have originated from the mobile money service provider. The fraudsters will then call and tell the recipient that, the fraudster's mother is sick on admission at the hospital and that, he/she has wrongly transferred some amount to the recipient's wallet instead to his/her sister at the hospital who is caring for the sick mother. The fraudster then asks for the money to be returned to a named number, and under the guise of emotional sympathy the prospective victim sends money without having verified the SMS's authenticity (Annan, 2018).

Furthermore, Annan (2018) identified anonymous calls from fraudsters as a type of mobile money fraud. Here, customers receive calls from fraudsters after deposits, to transfer funds received with the claim being that airtime has been wrongfully sent to the prospective victim and often times this is not cross-checked before (supposedly)

resending by subscribers. cash-out fraud was also mentioned as a type of momo fraud. With this fraud, customers are pushed by a payment approval prompt, and lured to enter their pin code in order to receive a prize won through mobile money, and are then tricked with an authorisation SMS.

The type of MoMo fraud that is usually targeted at MoMo agents, especially those who have high customer traffic is called vender-pin fraud. It is a common practice for these busy MoMo agents to initiate a transaction and then hand over his/her phone to the customer to punch in his/her number. The customer then gives the phone back to the agent to complete the transaction by inserting his/her PIN code. Fraudsters take advantage of this. They go to the agent in the guise of a normal customer wanting to process a transaction, and follow the usual process. During this time, the fraudsters study the buttons pressed by the agent for his/her PIN code. After a few visits to the agent, the fraudsters can usually identify the agent's PIN code as it is a 4-digit password (Annan, 2018). The fraudster then goes to the agent to transact (to either deposit or send money). This time when the agent hands over his/her phone to the supposed 'customer/subscriber' (fraudster), the fraudster quickly punches in a phone number, inserts the agent's PIN code and completes the transaction. The fraudster then starts another transaction to cover his/her tracks and hands the phone back to the vendor/agent to complete the genuine transaction (Annan, 2018).

Annan (2018) likened false promotion to an advance-fee fraud maintaining that, it is a new strategy used by fraudsters. These tricksters run on the ambit of the fierce competition in the telco industry that has precipitated price-wars, bonuses on airtime top-ups, and special prizes under loyalty programmes which include cash, cars, refrigerators,

houses among others. Winners are alerted through telephone calls asking them to pick up their prizes. The fraudsters respond quickly by creating their own 'call centres. Posing as staff from the telco, these tricksters call prospective victims, informing them that, they are lucky winners of bogus packages, and should come quickly to redeem their prizes. However, they request the subscriber (their "lucky winner") to make an initial deposit of mobile money to facilitate the process of handing over the prize. Also, customers can be lured to authorise cash-out transactions with the claim of winning a Mobile Money promotion.

In fortuitous scam, fraudsters call to dupe customers under the pretext of delivering goods from abroad (Vishing), which the subscriber never expected. Some fraudsters call and ask for specified amounts to be deposited into a mobile money account, in exchange for these goods from supposed relatives/ friends abroad (Annan, 2018).

Lastly, MNO fraud has been identified to be a type of momo fraud by Annan (2018). This type of fraud is usually perpetuated by the mobile network operator (MNOs) or service provider's employees. The victims of this type of fraud include the service provider, merchant, agent or the customer. Examples of this fraud include the service provider stealing customer's electronic cash; unauthorised transfer of funds from a customer's account; and collusion between fraudulent mobile money employees and other fraudsters to carry out unauthorised SIM swap and transactions from customers' mobile money wallets.

Employees also engage in identity theft/fraud by accessing and exploiting customer information without authorisation. Many incidents of this type of fraud have been

reported on the media across other African countries. Fraud situations for mobile network operators (MNOs) can be high; yet because of MNOs' non-disclosure, the extent of fraud with mobile money is unknown. Ayettey (2019), in her article "Momo fraud, How scammers steal your money", published on modernghana.com fully supported Annan's list on the types of mobile money fraud and their explanations provided.

On the other hand, Akomea-Frimpong, Akomea-Frimpong, Andoh and Dwomoh-Okudzeto (2020) in their study on Control of fraud on mobile services in Ghana: An exploratory study, classified mobile money fraud in Ghana into three, namely subscribers' fraud, employee and agents' fraud and systems' fraud.

Akomea-Frimpong et al. (2020) posit that, mobile money services are patronised by mobile subscribers who go through many steps before they are registered. Unfortunately, some of the subscribers register with the aim of using deceptive means to transact businesses, and steal money from other subscribers and the mobile money operators. The activities of fraudulent subscribers affect the unwitting people with estimated 50 per cent of mobile money subscribers and mobile money operators being subjected to the whims and caprices of the fraudulent subscribers. They steal mobile money codes, SIM cards, PINs and other relevant information to advance and manipulate the transactions to their favour (Akomeah-Frimpong et al., 2020). While there are honest, ethical, trustworthy and business-minded mobile money agents, who are burnt on helping the mobile money service to succeed, there are some who have lined themselves up to dupe and manipulate the transaction processes and profit from it with the employees of the mobile money operators. These scammers create multiple dummy accounts and passwords to siphon money into them, and use these funds for their own good. For instance, 3,000 mobile

money agents were caught in conniving with mobile money subscribers to defraud the mobile money operators in Ghana in 2017, and these agents were sanctioned. Also, employees of mobile money operators have been accused of helping the mobile money agents to steal money from the mobile money subscribers. These incidences can be attributed to poor and porous internal controls instituted by the mobile money operators that allow employees and agents to get away with their crimes Akomea-Frimpong et al. (2020).

Many sophisticated algorithms have been invented to help the activities of telecommunication operators to accomplish different purposes, but some of the operators do not have some of these information technology (IT) systems designed purposely for the mobile money operations. Some of the systems have become obsolete and cannot compete with the increasing challenges associated with mobile money operations (Vlcek, 2011). Due to these weaknesses, scammers go round the system and use it to dupe others of their money. Fraudulent technology experts also manoeuvre the IT systems to dupe others and cover them up. Mudiri (2012) also revealed that mobile money fraud can be categorised into consumer-driven fraud, merchant or agent-driven fraud, business partner-related fraud, system administration fraud and MNO fraud.

Akomea-Frimpong et al. (2020) further identified some common mobile money fraud cases on mobile money service that have been reported in Ghana as anonymous calls and text messages from fraudsters, false promotion, scam and false cash out SMS. Fraudsters call mobile money subscribers that, they have deposited money into their accounts mistakenly, and therefore, they should transfer back to them. These are normally detected as false claims after the mobile money account balances are checked.

Secondly, some mobile money subscribers are deceived to transfer money to fraudsters after they have been told to authorise cash out transactions because, they have won mobile money promotion. Fraudulent mobile money subscribers send fake messages to their agents, either from their own handsets or generated from computers as genuine messages by the recipients; they pay the money fraudsters, but later on detect that they were fake (Provencal, 2017). Thirdly, fraudsters call to deceive subscribers that they are to deliver goods from abroad or from a close relative under false pretence. 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.

Lastly, fraudsters send false cash out messages to merchants for authorisation of which the physical cash is issued by the merchant to the fraudster without the equivalent e-cash (Provencal, 2017). The scammers take a very long time to plan about it, and sometimes get resources and technical assistance from cartels that pounce on the weaknesses in the system to enrich themselves (Maurer, 2012).

Arhin, 2018 in his study on the impact of fraud on financial performance of payment companies in Ghana, sought to find the different types of fraud and which one is most commonly found in the telecom companies. It was found from the study that, anonymous calls from fraudsters, false promotion, cash out fraud, scam, false cash out sms and false promotion sms were the types of fraud and among them, anonymous calls from fraudsters was the most common fraud type happening in the telecommunication companies in Ghana.

According to Mudiri (2012), GNA (2021), Annan (2018), Akomea-Frimpong et al. (2020) and Arhin (2018), although there have been divergent views as to what the types of mobile money fraud are, the researcher deduced that Mobile Money Fraud could be through phone calls, phone messages or both phone calls and messages. Also, the researcher is in agreement with Annan (2018) as provided in the Business and Financial Times, and also supported by Ayettey (2019) in an article in modernghana.com. The reason being that, Annan (2018) and Ayettey (2019) simplified the types of mobile money fraud without merging them, and this makes it clear and easy to understand.

2.3.3 Reasons why Fraudsters Succeed in Defrauding People

Too often, we focus our attention on the culpability of victims in these situations. But, it is the offenders and their actions we should be focusing on. How exactly do fraudsters get victims to do such outlandish things?

Cross (2018), in her study on, "How to get away with fraud: The successful techniques of scamming", outlined three ways through which fraudsters succeed in defrauding people, namely grooming the victims, using the social engineering technique and coercive control. Cross (2018) explains grooming the victim as a culmination of efforts that result in the victim sending money or complying with a fraudster's request. Some offenders target specific victims and build a profile of them, through online or offline tracking. In other cases, the contact may start as random, but the fraudster will work hard to establish the trust and build rapport. Several fraud victims that Cross interviewed in her study confessed that, they saved all their chat logs with their offenders from the first contact. Re-reading these conversations allows them to feel a deeper connection to the words and the person sending them, compared to a verbal conversation. By being persistent and

patient with their contacts, fraudsters raise few red flags when they ask a victim for money. Many victims come to believe the situation they are being presented with and the reason behind the request (Cross, 2018).

Also, online offenders are able to identify a weakness or vulnerability in a person relatively quickly and decide on the appropriate strategy to exploit this. The use of authority to gain trust and compliance is a common place. Offenders will take on the identity of a person or organisation, and use this to threaten victims into submitting to their requests. Fear can be a strong motivating factor, and this explains why so many people fall for phishing emails, or those that appear in our inboxes from a bank or government organisation. These emails say there is a problem, and provide a negative consequence (such as the closure or freezing of a bank account) if their instructions are not followed.

A sense of authority has been clear in the recent scams targeting Chinese students in Melbourne who have been tricked into staging their own kidnappings. The victims receive calls from the Chinese "police" or some other authority, and are told there is a problem with their visa, or that they have been involved in criminal activity (Cross, 2018). In order to prove their innocence, the victims are asked to send money or, they are directed to stage their own kidnapping, with the intention of extorting money from their families. The threat of deportation and jail time is a powerful motivator for victims, who genuinely fear for their safety.

The use of scarcity or the idea of a limited offer is another successful technique of fraudsters. By implying their request has a limited time frame for response, or that the

promised reward is limited in availability, they compel people to respond. Examples of scarcity are commonly seen with lottery scams and sales fraud. Earlier in 2016, for instance, Scamwatch reported, that fraudsters advertised pedigree breeds of puppies for sale, and demanded money up front, to cover transport or medical costs. Victims were duped out of over AU$300,000 in a single year. This was attributed to the use of the social engineering technique (Cross, 2018).

Cross (2018) further maintains that, with coercive control, the use of psychological abuse tactics by online fraudsters helps to explain why they have so much power over victims, despite a lack of physical proximity. In these cases, offenders employ abusive techniques in their communication, to gain compliance at the beginning and maintain it throughout the fraud. In Cross' research, several victims reported being verbally abused when they questioned the nature of the relationship or refused to send money. Several victims felt the offenders were deliberately leading them to question themselves or their own judgment. This destabilisation is not exclusive to romance fraud and can allow offenders to exploit victims over long periods of time (Cross, 2018).

Many segments of society which traditionally have been at very low risk of crime victimisation, have in a short period of time, become much more high risk. For example, many crime surveys show young men as the most likely to be victims of crime (theft and violence), and older people to be the least likely victims of crime (ONS, 2013). However, the technological changes that has emerged have opened up many older people to be high risk of a variety of frauds (OFT, 2006). Thus, the pensioner who is offline is safe in his/her house, and are at very low risk of suffering a property-related crime, as soon as he/she switches on the computer or smartphone, check their email, surf the web or answer

the phone is suddenly connecting to a much higher risk world. There are many who readily accept that, older people are attractive targets for potential fraud offenders (Reiboldt & Vogel 2001), arguably through factors such as access to life savings, superannuation, ability to access additional lines of credit and their likely ownership of property. Many offenders will seek to target older people, specifically based on these circumstances and use the internet to perpetrate this.

Practitioners widely believe that people who were former victims of fraud are likely to be re-victimised (FTC, 2013b; NCVC & FINRA, 2013; Karp & Kirkman, 2016). Victims of identity fraud can be re-victimised because their personally identifying information, passwords, or other sensitive data have been exposed. This information can be re-used by the same perpetrator or sold to others and cause the victim to experience identity fraud once again (Pierce, 2009; Heckers & O'Brien, 2004). According to NCVS-ITS, many victims experience multiple types of identity fraud. Specifically, about 16 percent of all victims (1.8 million victims) experienced multiple types of identity fraud during a two-year period (Langton & Planty 2010). Although their personal information may not necessarily be compromised, victims of non-identity frauds can also experience re-victimisation.

Similar to identity frauds, the names of past non-identity fraud victims are, sometimes sold on the dark web; these are known as "mooch" or "sucker" lists, and they make victims more likely to be targeted again (Johnson, 2003; Deem, 2018; NCVC & FINRA, 2013). Sometimes, a fraud perpetrator premise a victim for the next fraud, while still scamming them (Karp & Kirkman, 2016). For example, some victims of fraud may be directed to fake remediation services that are also scams (Canan & Hume 2016). This re-

victimisation can also occur with victims who have memory impairments, because they may not recognise the crime or remember how to respond if they continue to be exposed, they may continue to be victimised (Deem, 2018). Notably, victims of non-identity frauds can also become victims of identity frauds through these same channels.

Practical evidence shows that, children are likely targets for identity fraud because of their clean credit histories and the lower likelihood of detection (Idaho Coalition Against Identity Theft, 2010b; FTC, 2011f). Parents may use their children's information to get credit without knowing the consequences (Toporoff et al., 2013; OVC, 2010), sometimes to meet their family's basic needs (FTC, 2011d; FTC, 2011f) or out of necessity for access to employment or services, as in the case of some undocumented immigrants (FTC, 2011f). This increases the risk of identity fraud for these children (Idaho Coalition Against Identity Theft, 2010b; Miller & Robuck, 2013), and this makes them the most exposed group among all children (FTC, 2011f).

Among adults, younger adults are among the most frequent victims of identity fraud and fraud in general, while older adults are at higher risk of specific other frauds. According to NCVS-ITS, persons aged between 25 and 64 have a higher prevalence rate of identity fraud than persons aged between 18 and 24 and 65 or older (Harrell, 2017; Harrell, 2019). A 2005 FTC survey found similar results: persons between ages 65 and 74 years were 32 percent less likely to report having experienced any of the identity frauds than those between 35 and 44 years. In the same survey, the likelihood of having experienced any of the frauds was 64 percent less for those who were 75 years and older than for those between 35 and 44 years (Synovate, 2007).

Furthermore, according to the FTC's 2011 Fraud Survey, people aged between 65 and 74 years were less likely to become victims of fraud in general, as well as the special categories of weight loss product fraud and prize frauds, relative to people who were 35-44 years (Anderson, 2013). Evidence from research studies and practice suggests that, older individuals can be more prone to certain types of fraud, such as sweepstake and lottery scams (AARP, 2003; Karp & Kirkman, 2016; Holtfreter et al., 2015). In addition, a report by AARP Foundation National in 2011 on "fraud victim study" came out with key findings that victims that were 55 years of age and older were significantly less likely to acknowledge that they were defrauded, significantly less likely to report their victimisation, and were less upset by the prospect of losing money in the future than victims under 55years' (AARP Foundation, 2011) report.

This implies that fraudsters have some factors to their advantage. However, with the exception of Cross (2018) who in a way spelt out ways and techniques used by fraudsters to succeed, all others including Karp and Kirkman (2016), Holtfreter et al., (2015), AAR (2003), Anderson (2003), Harrell (2017), Synvote (2007) outlined why and how victims are vulnerable to fraud.

2.3.4 The Effects of Fraud

The impact of fraud goes well beyond financial loss. Fraud affects people, industries, entities, services and the environment. Understanding the total impact of fraud allows entities to make better informed decisions. Serious impacts can arise from any type of fraud, whether it is carried out by opportunistic individuals or serious and organised crime groups. However, serious and organised crime can often increase the scale and effects of fraud. Since the introduction of technology, the banking industry has

experienced a paradigm change in the phenomenon (Dzomira, 2015a). However, with the development of technology, e-banking frauds have similarly increased, and its effects cannot be overlooked.

In Arhin's study, it was revealed that, fraudsters steal money ranging from Gh200-Gh3,500. Further, mobile money fraud negatively impacted the profit margin of telecommunication companies in Ghana (Arhin, 2018).

According to the Common Wealth Fraud Prevention Centre, (2020), fraud can affect humans. The centre report stated that, fraud can be a traumatic experience that often causes real and irreversible impacts for victims, their families, carers and communities. Those who rely on government services (such as the elderly, the vulnerable, sick and the disadvantaged) are often the ones most harmed by fraud (Common Wealth Fraud Prevention Centre, 2020). The International Public Sector Fraud Forum (2019) supports the position of the Common Wealth Fraud Prevention Centre that, fraud affects humans. The centre opines that, public bodies exist to improve the lives of the citizens they serve. Considering the effects of fraud on humans, it will help them approach fraud in a way that is most meaningful to those citizens. While the direct financial loss is borne by public bodies, behind every story of fraud, there are real individuals, families and communities whose lives have been impacted or even destroyed. The damage to these individuals can be financial, physical or mental, trust issues, business collapse etc.

The Common Wealth Fraud Prevention Centre, (2020) projected that, fraud indeed affects government's reputation, industry, security and finance. The centre added that, fraud undermines the government's ability to deliver services and achieve intended

outcomes. Money and services are diverted away from those who need it and the services delivered can be sub-standard or unsafe, and this can lead to programme failure (Common Wealth Fraud Prevention Centre, (2020). In line with the above, the International Public Sector Fraud (2019) opines that, when fraud against a public body occurs, it diverts finite resources and compromises the government's ability to deliver services and achieve intended outcomes. Also, fraud can affect any entity. However, when it is handled poorly, it can result in the erosion of trust in government and industries, and lead to a loss of international and economic reputation. This is particularly true when fraud is facilitated by corruption (Common Wealth Fraud Prevention Centre, 2020).

According to the International Public Sector Fraud Forum, (2019) report, reputational harm occurs when fraud could have been prevented or is mismanaged. Reputational impacts include: erosion of trust in government: significant fraud against a public body may result in general erosion of trust in government. This can negatively impact how people conduct business at the personal, industry and state levels. Other parties may not trust government with information; may feel a lack of confidence in the government's ability to deliver programmes or policies, or view government as a soft target for further exploitation. Erosion of trust in the integrity of the public sector has been shown to lead to a decrease in legal compliance.

Fraud can result in distorted markets where fraudsters obtain a competitive advantage and drive out legitimate businesses. It can affect services delivered by businesses, and expose other sectors to further instances of fraud. It can also result in greater burdens on charities and community services that help those affected by fraud (Common Wealth Fraud

Prevention Centre, 2020). The International Public Sector Fraud Forum, (2019) gives deeper explanations to that of Common Wealth Fraud Prevention on Industry Impact. In their view, erosion of trust in industry as an impact of fraud can result in not only loss to government, but can have further impacts on industry. Legitimate business in an industry where fraud has occurred against a government programme can be tarnished by association. The Fraud Forum points out the following; Employee morale and performance, damage to international and economic reputation (International Public Sector Fraud Forum, 2019).

A PricewaterhouseCoopers Global Economic Crime Survey (2021) found that, reputation, brand and employee morale are the most damaging effects of fraud. The study highlighted that while it is difficult to quantify the cost of such collateral damage, it can ruin careers by association, deter employees, investors, suppliers and customers, and should be of real concern to organisations. The Common Wealth Fraud Prevention Centre also believes that costs for dealing with fraud against government programmes are significant and go well beyond the direct financial loss. They can include assessment, detection, investigation and response costs as well as potential restitution. In addition, further costs can include programme reviews and audits, and retrofitting or redesigning programmes. Also, fraud can undermine national defence and security. It can also damage international standing and affect the ability of nations to get international support. The proceeds of fraud can also fund organised crime groups and terrorism, potentially leading to further crime and terrorist attacks (Common Wealth Fraud Prevention Centre, 2020). Where information leaks out from public bodies due to fraud, this leads to reduced trust, and reluctance by the public to provide government with

secure information (International Public Sector Fraud Forum, 2019). Government entities generally lose between 0.5 and 5 percent of their spending to fraud and related losses based on international estimates.

The majority of fraud is undetected and can be difficult to categorise. Measurement exercises can help entities uncover and more accurately estimate their potential fraud losses (Common Wealth Fraud Prevention Centre, 2020). Direct financial harms can occur through a range of methods. Victims of tax fraud lose their refunds to perpetrators of fraud who filed the return first, victims of existing account fraud (account takeover) have money from their bank accounts used by someone else, and victims of a broad range of frauds are tricked into giving up their money over the phone, through a wire transfer, in the mail, or over the internet under false pretences. Among reports of fraud in 2017 (excluding identity fraud), wire transfers were the most frequently reported to the FTC as the vehicle for financial losses, with a total of $333 million cumulatively lost from all victims (FTC, 2018a).

Collectively, fraud creates large financial losses for victims in the U.S. The 2008 NCVS-ITS estimated $17.3 billion was lost in the previous two-year period to identity fraud (Langton & Planty, 2010). Reports to the Federal Trade Commission's Consumer Sentinel Network produced an estimate of $905 million loss to fraud (excluding identity fraud) in 2017 alone (FTC, 2018a). For individual victims, fraud usually results in financial loss, but the amount differs by type of fraud. For non-identity frauds, the most recent estimate of median loss was $60, however, the costliest fraud – work-at-home scams – resulted in a median loss of $200 (Anderson, 2007). For identity fraud victims, the median value of goods and services lost was $500 as of 2005 (Synovate, 2007), but

these values differed among different types of identity fraud. For example, for victims of new account fraud the median value loss was $1,350 as of 2005 (Synovate, 2007) and $900 in 2016 (Harrell, 2019). For existing account fraud, including credit and non-credit card fraud, the median value was less than $500 in 2005, and similarly, $200 in 2016 (Synovate, 2007; Harrell, 2019). Likewise, NCVS (2017) reports that, the median loss for new account frauds was $1,900, whereas fraud in existing accounts had a median loss of $200.

The percentage of victims who experienced losses also differs by victimisation type. NCVS reported that, including both direct and indirect costs (such as legal fees or overdraft charges), 67 percent of identity fraud victims reported a financial loss in 2016, with a median average loss of $300 (Harrell, 2019). The percentage of victims who experienced financial loss due to existing account fraud (68%) was higher than the percentage of victims who had a financial loss due to new account fraud (40%), for example. Furthermore, among victims who experienced multiple identity fraud victimisations, 73 percent reported a direct financial loss.

It must be noted, however, that the initial loss of money does not always result in a personal financial loss to the victim. For some types of identity fraud existing and new account fraud in particular, an individual has limited financial liability. The Fair Credit Billing Act (FCBA) limits an individual's liability for credit card fraud and places limits on liability for debit card fraud, and this depend on the reporting time frame. Moreover, many state laws preclude an individual being held responsible for accounts opened in his/her name without permission (FTC, n.d.). As a result of these legal liability limitations, the actual personal financial loss from identity fraud and other fraud can be

considerably less than the amount stolen by the perpetrator. According to the NCVS (2017), for example, in 2016, only 12 percent of identity fraud victims experienced direct or indirect out-of-pocket losses greater than a dollar, in contrast with the 67 percent that had some initial financial loss (Harrell, 2017). Javelin's 2017 Identity Theft survey found that, the victims of account takeover paid an average of $290 out of pocket (Pascual, Marchini & Miller, 2018). In the specific case of identity theft related tax fraud, once an individual's victimisation experience has been confirmed by the victim and IRS, if the victim is due for a refund, the funds are typically released to them (IRS, 2019). However, these direct financial losses are not equally distributed among all victims of frauds, due to the varied types of fraud (of which only some have limited liability) and the differences of individual experiences. In addition, the victims of certain types of fraud have higher financial losses.

The FTC reported that, while in 2017 the median loss of fraud reports was $429, victims of Travel/Vacation Scams lost a median of $1,710, victims of Mortgage Foreclosure Relief/Debt Management Scams lost $1,200, and victims of business/ job opportunity scams lost $1,063 (FTC, 2018a). Moreover, in a small percentage of cases, victims experienced much higher losses than the median average. For example, for new account fraud victims, while the median amount lost in 2005 was $1,350, ten percent of cases involved initial losses of $15,000, and the top five percent lost $30,000 in goods or services (not necessarily out-of-pocket losses) (Synovate, 2007). Some victims never recover their financial losses, because a perpetrator may dispose of the funds immediately and there are barriers to accessing remediation and victim compensation (NCVC & FINRA, n.d.c). For example, receiving the benefits of legal protection often requires

extensive and complicated communication with the creditors and financial institutions that can be beyond the capabilities of some victims.

However, experts in fraud victimisation emphasise that the mental and emotional consequences of fraud victimisation can resemble those of victims of violent crimes (NCVC & FINRA, 2013). The emotional and mental responses may include shame, fear, paranoia, disbelief, hopelessness, anger, loss of ability to trust, questioning of spiritual beliefs, perception of lack of justice, and even depression, anxiety, psychological disorders, and suicidality (Heckers & O'Brien, 2014; NCVC & FINRA 2013; Texas Identity Theft Coalition 2010b; Texas Identity Theft Coalition, 2010c; Golladay & Holtfreter, 2017). Researchers even developed the term, "Fraud Trauma Syndrome" to describe the emotional experience of victims of fraud (Goldstein, Goldstein, & Fornaro, 2010). Estimates of the extent of these negative mental and emotional responses to fraud victimisation ranged from 20 percent to more than half of victims. Results of the 2008 NCVS-ITS suggested that, 20 percent of identity fraud victims perceived the experience as "severely distressing" (Langton & Planty, 2010).

The 2014 NCVS-ITS found that, 36 percent of victims experienced moderate or severe emotional distress (Harrell, 2017), and in 2016, one in ten respondents reported that, they were severely distressed as a result of the crime (Harrell, 2019). That year, severe stress was most prevalent among victims whose information was used to open a new account or for fraudulent purposes (Harrell, 2019). Furthermore, among 172 victims of the Bernie Madoff Ponzi Scheme surveyed through an online convenience study for 8-10 months following the revelation of the scam, the majority of respondents met the criteria for post-traumatic stress disorder (Freshman, 2012). Also, 61 percent of respondents reported high

levels of anxiety and 58 percent reported symptoms of depression (Freshman, 2012). The ITRC Aftermath Study reported that, 56 percent of identity fraud victims experienced rage while 37 percent reported fear about their future (ITRC, 2017).

Practitioners hypothesise about the reasons many victims of identity fraud and other fraud experience emotional responses to a financial crime. One potential contributing factor is the fear and perceived risk of revictimisation (Texas Identity Theft Coalition 2010b; FTC, 2017f). As described previously, victims of identity and other fraud may experience revictimisation due to their already compromised personally identifying information or the presence of their names on the lists of supposedly susceptible targets available on the dark web. The realistic fear of revictimisation may leave victims in a heightened emotional state. Practitioners note that non-responsive legal and law enforcement systems can make victims feel revictimised in instances where their cases go uninvestigated or unprosecuted (OVC, 2010).

Fraud victims may experience physical health consequences related to the mental, emotional, and stress responses to their victimisation, as they may miss out on rest, food, or social activities (OVC TTAC, n.d.c). For example, the ITRC aftermath study found that, in 2017, 48 percent of identity fraud victims experienced sleep disturbances, 35 percent had fatigue, and 34 percent experienced headaches following their victimization (ITRC, 2017). Medical identity theft, where an individual's identity is used by a thief who obtains health services in their name (potentially with their health insurance), can also be the source of unique physical health consequences. As a result of medical identity theft, a victim's medical records can be incorrect, including blood type and medical history. In the worst case scenario, this can be very dangerous, especially if information

like blood type or allergies is only discovered in an emergency (Dixon, 2006; Ponemon Institute, 2013). Practitioner sources suggest that, 20 percent of medical identity theft victims experience negative health outcomes, including mistreatment, misdiagnosis or delayed care (FTC, 2017d).

Synovate (2007) suggests that, civil and criminal legal troubles can also result from fraud victimisation. For example, victims of many types of identity fraud can end up being sued for debts that they did not incur themselves (Pierce, 2009). Furthermore, the victim can incur a false criminal record and this can impact employment, housing and other aspects of life for the victim (Heckers & O'Brien, 2014). First, the time burden of recovering from fraud can be substantial. Research shows that one-third to half of identity fraud victims are able to resolve problems stemming from their victimisation within one day (Synovate, 2007; Harrell 2017, 2019; Langton & Planty, 2010). However, some victims with more complicated cases can have protracted problems. One survey showed that, one-third of victims had problems lasting at least, a month (Harrell, 2017) and two other surveys showed that one to three percent of victims still had problems after six months (Langton & Planty, 2010; Harrell, 2019). Practitioners emphasise that, sometimes the problems, especially the fear associated with revictimisation, may never entirely be resolved (FTC, 2017d; FTC, 2011f). The total amount of time spent resolving these problems is, thus uneven among victims; while the median number of hours spent resolving identity fraud problems was four, the top five percent of victims of identity fraud spent more than 130 hours addressing the crime (Synovate, 2007). This time burden can also prevent victims from taking advantage of other opportunities (ITRC, 2018a).

The various proponents of fraud effects stem from the fact that indeed fraud effects are inevitable. However, they over concentrated the effects on government and public bodies than on individuals and the community.

2.3.5 Measures implemented to combat mobile money fraud

Mechanisms are being put in place to manage the risks associated with the mobile money service (Singh, 2012; Merritt, 2011; Gilman & Joyce, 2012).

In a study by Akomea-Frimpong, et al, 2020 on Control of fraud on mobile money services in Ghana: an exploratory study outlined the contributions of four key players to the fight against fraud in the mobile money industry. These four key players are: Central banks, partnering banks and fund managers, mobile money operators and their agents and mobile money subscribers.

Central banks: Central banks are responsible for laying out measures that control the activities of the mobile money service (Maurer, 2012). Central banks undertake exercise based on the comments by various industry players on some lapses in existing laws which guide the service. Central banks call for all the views of the key stakeholders on the service, and these views are analyzed thoroughly before a paper will be put out to assist in arriving at a policy document. Mobile money operators over the years have argued that these policy documents are not enough to help them address the numerous risk associated with the service (Mas and Radcliffe, 2011). Central banks clarify these issues in their updated policy documents they design to facilitate the process to further financial inclusion on yearly basis. Central banks educate mobile money operators on various digital financing and e-business transactions, as well as on money laundering, mobile

money fraud and the measures to combat them (Suárez, 2016). Central banks also connect the mobile money operators to the various security agencies and the government.

Partnering banks and fund managers: For years now, banks have always played many roles at the same time: serving as financial intermediaries, managing funds and assisting customers in financial transactions (Bara, 2013). But these transactions come with a lot of risks. The mobile money service is one of the financial innovation products the banks have added to their portfolio (Markovich and Snyder, 2017). In countries where the mobile money service was generated by the banks, they tend to have more control over the operations of the service (Singh, 2012) but in some countries like Ghana, banks serve as fund managers for the mobile money operators. These banks assist the MNOs to diversify their investments and revenue to avoid total cash-out in future to manage their operations. The banks manage the funds of the mobile money operators with the directives from the central bank. The banks put forth tight requirements for the mobile money operators and they also train them and give them guidelines on cash limits to their subscribers. Know Your Customer (KYC) is ensured by the banks to do away with fraudulent transactions. Nowadays, banks operate with sophisticated software which are capable of detecting and safeguarding funds from the mobile money operators against fraudsters and hacks (Narteh et al., 2017).

Mobile money operators and their agents: To facilitate financial inclusion and attract the unbanked to be part of the formal banking systems, the central banks starting from Kenya (through M-PESA) has encouraged telecommunication companies to be involved (Merritt, 2011). Cooperation among telecommunication companies and their stakeholders have been identified to be key in driving out fraudsters and sustaining the service (Klein

and Mayer, 2011). According to Gilman and Joyce (2012), collaboration of the mobile money operators and their agents with security agencies is the next major key that will help to regulate the service and root out fraudsters. Institution of effective internal controls is a prime priority of the mobile money operators, and they are guided religiously by industry standards and guidelines from the central banks. Regular in-house training on the mobile money services with improved remuneration packages are used to boost the morale of their employees and agents to cut out fraudulent activities. Mobile money operators also apply KYC procedures strictly and regularize the review of subscribers' accounts, passwords and other information (Sorooshian, 2018).

Mobile money subscribers: It is the responsibility of the mobile money subscribers to help the mobile money operators and security agencies to identify fraudsters (Gilman and Joyce, 2012). They report the cases of scam and assist in investigations to unravel fraudulent transactions (Suárez, 2016).

According to Katusiime, 2021, most governments introduce policies and laws to govern every facet of their citizens' social life, which include the operation of mobile money banking industries. The outcomes of such policies and laws in the mobile money service tend to have an overarching influence on the user's adoption of mobile money (David-West et al., 2021; Dolowitz & Marsh, 2000; Katusiime, 2021; Radaelli, 2005). Government policy is to bring sanity and protect customers, and industry players. Such policies must be fine-tuned to ensure a good balance and not disrupt the mobile money banking ecology (Katusiime, 2021; Radaelli, 2005).

The laws on mobile money by the Government of Ghana are several folds. The law and regulations set for both banks and non-banking financial institutions operating include mobile money and mobile banking services (Kelly & Palaniappan, 2022).

The Central Bank of Ghana, which regulates the establishment and implementation of all banking activities, is also tasked with ensuring the safety of customers' deposits, compliance with legal and regulatory standards, and the operation of an efficient mobile payment system. Previous studies show that such policies and laws have influenced the acceptance of mobile money and banking services in other jurisdictions (Kingiri & Fu, 2019; Martin, 2019). Other studies have revealed the challenges related to government policy with mobile money and mobile banking services, where government policy has impacted the SIM registration irregularities affecting the adoption of such technology related to mobile banking services (Kemal, 2019; Malinga & Maiga, 2020).

In 2017, the financial sector in Ghana underwent massive overhaul as banks and other financial institutions that were unlicensed or noncompliant were shut down by the Bank of Ghana (Banda, 2018). Many depositors of the collapsed institutions were heavily affected and were unable to recover their deposits and investments because of the institutions' mismanagement (Banda, 2018). However, mobile money operations continued. As mobile money grew, fraud began to emerge in the sector. The Ghana Chamber of Telecommunications reported 278 mobile money–related fraud cases in 2015 and 388 cases in 2016 (Akomea-Frimpong et al., 2019). In April 2021, the chamber mentioned that over 4,000 cases of mobile money fraud were under investigation (Brown, 2021).

By 2017, fraud was not an uncommon occurrence among MTN subscribers (Annan, 2017). It was reported that 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. Telcos 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 example, to curb fraud, MTN has made it mandatory for customers to display a national ID before transacting with any of its agents or merchants. This policy took effect in 2021 amid arguments that it could derail DFI because access to national IDs remains a challenge and that use of IDs for transactions would not help to curb fraud (Senyo, 2021). With this policy, about twenty thousand agents have been blacklisted by MTN Mobile Money Limited for creating false transactions and trying to earn commission fraudulently (Buachi, 2021). According Mr. Eli Hini (CEO, Mtn mobile money, Ghana) Significant success has been achieved in the company's quest to deal with MoMo fraud though the use of ID cards for MoMo withdrawals, and locking phones of fraudsters has made fraud expensive for the culprits.

The Ghana Cyber Authority outlined on their website, ways to avoid being a victim of mobile money fraud. According to them, Mobile Money fraud is among the common fraud that is reported. These were; never give your mobile money pin to anyone, make your pin harder for people to guess, don't give your phone to mobile money agents, wait for confirmation and beware of fraudulent text messages and calls. Annan, 2017 shared tips on how to prevent mobile money fraud in his article on MyJoy online for users. According to him, it is imperative for businesses, individuals alike who are merchants,

customers or subscribers to stay alert and put in place measures which mitigate Momo fraud. Annan came out with these measures.

Do not share your pin number with vendors/agents: Your pin (Personal Identification Number) is like your password or secret code for processing of transactions. Your pin should not be made known to the vendor or agent during transactions as this put the customer/ vendee at risk to fraud due to mobile money. According to Annan, no vendor or agent has the right to demand the private pin numbers of customers when performing a function on the mobile money platform and if you think someone has seen your pin or it has been compromised, change it immediately.

Protect your pin: Ensure you do not chose easy- to- guess pin codes as your PIN Numbers like Date-of-Birth, Year-of-Birth, Car Number Plates, Post Office Box addresses since third parties can easily breakthrough. Additionally, memorize your PIN, Do Not write them down nor note them on your phone or in an app on your computer nor tell anyone what they are and always remember to shield your keypad when entering your PIN at any Agent point during transactions. You are encouraged to change your PIN at least every 3 months.

Confirm the identity/ name of receiving subscriber: Do a due diligence (verification) of the name of the account you are sending funds to. Don't be outwitted by someone who says he has sent money mistakenly to your account, even if you believe their story, please check your balance first before you proceed to do any transactions. Pay attention when doing your transactions, Make sure what you type in is the name you want to type in. This is the commonest trend use by these tricksters, they call pleading that they have

mistakenly sent you some money so ask you to resend it immediately. Unfortunately many fall for this without cross checking their account balance first before responding to such calls or check if payment alert received earlier has same transaction ID number as that on deposit on account confirmation.

Don't let anyone carry your phones to withdraw money for you: Avoid the practice of sending third parties to cash out monies on your behalf. Some of these third parties may include friends, boyfriends, and girlfriends among other relations, could easily monitor your transactions and divert funds to other mobile money account numbers. Even if you want to send someone, ensure that you change your PIN when the phone is returned to you. If you are a vendor/agent ensure that you make an end to end transaction by yourself and avoid customer contact with agents' phones.

Check your balance after every transaction: Check and record your balance after every transaction is completed. Also check your account balance when you receive a suspicious message. You may also call the MNO call centre to verify if the number that called you is the genuine owner of an unallocated mistaken money as there could be genuine incidence of wrong receipts of money. For vendors, they should ensure records of all transactions are done with balances after every transaction recorded so that an audit trail can be made.

Ignore suspicious calls or messages: Ignore such calls and messages when you suspect them to be of a fraudulent activity. Report it to the telecommunication company to follow up and deal with the issue. The Telecommunications companies (telcos) are working closely with the e-crime bureau and the Ghana Police to clamp down on these criminals when reported.

However, Mr. Eli Hini in an interview with citi fm, categorised the tips on how to curb mobile money fraud into three which he referred as the golden rules. First of all the fraudster is not able to be effective if he is working independently and that is why they call send messages to consumers to try and get your mobile money PIN. Also, you should not entertain a call from someone saying you have won a promotion especially if you have not participated in one, and thirdly do not allow anybody to perform transactions on your behalf because that gives the person access to your PIN (businessinsiderafrica.com).

2.4 Chapter Summary

The literature review looked at the works surrounding theories of fraud, conceptual definitions such as; electronic banking, fraud, electronic fraud, mobile money and mobile money fraud, types of mobile money fraud in Ghana, why fraudsters succeed in defrauding victims and the effects of fraud. The review brought to light few theories in an attempt to understand fraud. These are the Fraud Triangle and the Theory of Planned Behaviour. However, the study was guided by the Fraud Triangle, but with a fourth component as capabilities or abilities of fraudsters. The review uncovered types of mobile money fraud such as scam messages, emotional messages, anonymous calls from fraudsters, cash-out fraud, false promotion, vender pin fraud fortuitous scam and mobile network operator (MNO) fraud.

One major gap from the literature review was that, there were no clear ways as to why people become victims or fraudsters succeed in defrauding people. Most literature provided the vulnerability of people to fraud. Also, even though there were effects of fraud, some of them were viewed from a national perspective. The study was therefore designed to fill the gaps.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter outlines the methodology that was employed for the study. It discusses the research paradigm, research approach, research design, study area, population, sample size, sample and sampling procedure, data collection instruments, validity and reliability of the instrument, trustworthiness, data collection procedure, data analysis methods and ethical consideration.

3.2 Research Paradigm

Research paradigm defines the worldview, the thinking, the believe or the school of thought ascribed by a researcher (Kivunja & Kuyini, 2017). It describes the philosophical underpinnings which guide the study. There are four main research paradigms namely, positivism (i.e. modernism), interpretivism (i.e. constructivism or post-modernism), critical or transformative and pragmstism. The positivist paradigm describes the worldview to research which is grounded in using scientific method of investigation. It is used to search for cause-and-effect relationships in nature and tries to interpret observations in terms of facts or measurable entities (Fadhel, 2002). The interpretivist paradigm is the worldview of researchers that is grounded in understanding the subjective world of human behaviour and experience (Guba & Lincoln, 1989 as cited in Kivunja & Kuyini, 2017). This approach tries to understand and interpret what the subject is thinking or the meaning one is making of the context. The main tenet of the interpretivist paradigm is that reality is socially constructed (Bogdan & Biklen, 1989). The critical or ttransformative paradigm defines the worldview of research which is grounded in issues

of social justice. It seeks to address the political, social and economic issues, which lead to social oppression, conflict, struggle, and power structure in the society. It also seeks to change the politics so as to confront social oppression and improve the social justice leading to transformation in the socio-political system (Kivunja & Kuyini, 2017). The pragmatist paradigm defines the worldview which provides the methods of research that are seen to be more practical and pluralistic in nature. It allows a combination of methods that in conjunction could shed light on the actual behaviour of participants, the beliefs that stand behind those behaviours and the consequences that are likely to follow from different behaviours. To the pragmatist, there is no single reality and all individuals have their own unique interpretations of reality (Alise & Teddlie, 2010; Biesta, 2010; Tashakkori & Teddlie, 2003).

This study employed the pragmatist paradigm because the researcher believes that no single scientific method is adequate enough to explain the social reality of the world at a particular instance (Alise & Teddlie, 2010). The study sought to identify the type of mobile money fraud that are prevalent fall in a positivist approach. The other aspect that involves in determining the factors that promote mobile money fraud and exploring how mobile money fraud affects the inhabitants make use of both positivist and constructivist approach. The study therefore requires the combination of some ideologies from both positivist and constructivist and hence the use of pragmatist paradigm.

3.3 Research Approach

According to Chetty (2016), research approach is a plan and procedure that consists of steps of broad assumptions to detailed method of data collection, analysis and interpretation.There are three types of research approaches; namely qualitative,

quantitative and mixed methods approach. Qualitative research is concerned with subjective assessment of attitudes, opinions and behaviour of a phenomenon. This approach normally generates results, either in non-quantitative form or in the form which does not require rigorous quantitative analysis (Saunders et al., 2008). Quantitative research, on the other hand, normally uses data collection techniques, such as questionnaire or analysis as graphs or statistics that generates numerical data.

For better interpretation and presentation of findings, both qualitative and quantitative research approaches were employed (Mixed Methods Approach) in this research. Mixed method approach is characterised by the fact that, it allows both quantitative and qualitative data to be collected at the same time, therefore, providing a more complete understanding than either quantitative or qualitative data only. Mixed method is useful in the sense that it can answer research questions that other methodologies cannot answer therefore, provide better inferences. It also provides the opportunity for presenting a greater diversity of divergent views, and also has the ability to increase validity of the study. This view is corroborated by Niglas (2004) that, the use of different methods in researching a phenomenon provides mutual confirmation and making the results more valid.

3.4 Research Design

A research design serves as a blueprint that guides a researcher on the process of collecting, analysing and interpreting data (Creswell, 2014). The explanatory sequential mixed method was adopted for this study. According to Plano and Creswell (2011), the design consists of, collecting quantitative data and then collecting qualitative data to further give explanations or throw more light on the quantitative results. Creswell (2014)

argues that, the rational for this approach is to make sure that quantitative data results provide a general overview of the research problem.

In an exploratory sequential design, the researcher first collects and analyzes qualitative data, and these findings inform subsequent quantitative data collection (Onwuegbuzie, Bustamante, and Nelson 2010). An explanatory sequential design, according to Plano (2011), consists of first collecting quantitative data and then collecting qualitative data to help explain or elaborate on the quantitative results. The rational for this approach is that the quantitative data and results provide a general picture of the research problem; more analysis, specifically through qualitative data collection is needed to refine, extend or explain the general picture.

3.5 The Study Area

The study was carried out in the Kasoa Township, the capital of the Awutu Senya East Municipal. The town is situated in the Central Region, along the Accra-Cape Coast Road. Fante (a dialect of Akan) and Ewutu (a dialect of Guan) are the main indigenous people of the Kasoa Township. Akan and English are the most commonly spoken languages. Kasoa is, traditioonally a home to the Gomoa and Awutu people who are part of the Akan ethnic group. Today, it is a home to other ethnic groups such as the Ga, Akan, Ewe, Wale/Dagarti, Mostrie and Basare, among others. As at 2020, Kasoa's population was estimated to be 69,384 (GSS, 2021). Ghana has experienced rapid population growth in the past three decades, and the Kasoa Township is no exception. In fact, Kasoa is reported to be one of the fastest growing communities in West Africa (en.m.wikipedia.org).

Since the year 2000, the “spill-over effect” of the growing population of the Accra-Tema Metropolitan Area on smaller towns around the edges has contributed greatly to the rapid increase in the population of the Kasoa Township. The challenges associated with living in Accra, including transportation and affordable housing, have influenced some individuals working to relocate to Kasoa and other nearby communities, thus compounding the population growth of Kasoa.

Kasoa's market is among the biggest markets in the Central Region. Mobile money usage by small, micro and medium scale enterprises and individuals in the Kasoa Township has really contributed to the growth of businesses such as sales transaction, efficiency in purchase of stocks, receipts of and payments for goods and services, savings and money transfer. In a report by B&FT online (thebftonline.com, 2020), it described Kasoa as a remittance epicentre adding that, over the last two years, the remittance transactions to the Kasoa Township and its environs annually was 200,000. The location of the Kasoa Township in the map of the Awutu-Senya East Municipality is shown in Figure 1.

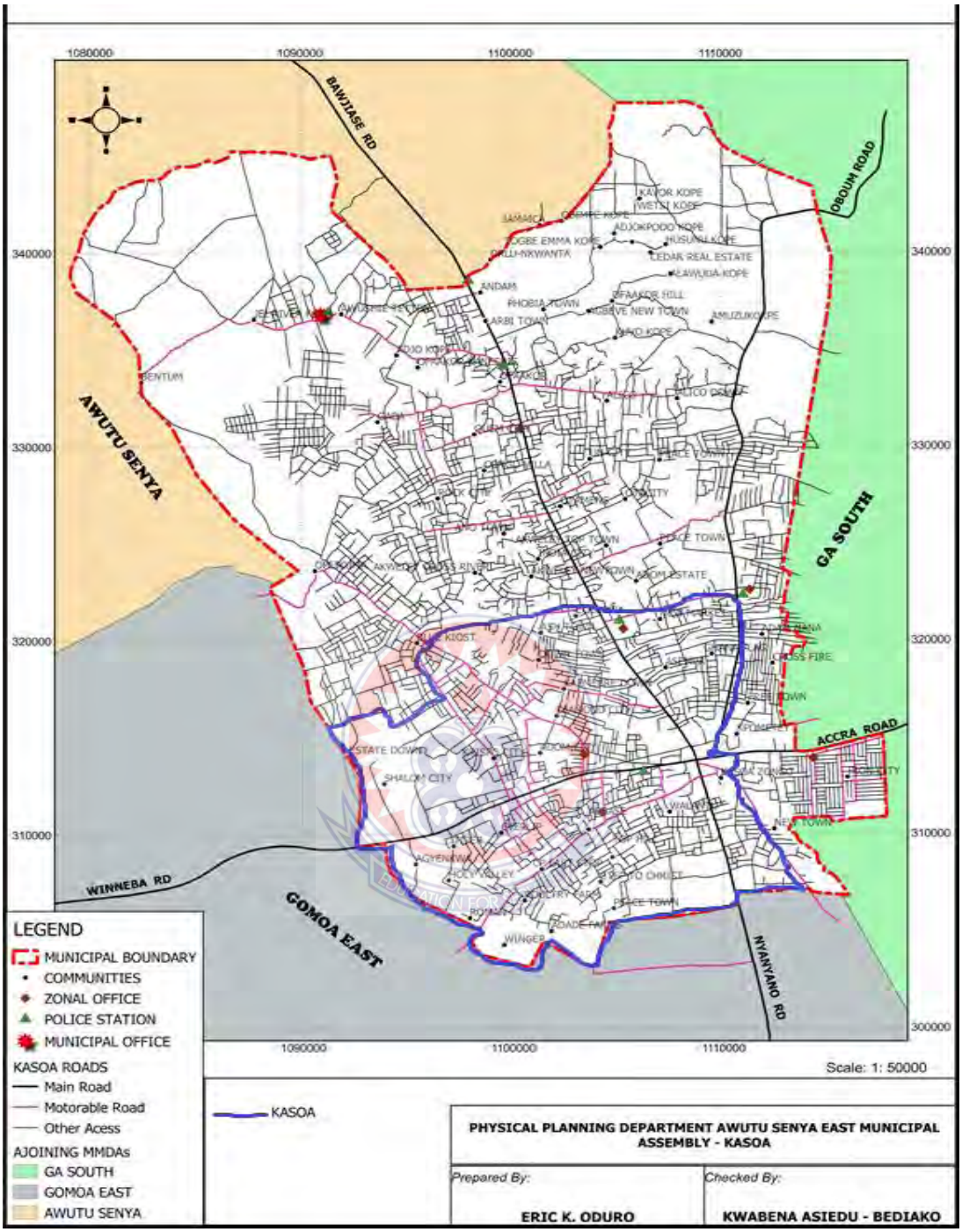


Fig. 1: The Map of the Awutu Senya East Municipality showing the Kasoa Township
Source: Awutu Senya East Municipal Assembly

3.6 Population

Asamoah-Gyimah and Duodu (2007) assert that, population is a group of elements or cases, whether individuals, objects, or events, that conform to specific criteria and to which a researcher intends to generalise the results of the research. O'Leary (2004) opines that, population is the total membership of a defined class of people, objects, or events. The population for this study comprised all persons who have subscribed to mobile money services (Mtn mobile money, Vodafone Cash and AirtelTigo Cash) and mobile money agents in the Kasoa Township.

3.7 The Sample

Sampling is very important in research because, working with the whole population is difficult, if not impossible in the research process due to time and resource constraints (Creswell, 2014). The researcher used Yamane's method of calculating sample size which was formulated by the statistician, Taro Yamane in 1967, to determine the sample size from a given population. Below is the mathematical illustration of Taro Yamane's sample determination:

$$n = \frac{N}{(1 + N\,(e)^2)}$$

Where:

n = Sample size

N = The population under study who are mobile money subscribers

e = the margin of error (it could be 0.10, 0.05 or 0.01)

The population of persons of 18 yrs and above in the Kasoa Township = 36,433

According to the 2021 population and housing census, 68% of the 18yrs and above population have subscribed to mobile money service.

Therefore, $N = \frac{36,433}{100} \times 68.9$

Population of 18yrs and above who have subscribed to mobile money service = 25,102

With the margin of error for this study, the researcher considered 0.05.

Hence: $n = \frac{25,102}{(1+ 25,102\ (0.05)^2)}$

$n = \frac{25,102}{(1+ 25,102\ (0.0025)}$

$n = \frac{25,102}{1+ 62.755}$

$n = \frac{25,102}{63.755}$

$n = 393.73$

n is, therefore, = 394

3.8 Sampling Procedure

For this research, the population of interest included individual mobile money subscribers and mobile money merchants/agents. The respondents for the research were sampled using the stratified sampling and purposive sampling methods. According to Cohen, Manion and Morrison (2003), with purposive sampling, the researcher handpicks the cases to be included in the sample on the basis of their judgments of their typicality. In

this way, the researcher selected a sample that is satisfactory to his or her specific needs. For this study, the researcher sampled 394 participants, made up of mobile money subscribers and mobile money merchants also known as agents. The researcher divided Kasoa into two, using Accra-Winneba main road. So the researcher selected respondents from each division and in this way there was a fair representation of the town.

In order to reduce the bias for the Third World economies, various modifications of the Kish grid were developed. The International Labour Organisation (ILO) modified the original Kish Grid to 8-members household and simplified it (Table 1). The first step in this grid is to find out how many people living in the household are eligible to be interviewed, including people who reside there, but are not present when the interviewer visits. The youngest person in the household is listed as number 1, the second youngest is number 2, and so on. The last digit in the household questionnaire number is then recorded. The intersection of the last digit and the number of persons in the household gives the person who is eligible for the interview. For example, if the last digit in the household number is 2 and there are 3 eligible persons in the household, then interview the first eligible person. If the selected respondent is not there then normally a call-back is arranged (International Labour Organisation, 2009).

Table 1: The ILO Modified Kish Grid

Last Digit in the HH Questionnaire Number	Number of Eligible Persons in the Household						
	1 2	**3**	**4**	**5**	**6**	**7**	**8**
1	1 1	1	1	1	1	1	1
2	1 2	1	2	1	2	1	2
3	1 2	3	1	2	3	1	2
4	1 2	3	4	1	2	3	4
5	1 2	3	4	5	3	4	5
6	1 2	3	4	5	6	3	6
7	1 2	3	4	5	6	7	4
8	1 2	3	4	5	6	7	8
9	1 2	3	4	5	6	7	8

Source: ILO Modified Kish Grid

In spite of the modifications, the argument still remains that, the Kish Grid needs to be modified as per the requirements of the target population. Studies in Hungary (Nemeth, 2001) and China (Ping, 2013) have shown that, the Kish grid digresses widely from the domestic population distributions, and hence needs to be used with care.

The ILO Modified Kish Grid was selected because of a strong setback of the original Kish Grid that, it was mainly developed in USA, and Kish (1949) the developer, estimated that only 1% of the households would have more than 5 adult members. This will be problematic in developing countries such as Ghana, and thus needed modification. Apart from it being problematic in usage, resource and other constraints necessitated further modification of the ILO Modified Kish Grid to fit into the study. Hence, the researcher made some adjustment in this procedure, and as such criteria of inclusion was: all persons who were 18 years or above in a dwelling structure, had subscribed or ever subscribed to mobile money services, and were present were all listed starting from the youngest to the eldest in that order, irrespective of their sexes.

The researcher adapted the ILO Modified Kish Grid, and hence, replaced “Last Digit in the Household Questionnaire Number” (First heading) with ‘’Number of Households in the Dwelling Structure’’ and also replaced the ‘’Number of Eligible Persons in the Household’’ (second heading) with “Eligible Persons Present in the Dwelling Structure” as displayed in Table 2 below.

Table 2: The Researcher's Modified ILO Modified Kish Grid

Number of Households in the Dwelling Structure	Eligible Persons Present in the Dwelling Structure							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	1	1	1	1	1	1	1
2	1	2	1	2	1	2	1	2
3	1	2	3	1	2	3	1	2
4	1	2	3	4	1	2	3	4
5	1	2	3	4	5	3	4	5
6	1	2	3	4	5	6	3	6
7	1	2	3	4	5	6	7	4
8	1	2	3	4	5	6	7	8
9	1	2	3	4	5	6	7	8

Source: Field Data, 2021

From the table above, the last digit for 'eligible persons present in the dwelling structure' was 8. This means that, in cases where the total eligible persons present were more than 8, the 8th person is selected after listing names from the youngest to the oldest. This made it easy, simple and helped in facilitating the process of selecting respondents and questionnaire administration as any person selected was available for the study.

3.9 Data Collection Instruments

3.9.1 Questionnaire

According to Creswell (2014), a good research must use a combination of different instruments in data collection. It is against this background that the researcher used a questionnaire and an interview guide to collect data for the study. The questionnaire was in 4 sections. Section A comprised bio data, section B answered research question one (What types of mobile money fraud are prevalent in the Kasoa Township?), section C answered research question two (Which factors promote mobile money fraud in the Kasoa Township?, and section D also answered research question 3 (in what ways do mobile money fraud affects the inhabitants in the Kasoa Township?).

Questionnaire was employed to gather data from respondents for the study. Kusi (2012) maintains that, structured questionnaire contains predetermined standardized items intended to collect statistical data that can be analysed.

3.9.2 Interview Guide

Creswell (2014) defines interview as a face-to-face verbal exchange of information in which one person, the interviewer, attempts to elicit information from the interviewee. Interviewing as a method of data collection is at the heart of a qualitative research.

Similarly, Awoyemi (2002) observes that, the interview method is useful where the educational levels of the respondents are low. Kusi (2012) argues that, this instrument gives the interviewer the opportunity to ask initial questions, followed by probing questions meant to clarify issues raised. The reason of including interview guide was to supplement the quantitative findings to enhance the validity of the result, in order to enhance in-depth understanding of the study variables. Prior to the interview, mobile money agents were briefed on the purpose of the study, and were encouraged to feel free and express themselves. In all, 6 mobile money agents were interviewed.

3.10 Reliability and Validity

According to Bloomberg, Cooper and Schindler (2005), validity is often defined as the extent to which an instrument measures what it intends to measure. Validity of research instrument is an extent to which the requirements of scientific research method have been followed during the process and procedures of generating research findings.

In order to ascertain the validity of the questionnaire, the researcher did face validity where a few individuals in Winneba Township who have subscribed to the mobile money service were asked to respond to the questions. Follow-up questions were then shared to respondents to ascertain from them, the readability, clarity of wording, layout and style, as well as feasibility of the questionnaire. The results showed that, some of the questions (e.g. What type of mobile money fraud do people normally complain about?) did not meet its intended purpose, and therefore, the researcher made some amendments to fit the study.

Pilot and Berck (2004) define reliability as the extent to which the results are consistent over time, if the results of the study can be produced with a similar methodology, the research instrument is considered reliable. The reliability of the questionnaire was ensured through pre-test which was also conducted in the Winneba Township.

3.11 Trustworthiness

In the interview section, the participants were allowed to tell their stories, so the researcher was able to capture their experiences regarding mobile money fraud in the Kasoa Townwship. The researcher ensured trustworthiness of the study by ensuring credibility and dependability.

3.11.1 Credibility

Credibility as an element of trustworthiness rallies the richness of data for the research as well as the quality of data obtained for the study. Yin (2014) stated that, building rapport with participants was one significant commitment of the researcher necessary to collect accurate data to strengthen the credibility of the study. The researcher therefore established credibility through engagement with the six (6) participants during the interview. Additionally, member check was employed to ensure the credibility of the data gathered. Participants interviewed for the study reviewed the data obtained from them. Thus, participants were given the opportunity to verify their statements.

3.11.2 Dependability

Pilot and Beck (2014) contend that, research data is dependable when such data retained its value in comparable setting. This is measured by the standard of which the research is conducted, analysed and presented.

The researcher ensured dependability in the study by reporting in detail, each process to enable a researcher who may repeat the inquiry achieve the same results. Additionally, rules and principles regarding methods of collecting data were adhered to. Thus, similar results would come out if same study is repeated with the same methods of instruments.

3.12 Data Collection Procedure

In conducting a study, Creswell (2005) advises researchers to seek and obtain permission from the authorities in charge of the site of the study because it involves a prolonged and extensive data collection. In line with this, an introductory letter was obtained from the Head, Department of Social Studies Education, University of Education, Winneba. The researcher then divided the Kasoa Township into two divisions, for a fair representation of the town, briefed the researcher's team on the sampling procedures and strict adherence to ethical issues. A copy of the introductory letter was given to one of the Assembly members in each division for approval to conduct the study and also introduced the researcher's team of four persons, including the researcher to them. Upon granting permission, the researcher and his team placed themselves in one division of the town to administer 197 questionnaires and repeated same in the other division of the town. Each team member located a landmark that could easily be identified such as a Mosque, church building or a school and moved towards the right hand side towards dwelling structures. On the right side of the landmark, every first dwelling structure was selected after which, every other tenth dwelling structure was included. Participants were sampled first taking into accounts the criteria of inclusion and the presence of respondents. With the exception of those who could not read and answer the

questionnaire, all others filled the questionnaires themselves. To ensure there was no back lack, the researcher made sure to replace unanswered questionnaires.

The administration of interviews was solely done by the researcher. Mobile money agents were purposively sampled for the interview. All protocols regarding ethical issues were observed as the researcher made sure that, permission was sought from both superiors of the agents and agents also consented to be interviewed. Although the researcher reached a saturation point after interviewing the fifth mobile money agent, the six agent was interviewed anyway.

3.13 Data Analysis Methods

Creswell (2014) explains data analysis in research as preparing and organising the data for analysis, reducing data into themes through a process of coding and condensing the codes. The data collected for this study was put into tables of frequency counts and percentages and interpreted in line with the research questions. The data collected for the quantitative study was coded and analysed using SPSS version 21. In all, 388 questionnaires were answered and 6 agents interviewed, and used for the analysis. The data gathered for the qualitative study was analysed through content analysis, and was further transcribed into themes for analysis. Patton (2002) validates this process by saying that content analysis is the process of discovering themes, patterns and categories in a collected data. The qualitative data (interview) was transcribed and used to support the quantitative data.

3.14 Ethical Consideration

According to Alhassan (2006), ethical issues of anonymity, confidentiality and privacy are, particularly relevant in ensuring that researchers' ethical obligations to their respondents were not violated during data collection. Based on the above assertion, all the ethical considerations were observed during the study.

Firstly, participants were informed of the purpose of the study and were asked to give their consent before the study was carried out, and hence no one was coerced into participating in the study. Also, the researcher ensured participants' anonymity by not disclosing their identity after information is gathered. Finally, information provided was treated with utmost confidentiality.

3.15 Chapter Summary

This chapter described in detail, the methodology used to conduct the study. The research approach adopted was the mixed method, where both quantitative and qualitative data was collected. The population for the study was mobile money subscribers and agents in the Kasoa Township out of which 394 respondents were sampled and used for the study. Using the stratified and purposive sampling techniques, a questionnaire and an interview guide were used to collect data from respondents whiles putting in place the necessary measures to address issues of privacy and confidentiality.

CHAPTER FOUR

FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents the findings and discussions of the study. The demographic information of respondents is first presented, followed by the data analysis based on the research questions.

4.2 Demographic Characteristics of Respondents

The study sampled 394 respondents of mobile money subscribers who were 18 years and above in the Kasoa Township. A questionnaire was administered to 394 mobile money subscribers and mobile money agents and 6 agents were interviewed for data collection. Out of this, the researcher was able to interview all 6 agents and retrieved all 394 questionnaires. Therefore, the analysed results are based on the responses received from the 394 mobile money subscribers and mobile money agents as well as 6 agents interviewed in the Kasoa Township. The responses from the questionnaire were made up of 208 (52.8%) males and 186 (47.2%) females. Table 3 illustrates the above information.

Table 3: Sex Distribution of Respondents

Sex	**Frequency**	**%**
Male	208	52.8
Female	186	47.2
Total	**394**	**100**

Source: Field Data, 2021

Table 4 below shows that, those between the ages of 18 and 29 years constituted the highest respondents, recording 191 (48.5%) of the total respondents. Those between 30

and 39 years were 118 (29.9%) respondents, followed by 40-49 years, recording 54 (13.7%), while 50-59 years were 14 (3.5%), and 60 years above were 17 (4.3%). Table 4 below shows the age distribution of respondents for the study.

Table 4: Age of Respondents

Age range	**Frequency**	**%**
18-29	191	48.5
30-39	118	29.9
40-49	54	13.7
50-59	14	3.5
60+	17	4.3
Total	**394**	**100**

Source: Field Data, 2021

Table 5 below shows the educational qualifications of the respondents. In Table 5, out of 394 respondents, 148 (37.6%) were university graduates. Respondents who had Diploma certificate were 52 (13.2%), SHS graduates were 108 (27.4%), 56 (14.2%) had completed Basic Education, while respondents in the category of Informal Education were 30 (7.6%).

Table 5: Educational qualifications of respondents

Qualification	**Frequency**	**%**
Informal	30	7.6
Basic	56	14.2
SHS	108	27.4
Diploma	52	13.2
Degree	148	37.6
Total	**394**	**100**

Source: Field Data, 2021

The researcher also sought to determine the mobile money operator services that had most subscriptions and the responses are presented in Table 6.

Table 6: Mobile money operator services respondents use most

Operator	**Frequency**	**%**
AirtelTigo Money	13	3.3
MTN Momo	284	72.1
Vodafone Cash	97	24.6
Total	**394**	**100**

Source: Field Data, 2021

Table 6 shows that, MTN had the highest money operator services with 290 (72.1%) of the respondents. This was followed by Vodafone Cash which had 91 (24.6%) respondents while 13 (3.3%) respondents identified AirtelTigo Money as their main mobile money service provider.

The study further found other mobile money operator subscription by respondents, apart from their main mobile money service provider and this is captured in Table 7 below.

Table 7: Other mobile money operator services respondents use

Operator	**Frequency**	**%**
AirtelTigo Money only	63	16.0
MTN Momo only	27	6.9
Vodafone Cash only	130	33.0
AirtelTigo Money and Vodafone Cash only	54	14.0
MTN Momo and Vodafone Cash only	58	15.0
None	62	16.0
Total	**394**	**100**

Source: Field Data, 2021

In Table 7, 63 (16.0%) respondents stated that, apart from their main mobile money service provider subscription, they subscribed to AitelTigo Money, 27 (6.9%) respondents said they subscribed to MTN Momo, 130 (33.0%) respondents said they had in addition subscribed to Vodafone Cash, 54 (14.0%) respondents in addition use AirtelTigo Money and Vodafone Cash, 58 (15.0%) of the respondents said they use MTN Momo and Vodafone Cash while respondents who had no additional subscription were 62 (16.0%).

Respondents were also asked about how they had subscribed to mobile money services and their responses are presented in Table 8.

Table 8: How long respondents have been accessing mobile money services using their phones

Length (in years)	**Frequency**	**%**
1-3 years	15	3.8
4-6 years	88	22.0
7-9 years	194	49.2
More than 10 years	97	25.0
Total	**394**	**100**

Source: Field Data, 2021

Table 8 illustrates the length of time respondents had subscribed to mobile money services.. Out of 369 respondents, 15 (3.9%) mentioned 1-3 years of subscription, 88 (22.0%) said that, they had used the mobile money services between 4-6 years, 194 (49.2%) also said that, they had subscribed to the service between 7-9 years, and 97 (25%) of respondents had more than 10 years of subscription to mobile money services.

4.3 Presentation of Findings and Discussion

4.3.1 Research Question One

What types of mobile money fraud are prevalent in the Kasoa Township?

To answer research question one, the researcher, first of all, determined if respondents had ever received mobile money fraud attempts on their phones, and their responses are presented in Table 9.

Table 9: Whether or not respondents had received mobile money fraud attempts on their phones

Response	**Frequency**	**%**
Yes	385	97.7
No	9	2.3
Total	**394**	**100**

Source: Field Data, 2021

In Table 9, 385 (97.7%) respondents said that, they had received mobile money fraud attempts on their phones while 9 (2.3%) of the respondents said that they had not yet received mobile money fraud attempts on their phones. The respondents who said 'Yes' to receiving mobile money fraud attempts were asked of the frequency of the attempts, and the results are presented in Table 10.

Table 10: Frequency of mobile money fraud attempts received

Mobile money fraud attempts	**Frequency**	**%**
Less than 5 times weekly	28	7.3
Less than 5 times Monthly	240	62.3
Less than 5 times Quarterly	47	12.2
5-9 times Quarterly	34	8.8
10-14 times Quarterly	21	5.5
15-19 times Yearly	15	3.9
Total	**385**	**100**

Source: Field Data, 2021

In Table 10 above, the question about the frequency of mobile money fraud attempts had varying responses where the majority of the respondents, 28 (7.3), mentioned less than 5 times a week, 240 (62.3%) also mentioned less than 5 times a month, 47 (12.2%) said less than 5 times quarterly, 34 (8.8%) responded 5-9 times quarterly, 21 (5.5%) said 10-14 times quarterly while 15 (3.9%) said that, they received 15-19 times of mobile money fraud attempts a year. In addition, respondents were questioned on the category of mobile money fraud attempts they received, and their responses are shown in Table 11.

Table 11: Category of attempts received

Category	**Frequency**	**%**
Text messages only	51	13.2
Voice calls only	86	22.4
Both text and voice calls	248	64.4
Total	**385**	**100**

Source: Field Data, 2021

Table 11 shows that, 51 (13.2%) respondents receiving mobile money fraud attempts via text message, 86 (22.4%) said that they mostly received mobile money fraud attempts via voice calls, while 248 (64.4%) received mobile money fraud attempts via text messages and voice calls. Table 11, thus shows that, most mobile money subscribers received mobile money fraud attempts through both text messages and voice calls.

To ascertain the type of mobile money fraud in the Kasoa Township, respondents were asked about the mobile money fraud types they mostly experienced, and the responses are shown in Table 12.

Table 12: Mobile money fraud type mostly experienced by respondents

Fraud	**Frequency**	**%**
Scam messages	84	21.8
Emotional scam	6	1.6
Anonymous calls	168	43.6
Cash-out fraud	18	4.7
False promotion	61	15.8
Fortuitous scam (Goods from abroad)	45	11.7
MNO fraud	3	0.8
Total	**385**	**100**

Source: Field Data, 2021

In Table 12, out of 379 respondents, 84 (21.8%) stated that scam messages were the most mobile money fraud they had experienced, 6 (1.6%) mentioned emotional scam, 168 (43.6%) mentioned anonymous calls, 18 (4.7%) identified cash-out fraud, 61 (15.8%) mentioned false promotion, 45 (11.7%) mentioned fortuitous scam and 3 (0.8%) identified Mobile Network Operator (MNO) fraud. Although the responses from respondents supported Annan (2018) and Ayettey's (2019) list on the types of mobile money fraud being scam messages/reversal of erroneous transfer, emotional scam, anonymous calls from fraudsters, cash-out fraud, vender pin fraud, false promotion, fortuitous scam and MNO fraud, the study revealed that, anonymous calls from fraudsters was the most common type of mobile money fraud in the Kasoa Township, with 168 (43.6%) respondents. This is about a half of the total respondents involved in the study followed by scam messages with 84 (21.8%) while Mobile Network Operator fraud had

the least responses of 3 (0.8%) respondents. In furtherance, this results is in line with the study by Arhin (2018) which revealed that, anonymous call is the most common mobile money fraud type.

The researcher also determined whether or not respondents had ever been defrauded through mobile money, and their responses are presented in Table 13.

Table 13: Whether or not respondents had been defrauded through mobile money

Response	**Frequency**	**%**
Yes	154	39.0
No	240	61.0
Total	**394**	**100**

Source: Field Data, 2021

Table 13 shows respondents' responses as to whether they had ever been defrauded through mobile money. In response to this question, 154 (39.0%) said, 'Yes' they had ever been defrauded through mobile money, while 240 (61.0%) answered no.

Moreover, the researcher sought from respondents who answered yes in Table 13, the details of their experience (evidence of mobile money fraud). Their reasons are presented in Table 14.

Table 14: Respondents' mobile money fraud experience (evidence of mobile money fraud)

No. of respondents	Total amt. of money involved (range) Gh₵	Type (s) of momo fraud	No. of times defrauded	%
15	700-2000	Anonymous calls	1	11.0
33	2500-3500	False promotion & Anonymous calls	3	21.4
12	700-1500	Anonymous calls & Fortuitous scam	2	7.8
20	200-700	Emotional scam & Cash-out fraud	1	13.0
10	50-200	Scam messages & false promotion	3	6.5
8	20-200	False promotion & Anonymous calls	2	5.2
23	1500-2500	Anonymous calls, Cash-out fraud & MNO fraud	2	15.0
14	3500-5000	Scam messages & Anonymous calls	2	9.1
13	200-700	Scam messages	2	8.4
6	50-200	False promotion & Anonymous calls	1	3.9
154				**100**

Source: Field Data, 2021

Table 14 illustrates cases of mobile money fraud in the Kasoa Township. It shows the number of times respondents had been defrauded, total amount of money involved and the type (s) of mobile money fraud that the fraudster used. In the Table 14, (11.0%) respondents out of 154 had been defrauded once, and lost between Gh700-Gh 2000 through anonymous calls, 33 (21.4%) respondents mentioned that, they had been

defrauded 3 times, and had lost between Gh2500-Gh3500 through false promotion and anonymous calls, 12 (7.8%) said that, they had been defrauded 2 times and the total amount lost was between Gh700-Gh1500 through anonymous calls and fortuitous scam, 20 (13.0%) of the respondents said that, they had been defrauded once and lost between Gh200-Gh700 through emotional scam and cash-out fraud. In addition, 10 (6.5%) respondents disclosed that, they had been defrauded 3 times, and lost between Gh50-Gh200 through scam messages and false promotion, 8 (5.2%) respondents commented that, they had been defrauded 2 times, and lost between Gh20-Gh200 through false promotion and anonymous calls, 23 (15.0%) said that, they had been defrauded 2 times, and lost between Gh1500-Gh2500 through anonymous calls, cash-out fraud and MNO fraud, 14 (9.1%) disclosed that, they had been defrauded 2 times, and lost between Gh3500-Gh5000 through scam messages and anonymous calls, 13 (8.4%) said that, they had also been defrauded 2 times, and lost between Gh200-Gh700 through scam messages and 6 (3.9%) said that, they had also been defrauded once, and lost between Gh50-Gh500 through false promotion and anonymous calls.

The outcome of Arhin' (2018) study which revealed that, victims lost between Gh200-Gh3,500 is in line with this results.

4.3.2 Research Question Two

What factors promote mobile money fraud in the Kasoa Township?

The researcher sought from the respondents who answered yes in Table 13, why they were defrauded and the reasons are presented in Table 15.

Table 15: Reasons for being a victim

Reason	Frequency	Percentage
I was afraid of being blocked.	13	8.4
My Momo account was hacked.	10	6.5
I trusted the fraudster.	42	27.3
I had pity on the fraudster after listening to his story.	11	7.1
I was unaware of fake promotions.	16	10.4
The fraudster built rapport with me.	31	20.1
I had no ICT knowledge.	9	5.8
I tolerated the fraudster.	22	14.4
Total	**154**	**100**

Source: Field Data, 2021

Table 15 shows why respondents were defrauded successfully. Out of 154 respondents, 13 (8.4%) mentioned that, they were afraid of being blocked, 10 (6.5%) said that, their mobile money account was hacked, 42 (27.3%) said that, they trusted the fraudster, 11 (7.1%) said that, they had pity on the fraudster after listening to his story, 16 (10.4%) said that, they were unaware of fake promotions, 31 (20.1%) said that, the fraudster built rapport with them, 9 (5.8%) said they had no ICT knowledge and 22 (14.4%) said that, they tolerated fraudsters leading to their being defrauded. This implies that majority of mobile money subscribers became mobile money fraud victims by first tolerating them leading to building rapport and eventually end in trust where fraudsters succeed in defrauding them. This confirms Cross' (2018) assertion that, the use of authority to gain trust and compliance is a common place.

Respondents who responded 'No, if they had been defrauded before were also asked to provide their reasons and their responses are shown in Table 16.

Table 16: Reasons for unsuccessful attempt

Reason	**Frequency**	**%**
I was aware of fraudulent messages and calls.	125	52.1
I did not tolerate/entertain unknown contacts.	22	9.2
I had technical knowledge in ICT.	6	2.5
I was prompted by a third party.	58	24.2
I had no money in my momo account.	19	7.9
I verified from MNO/ Service Providers.	10	4.2
Total	**240**	**100**

Source: Field Data, 2021

Table 16 shows that, out of 240 respondents, 125 (52.1%) said that they were aware of the fraudulent tricks used by these fraudsters, 22 (9.2%) opined that they did not tolerate calls and text messages from unknown numbers, 6 (2.5%) said that they had technical knowledge in ICT, and that led to their rescue, 58 (24.2%) contended that, they were prompted by a third party leading to their rescue, 19 (7.9%) said that they had no money in their mobile money account/wallet and 10 (4.2%) maintained that, they verified calls or messages from Mobile Network Operator (MNO)/service providers.

Also, the researcher sought to determine which factor of fraud led to mobile money fraud and the responses are captured in Table 17.

Table 17: Factors leading to mobile money fraud

Factor	**Frequency**	**%**
Motive/Pressure	181	46.0
Opportunities	110	28.0
Rationalisation of Crime	17	4.3
Capabilities/skills/abilities of the fraudster	86	21.7
Other	0	0
Total	**394**	**100**

Source: Field Data, 2021

In Table 17, 181 (46.0%) respondents identified motive/pressure as cause of mobile money fraud, 110 (28.0%) mentioned that opportunities as a factor, 17 (4.3%) mentioned rationalisation of crime is a factor, while 86 (21.7%) identified capabilities/abilities of the fraudster as also a factor leading to mobile money fraud. Thus, respondents were in agreement with the fraud triangle, but with a fourth component being capabilities/ abilities of the fraudster as opined by Wolfe and Hermanson (2004) that, a fraudster must be capable of successfully deceiving the other party in an exchange.

All six agents who were interviewed also supported this assertion. Some of their excerpts are shown below.

> These fraudsters are very brilliant, and as a matter of fact, they really know what they are about. So even before they call you, they have really rehearsed, and in addition have a coach sitting beside to assist when victims seem to be difficult. They will mention your name and say he/ she is speaking from one of the Mobile Network Operator's Office. This way, the victim knows it is authentic and gives every information he/she requests for. Their personal capabilities are really helping to succeed in this activity. (A participant disclosed)

> Most of these fraudsters are already criminals and so the will power is available and they just need to locate the loop whole in the system to act. This is because it takes some personal abilities and experiences for a fraudster to tell you that, you have won a promotion and that he/she needs you to generate the promotion code which will enable you go for your reward. This way, the victim's mind is taken off and the fraudster begins the process. So you see, whenever you are told you have won a promotion, you are very happy to cooperate with authorities in order to get your reward. (A participant said)

From the way they attack us, they are been let by greed, their personal abilities and weak control system in the momo industry. (A participant contended)

> Some fraudsters are very technically good with regard to ICT, and so they hack your account first, send you a message and immediately the victim logs into his mobile money account to check his/her balance, the fraudster will then cash out money from the account. This is technical and I do not know how it happens. (A respondent said)

> Although fraudsters have their own capabilities, I would also say that poor remuneration of employees contribute to fraud. Some subscribers, instead of coming in person to cash-out or withdraw money, they will either send a friend, child, spouse or a relative, and many at times, write the mobile money pin on a paper to be used by the sender for the cash-out. When a fraudulent merchant gets hold of this pin, he/ she can order cash out from the account. (A respondent commented)

> In my view, fraudsters may be pressured by negative influences, possess a set of skills that fuel their activities and may even have an insider to help him/her to succeed. Some employees of merchants also undertake fraudulent activities using written records of subscribers in their books. Other times, they leak this information to their counterparts to defraud subscribers. In our case as agents, we normally give the phone to subscribers to enter their phone numbers when undertaking a transaction and fraudulent subscribers defraud agents as well. We usually do this mainly based on trust. (A respondent maintained)

These responses confirm the results from respondents who answered the questionnaires. Also, some of these explanations are in line with Cross' (2018) assertion on how to get away with fraud. Cross (2018) said that, in many cases, it is a culmination of efforts that result in the victim sending money or complying with a fraudster's request. Some fraudsters target specific victims and build a profile of them through online or offline tracking. This was grouped under what Cross referred to as Grooming the victim. In addition, the contact may start as random, but the fraudster will work hard to establish trust and build rapport. Several fraud victims interviewed in Cross' study said that, they saved all their chat logs with their offenders from the first contact and re-reading these conversations allows them to feel a deeper connection to the words and the person sending them, compared to a verbal conversation (Cross, 2018). Also, the use of authority to gain trust and compliance is a common place. Offenders take on the identity of a person or organisation, and use this to threaten victims into submitting to their requests, thus fear can be a strong motivating factor. These messages say there is a problem and threaten a negative consequence (such as the closure or freezing of an account) if victims do not compromise (Cross, 2018). These are all underpinned by personal skills of the fraudster. These skills or abilities could be innate or learnt.

From the responses above, it could be confirmed that, a fraudster must possess a set of capabilities that fits the requirements needed to successfully defraud a victim. Fraudsters and social engineers use their abilities to influence others and develop a false sense of trust in others, in order to gain some advantage (Ramamoorti, 2008).

4.3.3 Research Question Three

In what ways do mobile money fraud affects the inhabitants of Kasoa Township?

The study sought to explore how mobile money fraud affected the inhabitants of the Kasoa Township and the responses are contained in Table 18.

Table 18: Ways in which mobile money fraud affects the inhabitants of Kasoa Township

EFFECT	**FREQUENCY**	**%**
Mental and Physical Trauma	29	7.4
A threat to business survival	56	14.2
Destroys business relationships	41	10.4
Loss of customer trust	117	29.6
Erosion of business trust	100	25.4
Increases vulnerability	24	6.1
Discourages investors	27	6.9
Total	**394**	**100**

Source: Field Data, 2021

Table 18 provides respondents views on ways mobile money fraud affected the inhabitants of the Kasoa Township. In the table, 29 (7.4%) respondents identified mental and physical trauma as one of the ways mobile money fraud affected the Kasoa

inhabitants, 56 (14.2%) said that, it threatened business survival, 41 (10.4%) mentioned that, it destroyed business relationships, 117 (29.7%) mentioned loss of customer trust, 100 (25.4%) said that, it eroded business trust, 24 (6.1%) said that, it increased vulnerability and 27 (6.9%) said it discouraged investors from investing in Kasoa. In Table 17 above, respondents provided some other ways mobile money fraud affected them and this is evident that those outlined by the International Public Sector Fraud Forum (2019) and Common Wealth Fraud Prevention (2020) mainly deliberated on how mobile money fraud affects governments and or a nation (s) as a whole. However, most of their outlined impacts were maintained by respondents. For example the International Public Sector Fraud Forum, (2013) gave deeper explanations to that of Common Wealth Fraud Prevention on Industry impacts. In its view, the erosion of trust in industry as an impact of fraud can result in not only a loss to government, but can also have negative impacts on industry.

On ways in which mobile money fraud affected them, respondents gave divergent views, but there were some that run through all their responses. These are some of their responses:

> Mobile money fraud, first and foremost, makes people lose trust in the mobile money business, most especially those who have been victims more than ones, and also end people in emotional conditions. This, in the long run, puts fear in people when engaging in business transactions in the Kasoa Township. It also shows how weak our cyber security system is. (A respondent said)

One respondent also retorted, “Yes at times, these fraudsters use foreign numbers to call and start business conversations, which turn out to be fraudulent”. This act in turn

destroys business relationships in the Kasoa Township. (A respondent commented). A respondent also commented:

> Loss of customer trust is very obvious, people's businesses struggle or even collapses as a result of mobile money fraud because, it might be that money on the wallet was going to be used to pay his/her workers or utilities, but interrupted by fraudsters. It also results in people losing trust in even engaging in a business because they tried and have been defrauded.

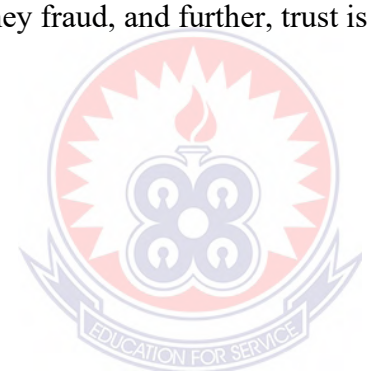
> Mobile money fraud has discouraged people from saving their money on their wallets and thereby exposing such people to robbery. It also puts people in mental and or physical trauma. Mobile Network Operators (MNO's) also lose in the sense that they trade with what is deposited in their wallets to also gain some interest on them. Activities of these fraudsters distort the market and people eventually loss confident in the system because they doubt how secure it is. (A respondent maintained)

Responses from respondents interviewed confirm results from the questionnaires in that, all the respondents interviewed made mention of how inhabitants were affected by mobile money fraud including loss of trust, loss of business trust and confidence, destroying business and customer relations, a reduction in investment and emotional trauma. From the literature review, as the International Public Sector Fraud Forum report, (2019) report and the Commonwealth Fraud Prevention Centre (2020), Texas Identity Theft Coalition (2010b); FTC (2017f) and Freshman, (2012), all agreed that, fraud has affected individuals and the community as a whole.

4.5 Chapter Summary

The chapter presented the findings and discussion of the data collected for the study based on the research questions. Descriptive statistics were used for the analysis. Qualitative analysis was used to support the quantitative analysis. The study revealed that, the majority of Kasoa residents subscribed to MTN mobile money, with Vodafone

cash being the other mobile money operator services mostly used. Most mobile money subscribers signed up mobile money between 2014 and 2016, that is, 4 to 6 years after it was introduced in Ghana. Almost all respondents have ever received mobile money fraud attempts and these attempts are in both voice calls and text messages, but anonymous calls is the most prevalent type of momo fraud. Majority of Kasoa residents receive mobile money attempts almost every week. About one third of the respondents have been successfully defrauded. The study also brought to light that, trust and awareness contributed to either a successful or unsuccessful mobile money fraud attempts, motive, opportunities, rationalisation and capabilities of the fraudster were the factors that contributed to mobile money fraud, and further, trust is lost when people are defrauded.



CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter summarises the research. It presents the summary of the findings, conclusions and the recommendations made.

5.2 Summary

The objectives for the study were to:

(i) identify the type of mobile money fraud that are prevalent in the Kasoa Township.

(ii) determine the factors that promote mobile money fraud in the Kasoa Township.

(iii) explore the effects of mobile money fraud on the Kasoa Township.

The study explored mobile money fraud in the Kasoa Township. With the use of the stratified and purposive sampling technique, a sample size of 394, made up of mobile money subscribers and merchants/agents were selected for the study. The researcher used a questionnaire and an interview guide for data collection. Data was analysed using frequency counts and percentages.

The major findings of this study include the following:

1. The study found that, anonymous call from fraudsters is the most prevalent type of mobile money fraud. Also, most mobile money fraud come in both calls and text messages and irrespective of one's educational background, one can be a victim of mobile money fraud since majority of the respondents were university

graduates, It was also realised that no matter the numbers of years of mobile money usage, one is eligible to be a victim of mobile money fraud.

2. The study found that, motive/pressure, opportunities, capabilities and rationalisation of crime are factors that promote mobile money fraud. Tolerance is one major habit of mobile money fraud victims where the fraudsters build rapport with them, and end up trusting them because, usually fraudsters come in the name of MNO/ Service Provider. However, more than half of the respondents who could not be defrauded gave credit to awareness.

3. The study found that, there are a number of effects of mobile money fraud on mobile money operations such as loss of customer and business trust, destroying business relationships, clean-up cost, collapse of business, market distortion. However, since trust was the main basis for defrauding victims, the same trust is lost by customers and erosion of business trust when victims are defrauded.

5.4 Conclusions

Based on the findings, the following conclusions are made:

Anonymous call is the most prevalent mobile money fraud type that the people of Kasoa experience. Motive/pressure, opportunities, capabilities and rationalisation of crime are factors that promote mobile money fraud and they thrive on trust. Mobile money fraud has a number of effects on the inhabitants of Kasoa Township, most of which has to do with loss of trust, especially customer trust. From the above, it could be realized that fraudsters combine motive/pressure such as greed etc, opportunities in the system coupled with their personal abilities/ capabilities after which they justify their actions (rationalisation) to embark on mobile money fraud. Fraudsters usually attack mobile

money customers through anonymous calls, aim at building trust to defraud, and victims have lost trust (customer and business trust).

5.5 Recommendations

On the basis of the findings and the conclusions, the following recommendations are made:

1. Both merchants and individual subscribers in Kasoa are encouraged to save the contacts of their Mobile Network Operator on their phones in order to detect fake calls claiming to have come from the Mobile Network Operator's Office to help curb anonymous call related fraud.

2. Mobile money operators/service providers need to intensify awareness creation or sensitisation of mobile money fraud, by using the local languages such as Fante, Ewe, Nzema, Hausa and Ga, with the help of the local information centres in the Kasoa Township.

3. The Police, in collaboration with Mobile Network Operators/Mobile Money Service providers in Kasoa, should publish the names and pictures of fraudsters anytime they are arrested to deter others from engaging in such activities in order to build trust in Kasoa inhabitants.

4. There is the need for the government to support the Ghana Police Service to establish the Cyber Crime Unit at Kasoa to combat mobile money fraud to build trust in the system.

5. The Police should support more police officers in the Kasoa Municipality to study Cyber Crime/Security, by giving them scholarships and study leave, to equip

themselves with the requisite knowledge and skills to enable them to effectively deal with momo fraud.

6. The Ghana Police Service in conjunction with the mobile network operators/service providers and the Awutu Senya East Municipal Assembly must organise workshops and seminars for all mobile money merchants/agents operating in the Kasoa Township to acquire the requisite knowledge, skills and experiences for the mobile money business.

5.6 Suggestions for further studies

It is suggested that, similar studies on mobile money fraud should be conducted in commercial towns in other regions using large sample size since this study and others were done in the Central Region with small sample size. Moreover, other studies should also focus more on mobile money fraudsters using qualitative approach to further come out with detailed explanations.

REFERENCES

AARP Foundation. (2003). Off the Hook: reducing participation in telemarketing Fraud. Retrieved Jun 2019 from https://assets. aarp.org/rgcenter/consume/d17812_fraud.pdf

Abdullahi, R. & Mansor, N. (2015). Forensic Accounting and Fraud Risk Factors: The influence of fraud diamond theory. *The American Journal of Innovative Research and Applied Sciences*, 1(5):186-192.

Acquah, P. A. (2006). Evaluating the banking system in Ghana. Fifth Banking Awards Ceremony, Accra, 6 May 2006.

Afanu, K. E & Mamattah, S. R. (2013). Mobile money security: A holistic approach. Mobile Money security –A Holistic Approach.

Afful, E. K. & Sellappan Palaniappan
Article: 2138105 | Received 29 Aug 2022, Accepted 17 Oct 2022, Published online: 27 Oct 2022 https://doi.org/10.1080/23311886.2022.2138105

Ajzen, I. (1991), "The theory of planned behaviour," *Organisational behaviour and human decision processes*, vol. 50, no. 2, 1, pp. 179-211.

Akoh, B. (2001). E-Business in the development world: Africa and Ethiopia

Akomea-Frimpong, I. (2017), "How mobile money operators can minimize fraud", available at:http://gheconomy.com/mobile-money-operators-can-minimize-fraud/ (accessed 7 May 2017).

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., & Dwomoh-Okudzeto, Y. (2019)."Control of Fraud On Mobile Money Services In Ghana: An Exploratory Study," *Journal of Money Laundering Control* 22, no. 2 (2019): 301.

Albrecht, W. S., Romney, M., Cherrington D., Payne I., & Roe A., (1982). How to detect and prevent business fraud, *Englewood Cliffs, NJ: Prentice-Hall*.

Albrech, W. S. T., Albrecht, C. C., Albrecht, C., & Zimbelman M. (2009*). Fraud examination*, *3rd ed. Mason, OH: South-Western Cengage* Learning.

Alhassan, S. (2006). Modern approaches to research in educational administration for Research students. Kumasi: *Payless Publication Ltd*.

Alise, M. A., & Teddlie ,C. (2010). A continuation of te paradigm wars? Prevalence rates of methodological approaches across the social/behavioural sciences. *Journal of Mixed Methods Research,* 4(2), 103-126. https://doi.org/10.1177/1558689809360805

Angelakopoulos, G. & Mihiotis, A. (2011). 'E-banking: Challenges and opportunities in the greek banking sector', *Electronic Commerce Research,* 11(3), pp. 297-319.

Applegate, L. M. et al. (1996). Electronic commerce: Building blocks of new business opportunity", *Journal of Organisational Computing and Electronic commerce*, Vol. 6, No. 1, pp. 1-10

Annan, E. S. (2017). Avoiding fraud due to Momo. theb&ftonline.com

Annan, S. (2017). "Avoiding Fraud Due to Mobile Money," Ghana Web, October 7, 2017.Veronica Owusu Ansah, "MTN Mobile Money Fraud, An Inside Job?" Ghana Web, October 23, 2017, https://www.ghanaweb.com/GhanaHomePage/NewsArchive/MTN-Mobile-Money-fraud-an-inside-job-593205.

Anderson, K. B. (2013). Consumer fraud in the United States, 2011: *The Third FTC Survey*. Retrieved June 2019 from https://www.ftc.gov/sites/default/files/documents/ reports/consumer-fraud-united-states-2011-third-ftcsurvey/130419fraudsurvey_0.pdf

Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T., & Savage, S. (2012). *Measuring the cost of cybercrime. A paper presented at the WEIS Conference,* Berlin.

Anderson, K. B. (2007). Consumer fraud in the United States: The second FTC survey. Retrieved Jun 2019 from https://www. ftc.gov/sites/default/files/documents/reports/consumerfraud-united-states-second-federal-trade-commissionsurvey-staff-report-federal-trade/fraud.pdf

Arhin, S. (2018). The impact of fraud on the financial performance of mobile payment (telecom) companies in Ghana. *International Journal for Social Studies*. ISSN:22455-3220.Vol. 04 Issue 12

Arya, H., (2019). "E-Banking: The Emerging Trend" Published in *International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 Issue-4*, June 2019, pp.449-455, URL: https://www.ijtsrd.com/papers/ijtsrd23689.pdf

Attom, B. E. (2014). "Cash management practices by micro and small-scale enterprises at Kasoa in the Central Region of Ghana". *Asian journal of business management sciences.* Vol. 3. No. 2 (01-12).

Asongu, S. & 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.

Asomoah-Gyimah, K. & Duodu, F. (2007). Introduction to research methods in education. *University of Education, Winneba: Institute of Educational Development and Extension (IEDE).*

Awoyemi, M. O. (2002). Research methodology in education. Winneba: University of Education, Winneba.

Ayettey, T. L. (2019). MOMO fraud – How scammers steal your money. modernghana.com

Ayers, R., Jansen, W., Moenner, L, & Delaitre A (2007), 'NIST Interagency Report (IR) 7387' Cell phone forensic tools: An overview and analysis update, viewed 15 December 2012, http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

Bawumia, M. (2007). Banking in Ghana in the last 50 Years: Challenges and prospects.

Barker, K. J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: Awareness and prevention. *Journal of Financial Crime*, 15(4), 398-410. doi:http://dx.doi.org/10.1108/13590790810907236

Barnes, S. J. & Corbitt, B. J, (2003). Mobile banking: Concept & potential. *Int. J. Mobile Communications, Vol*. X, No. X, xxxx.

Banda, H. (2018). "Ghana's Banking Bust," Africa Report, November 22, 2018. https://www.theafricareport.com/445/ghana-finance-banking-bust.

Bank of Ghana (2015), "EMI guidelines", available at: www.bog.gov.gh/privatecontent/Banking/E-MONEY%20GUIDELINES-29-06-2015-UPDATED5.pdf (accessed 6 July 2017).

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

Bogdan, R. C. & Biklen, S. K. (1989). Qualitative research in education: An introduction to theory and methods (3rd ed.). *Needham Heights, MA: Allyn & Bacon*.

Biesta, G. (2010). Pragmatism and the philosophical foundations of mixed methods research. In Tashakkori & Teddlie, C. (Eds.), Sage handbook of mixed methods in social & behavioural research (2nd ed., pp. 95-118). *Thousand Oaks, CA: Sage*. https://doi.org/10.4135/9781506335193.n4

Buchan, H. F., (2005) "Ethical decision making in the public accounting profession: an extension of Ajzen's Theory of planned behaviour," *Journal of Business Ethics,* vol. 61, no. 2, pp. 165- 181.

Buachi, B. (2021). Over 20,000 MoMo agents blacklisted for false transactions. www.theb&ft.com (Dec. 9, 2021)

Breeuwsma, M, de Jongh, M, Klaver, C, van der Knijff, R & Roeloffs, M (2007). "Forensic data recovery from flash memory", *Small scale digital device forensics Journal,* Vol. 1, No. 1, June 2007, http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

Camillo, M. (2017). 'Cybersecurity: Risks and Management of Risks for Global Banks and Financial Institution', *Journal of Risk Management in Financial Institutions,* **10**(2), pp. 196-200.

Canan, S. & Hume, C. (2016). Older consumers targeted by fraudsters not once, but twice!. Consumer financial protection bureau. Retrieved from https://www.consumerfinance.gov/about-us/blog/older-consumerstargeted-by-fraudsters-not-once-but-twice/

Centre for Victim Research report, (2019). Identity Theft and fraud victimization: What we know about identity theft and fraud victims from Research- and Practice Based Evidence.

Chauhan, S. (2015), "Acceptance of mobile money by poor citizens of India: Integrating trust into the technology acceptance model", info, Vol. 17 No. 3, pp. 58-68.

Choo, F. & Tan, K. (2007) "An 'American Dream' Theory of corporate executive fraud," *accounting forum, vol. 31*, no. 2, pp. 203-215.

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.*

Chen, K. Y. & Elder, R. J. (2007). Fraud Risk Factors and the Likelihood of Fraudulent Financial Reporting: *Evidence from statement on auditing standards No. 43 in Taiwan, Working paper*

Chetty, P. (2016). Importance of research approach in a research. Retrieved from https://www.google.com/search?q=ns&aqs=chrome

Checkpoint (2005), Taxis hailed as black hole for lost cell phones and PDAs, as confidential data gets taken for a ride, viewed 24 January 2013, http://www.checkpoint.com/press/pointsec/2005/01-24a.html

Majorie, C. M., Duflos, E. & Coetzee, G. (2022). "The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence." Slide Deck. Washington, D.C.: CGAP

Chavan, J. (2013). Internet banking – Benefts and challenges in an emerging economy. International Journal of Research in Business Management, 1(1), 19–26

Chaimaa, B., Naib, E. & Rachid, H. (2021). E-banking Overview: Concepts, challenges And solutions. Wireless Pers Commun 117, 1059-1078. https://doi.org/10.1007/s11277-020-07911-0

Creswell, J. W. (2003), *Research design: Qualitative, quantitative, and mixed methods approaches*(2nd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2014). Research design: Qualitative, quantitative and mixed methods approaches. *(4th ed.). Thousand Oaks, CA: Sage publications*

Cressey, D. R. (1953). Other People's Money. *New York, NY: The Free Press*.

Cross, C. (2018). How to get away with fraud: the successful techniques of scamming. Senior lecturer in criminology, Queensland University of Technology. Copyright © 2010–2022, *The Conversation Africa, Inc*

Cohen, J., Ding Y., Lesage, C., & Stolowy, H. (2010), "Corporate fraud and managers' behaviour: Evidence from the Press." *Journal of Business Ethics,* vol. 95, pp. 271-315.

Cohen, L., Manion, L., & Morrison, K. (2004). Research methods in education. *London: Routledge Falmer.*

Carpenter, T. D. & Reimers J. L. (2005) "Unethical and fraudulent financial reporting: applying the theory of planned behaviour," Journal of Business Ethics, vol. 60, no. 2, pp. 115-129.

Cross, C. (2018). How to get away with fraud: the successful techniques of scamming. Senior lecturer in criminology, Queensland University of Technology. Copyright © 2010–2022, The Conversation Africa, Inc

Deem, D. (2018). International Financial Crimes: *How do we turn the tide and help older victims?* Federal Bureau of Investigations. Retrieved from: https://www.elderjusticecal.org/uploads/1/0/1/7/101741090/debbie_deem-elder_justice_ca_aug1_with_sbaker_7.29.18-1.pdf

Deem, D., & Lande, E. S. (2018). Transnational scam predators and older adult victims: Contributing characteristics of chronic victims and developing an effective response. *US Att'ys Bull.,* 66, 177.

Deloitte (2015), "Mobile money", available at: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-mobile-money-payment-industry-marketing-distribution.pdf(accessed 6 June 2017).

Dilla, W., Harrison, A., Mennecke, B., & Janvrin D., (2011). "Avatars, capital ships, and false promises: An analysis of fraud in virtual worlds and its implications for the real world", *proceedings of the American accounting association Annual meeting, Denver, CO,*.

Ayamga, D. (2018) "Telecommunication Fraud Prevention Policies and Implementation Challenges" (master's thesis, Luleå University of Technology, 2018), https://www.diva-portal.org/smash/get/diva2:1222014/FULLTEXT01.pdf.

Drig, I., & Isac, C. (2014). E-banking services – Features, challenges and benefits. 10.

Dzomira, S. (2015). Online & electronic fraud prevention & safety tips cognizance in South African banks. *Socioeconomical – the Scientific Journal for Theory and Practice of Socio-Economic Development,* 4(8), 527-540. doi: dx.doi.org/10.12803/SJSECO.48131

Dzomira, S. (2014*).* Electronic fraud (cyber fraud) risk in the banking industry, ZIMBABWE. Risk governance & control*: financial markets & institutions/Volume 4, Issue 2.*

Dixon, P. (2006). Medical Identity Theft: The information crime that can kill you. *World Privacy Forum.* Retrieved from http://www.worldprivacyforum.org/wp-content/ uploads/2007/11/wpf_medicalidtheft2006.pdf

Etim, A. S. (2014), "Mobile banking and mobile money adoption for financial inclusion", *Research in Business and Economics Journal*, Vol. 9, p. 1.

Fadhel, K. (2002). Positivist and Hermeneutic Paradigm, A critical evaluation under their Structure of Scientific Practice. *The Sosland Journal, 21-28*

Federal Trade Commission (FTC). (2018a). Consumer Sentinel Network Data Book 2017. Washington, DC: Federal Trade Commission. Retrieved from https://www.ftc.gov/system/ files/documents/reports/consumer-sentinel-network-databook-january-december-2016/csn_cy-2016_data_book.pdf

Federal Trade Commission (FTC). (2017d). Identity Theft: Planning for The Future, Parts 1, 2, and 3. Retrieved from https:// www.ftc.gov/news-events/audio-video/video/identitytheft-planning-future-part-1

Federal Trade Commission (FTC). (2013b). Guide for Assisting Identity Theft Victims Retrieved from https://www. consumer.ftc.gov/articles/pdf-0119-guide-assisting-idtheft-victims.pdf

Federal Trade Commission (FTC). (2011d). Prepared statement of the federal trade commission before the subcommittee on socialsSecurity of the house committee on ways and means on child identity theft. Retrieved from https://www.ftc.gov/sites/default/files/documents/public_statements/preparedstatement-federal-trade-commission-child-identity-theft/110901identitythefttestimony.pdf

Federal Trade Commission (FTC). (2011f). *Stolen Futures: A Forum on Child Identity Theft.* Retrieved from https://www.ftc.gov/ news-events/events-calendar/2011/07/stolen-futuresforum-child-identity-thef

Freshman, A. (2012). Financial disaster as a risk factor for posttraumatic stress disorder: Internet survey of trauma in victims of the Madoff Ponzi scheme. *Health & Social Work*, 37(1), 39-48.

Fintech Africa (2017), available at: www.financialtechnologyafrica.com/2017/08/15/13-years-of-mtn-mobile-money/ (accessed 15 December 2017).

Fishbein, M. & Ajzen, I. (2011). Attitude, Intention and Behaviour: An Introduction to Theory and Research, *Reading, MA: Addison-Wesley.*

Frickenstein, J. (2019).“3 Mobile Money Fraudsters Busted,” Ghana Web. https://www.ghanaweb.com/GhanaHomePage/NewsArchive/3-mobile-money-fraudsters-busted-579138; “How IT-Security Affects Africa’s Financial System,” Africa Finance Forum Blog (blog), Making Finance Work for Africa, May 8, 2019.

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.

Golladay, K. A., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders, 12(*5), 741-760

Gilman, L & Joyce, M 2012, ‘*GSMA* — Mobile Money for the Unbanked’, Managing the Risk of Fraud in Mobile Money, Viewed 12 January 2013 http://www.gsma.com/mobilefordevelopment/wpcontent/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobilemoney.pdf

Ghana News Agency (report), September 3, 2021

Ghana Cyber Authority: https://www.csa.gov.gh/mobile_money_fraud.php

Gilman, L. & Joyce, M. (2012). "Managing the risk of fraud in mobile money",GSMA: Mobile Moneyfor Unbanked (MMU), https://www.researchgate.net/deref/https%3A%2F%2Fwww.gsma.com%2Fmobilefordevelopment%2Fwp-content%2Fuploads%2F2012%2F10%2F2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf

Givens, B. (2005). Criminal identity theft in california: Seeking solutions to the "Worst Case Scenario". *Privacy Rights Clearinghouse*. Retrieved from https://www.privacyrights. org/blog/criminal-identity-theft-california-seekingsolutions-worst-case-scenario

Gina, P., Hampshire, K., Kyei, P., Adjaloo, M., Rapoo, G, & Kilpatrick, K. (2008). *"Linkages between livelihood opportunities and refugee–host relations:* learning from the experiences of Liberian camp-based refugees in Ghana". *Journal of Refugee Studies* 21 (2): 230–252.

Glodstein, D., Glodstein, S.L., & Fornaro, J. (2010). Fraud trauma syndrome: The victims of the Bernard Madoff scandal. *Journal of Forensic Studies in Accounting and Business, 6, 1-9.*

Granberg, D & Holmberg, S 1990. 'The intention-behaviour relationship among U.S. and Swedish Voters'. *Social Psychology Quarterly*, vol. 53, No. 1, pp. 44-54.

Grazioli, S. & Jarvenpaa, S. L. (2000). "Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers," in *IEEE transactions on systems, Man and Cybernetics, Systems and Humans,* vol. 30, no. 4, 2000, pp. 395-410

Guba, E. G. & Lincoln, Y. S. (1989). What is this constructivist paradigm anyway? In fourth generation evaluation, London: *Sage Publications*, 79-90

GSM 2018 State of the Industry *Report on Mobile Money*

Harrell, E. (2019). Victims of identity theft, 2016. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Retrieved April 2019 from: https://www.bjs.gov/content/pub/pdf/vit16.pdf

Harrell, E. (2017). Victims of identity theft, 2014. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Retrieved June 2019 from https://www.bjs.gov/content/pub/pdf/vit14.pdf

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, 21(7), 681-698.

Heckers, H. & O'Brien, M. (2014). Advanced Identity Theft Responses: Financial identity theft. *The National Center for Victims of Crime & The Financial Industry Regulatory Authority Investor Education Foundation*. Retrieved from https://victimsofcrime.org/top-links/events/2014/09/10/ default-calendar/advanced-identity-theft-responses

Idaho Coalition Against identity theft. (2010a). *Identity Theft: A Training for Financial Institution Employees.* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/ toolkit/TrainingMaterials/TrainingForBankEmployees.pdf

Identity Theft Resource Center. (2017). The aftermath: *The non-economic Impacts of Identity Theft*. Retrieved Jun 2019 from: https://www.idtheftcenter.org/wp-content/ uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf

Internal Revenue Service. (2019). Identity theft victim assistance: How It Works. Retrieved from https://www.irs. gov/individuals/how-irs-id-theft-victim-assistance-works

Jansen, W. & Ayers, R. (2007). Guidelines on cell phone forensics, NIST Special Publication 800-101, Viewed 20 May 2013, http://csrc.nist.gov/publications/nistpubs/800- 101/SP800-101.pdf

Jenkins, B. (2008). Developing mobile money ecosystems, *International Finance Corporation and Harvard Kennedy School, Washington, DC*

Johnson, K. (2003). Financial crimes against the elderly. *Washington, DC: U.S. Department of Justice Office of Community Oriented Policing.* Retrieved from https://riczai-inc.com/Publications/cops-w0768-pub.pdf

Kadleck, C. (2005). Banks battle against growth of electronic payment fraud. *Crain's Cleveland Business 26.* No.3, http://www.craincleveland.com/

Kavitha, S. (2017). 'Factors Influencing Satisfaction on E-banking', *AIMS International Journal of Management,* **11**(2), pp. 103-115.

Kennedy, K. A. (2012). An Analysis of fraud: Causes, prevention, and notable cases. *University of New Hampshire Scholars' Repository*. University of New Hampshire.

Kenyon, W. & Tilton, P. D. (2006). Potential red flags and fraud detection techniques: A Guide to Forensic Accounting Investigation, *First Edition, John Wiley & Sons, Inc, New Jersey.*

Khan, A. S. (2001). "Telecom industry in Bangladesh: Current status and emerging issues." Telecommunications in Bangladesh: *Emerging Issues.*

KPMG report (2013). International Cooperative 'Global profiles of the fraudster',

Karp, N. & Kirkman, D. (2016). *Financial frauds and scams against elders:* Government responses and resources. National Consumer Law Center. Retrieved from https://www.nclc. org/national-elder-rights-training-project/consumer-fraudscams/financial-frauds-scams-against-elders.html

Klein, M. & Mayer, C. (2011). "Mobile banking and financial inclusion: the regulatory lessons", *The World Bank.*

Klutse, J. B. (2020). Five common tricks momo fraudsters use to steal your money. Retrieved from: Jbklutkse.com

Kusi, H. (2012). *Doing qualitative research. A guide for research*. Accra Newtown: Emmpong Press.

Knijff van der, R. (2002). Embedded systems analysis, handbook of computer crime investigation, Edited by Eoghan Casey, *Academic Press*, 2002.

Kish, L. (1949). A Procedure for objective respondent selection within the household. *Journal of the American Statistical Association*, 44, 380-387.

Kivunja, C. & Kuyini, A. B. (2017). Understanding and Applying Research Paradigm in Education Contexts. *International Journal of Higher Education*. 6(5). Doi:10.5430/ijhe.v6n5p26

Kumar, V. R. (2014). Respondent selection methods in household surveys. *ResearchGate Journal*. www.researchgate.net/publication/267512058

Kurnia, S., Peng, F., & Liu, Y. R. (2010). Understanding the adoption of electronic banking in China. *In 43rd Hawaii International Conference on system sciences, Honolulu, Hawaii, USA, pp*. 1–10.

Larnyoh, T. M. (2020). Tackling mobile money fraud in Ghana. *Business Insider Africa Businessinsiderafrica.com* Aug. 8, 2020

Matthew, N. O. S, Tembely, M., Musa, M. S. & Momoh, D. O. (2017). Mobile banking. mobile banking. *International Journal of Advanced Research in Computer Science and Software Engineering*. 7. 75-76. 10.23956/ijarcsse/V7I6/01615.

Maurer, B. (2015). How would you like to pay? How Technology Is Changing the Future of Money, *Duke University Press, Durham*.

Mazer, R., & Nitin G. (2015). "Recourse in Digital Financial Services: Opportunities for Innovation." *Brief. Washington*, D.C.: CGAP.

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.

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.

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

Mas, I. & Radcliffe, D. (2011). "Scaling mobile money", *Journal of Payments Strategy and Systems,* Vol. 5 No. 3, pp. 298-315

Miller, J. & Robuck, R. (2013). Youth and Credit: Protecting the Credit of Youth in Foster Care.Baltimore, MD: Annie E. Casey Foundation. Retrieved from http://www.aecf.org/m/ resourcedoc/AECF-YouthAndCredit-2013.pdf

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

Merritt, C (2010). Mobile money transfer services: the next phase in the evolution in person-to-person payments. Viewed 19 April 2013, http://www.frbatlanta.org/documents/rprf/rprf_resources/wp_0810.pdf

Mensah, E. C., & Dzokoto, V. (2011). Post redenomination and money management among ghana's urban poor. *Technical Report. Institute for Money, Technology, & Financial Inclusion (IMTFI)*, University of California, Irvine

Morales, J., Gendron, Y. & Guénin-Paracini, H., (2014). "The construction of the risky individualand vigilant organisation: A genealogy of the fraud triangle". *Accounting, Organisations and Society, 2014*. Available at: http://dx.doi.org/10.1016/j.aos.2014.01.006

Molla, A. (2005). Exploring the reality of E-commerce –benefits among business in a developing country. Available at http://www.sed.manchester.ac.uk/idpm/ publications/wp/di/index.htm [Accessed 9 April,2012]

Mhamane, S. S., & Lobo, L. M. R. (2012). Internet banking fraud detection using HMM. Paper presented at the icccnt'12, Coimbatore, India. IEEE-20180.

Ministry of Food and Agriculture Republic of Ghana. Retrieved 15 March 2014.

Mudiri, J. L. (2012). Fraud in mobile financial services, *MicroSave Publication*, Viewed 20May 2013, http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services _JMudiri.pdf Findings from CGAP research in Ghana, Kenya, Rwanda, Tanzania, and Uganda

Mudiri, J. L., (n.d.) "Fraud in Mobile Financial Services." Hyderabad: MicroSave. http://www.microsave.net/files/pdf/RP151_ Fraud_in_Mobile_Financial_Services_JMudiri.pdf

Mugisha, I. R. (2014). "Two Men Arrested for Allegedly Defrauding Rwf495m from Tigo."Blog post, 20 November. http://www.newtimes.co.rw/section/article/2014-11-20/183244/

Mudiri, J. L. (2012). Fraud in mobile financial services, *MicroSave Publication*, Viewed 20 May 2013, Retrieved from: http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMu diri.pdf

Mustapha, S. (2017). "MTN Sanctions 3,000 Agents for Mobile Money Fraud," Graphic Online, October 27, 2017, https://www.graphic.com.gh/news/general-news/mtn-sanctions-3-000-agents-for-mobile-money-fraud.html."Staff of Telcos Accomplices in Mobile Money Fraud – Police," Ghana Web, October 23, 2017, https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Staff-of-telcos-accomplices-in-mobile-money-fraud-Police-593227.

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.

Nemeth, R. (2005). Respondent selection within the household- A Modification of the Kish Grid. *Paper presented at the Sixth Austrian, Hungarian, Italian and Slovenian Meeting of Young Statistical, Ossiach, Carinthia, Austria.*

Brown, N. (2021). "Over 4,000 Cyber Fraud Cases Currently Under Investigation," Joy Online.April 23, 2021, https://www.myjoyonline.com/over-4000-cyber-fraud-cases-currently-under-investigation/?param=.

Nyasulu, T. U. (2012). Governance and customary land tenure in peri-urban Kasoa in Ghana.

Nyarko, P (2013). "2010 Population and housing census". *National Analytical Report. Ghana Statistical Service.*

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*.

NIST (National Institute of Standards and Technology) Special Publication 800-124 2008, Guidelines on Cell Phone and PDA Security, 2008, viewed 15 May 2013, http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

Office for Victims of Crime (OVC). (2019a). Crime victimization glossary. Retrieved fromhttps://www.ovc.gov/library/ glossary.html

Office for Victims of Crime (OVC). (2019b). Fraud and identity theft. Retrieved from https://ovc.ncjrs.gov/topic. aspx?topicid=29

Office for Victims of Crime (OVC). (2010). Expanding services to reach victims of identity theft and financial fraud. Retrieved from https://www.ovc.gov/pubs/ID_theft/pfv.html

Office of Fair Trading (2006). Research on Impact of Mass Marketed Scams, London: Office of Fair Trading.

ONS (2013) The likelihood of becoming a victim of crime. online. Available HTTP: http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-march-2012/sty-a-victim-of-crime.html (accessed 14 July 2015). http://www.pwc.com/gx/en/economic-crime-survey/downloads.jhtml (accessed 13 August 2015).

O'Leary, Z. (2004). The essential guide to doing research. *Great Britain: Cronwell Press Ltd*

Orr, B. (1999). "At last, internet banking takes off", *ABA Banking Journal*, Vol. 91, pp. 32-34.

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. 42No. 11, pp. 962-979.

Oghenerukevbe, E. A. (2008). Customers perception of security indicators in online banking sites in nigeria. *Journal of Internet Banking and Commerce, 13(3), 1-14.*

Ozyurt, S. (2019). Ghana is now the fastest growing mobile market in Africa. *Agence francaise de development (AFD).*

Pandey, M., (2010). A model for managing online fraud risk using transaction validation. *The Journal of Operational Risk. 5(1),* 49-63.

Pascual, A., Marchini, K., & Miller, S. (2018). Identity fraud: Fraud enters a neweEra of Complexity. *Javelin Strategy & Research*.

Pierce, P. (2009). Identity theft. office for victims of crime training and technical assistance center. Retrieved from http://www.ncdsv.org/images/OVCTTAC_ IdentityTheftResourcePaper_2012.pdf

Pilot, D., & Beck, C.T. (2014). Essentials of nursing research: Appraising evidence for nursing practice *(8th ed). Wolters Kluwer*

Plano, C. & Creswell, J. W. (2011). Designing and conducting mixed research. Los Angeles, Calif: *Sage publications.*

Ponemon Institute. (2013). 2013 Survey on Medical identity theft. Retrieved June 2019 from https://www.ponemon.org/local/ upload/file/2013%20Medical%20Identity%20Theft%20 Report%20FINAL%2011.pdf

Poong, Y., Eze, U. C. & Talha, M. (2009). 'B2C E-commerce in Malaysia: Perceived characteristics of innovating and trust perspective', *International Journal of Electronic Business,* 7(4), pp. 392-427.

Provencal, R.O. (2017). "Mobile money fraud on the rise in Ghana: victims share their stories", availableat: http://rainbowradioonline.com/index.php/general-news/item/9324-mobile-money-fraud-on-the-rise-in-ghana-victims-shares-their-stories (accessed 2 August 2017).

PricewaterhouseCoopers (2011). available at: www.pwc.com/gh/en/pdf/ghana-banking-survey-2011.pdf (accessed 11 October 2017).

Ramamoorti, S., (2008). "*The* psychology and sociology of fraud: integrating the behavioural sciences component into fraud and forensic accounting curricula", *issues in accounting education*, vol. 23, no.4, pp. 521-533.

Rofiq, A. & Mula, J. M. (2010). "Impact of cyber fraud and trust on e-commerce use: a proposedmodel by adopting theory of planned behaviour," 21st Australasian Conference on Information Systems, Information Systems: *Defining and*

Establishing a High Impact Discipline, Brisbane, Australia, Queensland University of Technology.

Rittenberg, L. E., Johnstone, K. M. & Gramling, A. A (2010). "Auditing: A business risk approach." 8th ed. Mason, OH: South-Western Cengage Learning.

Reiboldt, W. & Vogel, R. (2001). A critical analysis of telemarketing fraud in a gated senior community, *Journal of Elder Abuse and Neglect*, 13(4): 21-38.

Roberds, W. (1998). 'The impact of fraud on new methods of retail payment', *Economic Review-Federal Reserve Bank of Atlanta,* **83**(1), p. 42.

Roberts, P. (2016). "Mobile money sees 118% growth", available at: http://thebftonline.com/business/economy/21586/mobile-money-sees-118-growth.html (accessed 7 March 2017).

Saleh, Z. (2013). The impact of identity theft on perceived security and trusting Ecommerce. *Journal of Internet Banking and Commerce*, 18(2), 1-11.

Saunders, L., Pizor, A., & Twomey, T. (2009). Desperate homeowners: Loan Mod Scammers Step in When Loan Services Refuse to Provide Relief. *National Consumer Law Center*. Retrieved from https://www.nclc.org/images/pdf/ pr-reports/report-loan-mod-scams-2009.pdf

Saunders, M. N. K., Lewis, P., & Thronhill, A. (2008). *Research methods for business students,* 6thEdition, Pearson.

Senyo, P. K, (2021). "Ghana's New Mobile Money Rule Could Derail Financial Inclusion. But There Are Answers," The Conversation, April 18, 2021, https://theconversation.com/ghanas-new-mobile-money-rule-could-derail-financial-inclusion-but-there-are-answers-158770.

Singhal, D., & Padhmanabhan, V. (2009). A study on customer perception towards Internet banking: Identifying major contributing factors. *Journal of Nepalese Business Studies, 5(1), 101–111.*

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*

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/.

Sutherland, E. H., (1949). White collar crime. *New York, NY: Dryden*,

Sutherland, E. H., (1983). White collar crime: *The Uncut Version, New Haven, CT: Yale University Press.*

Suri, T. & Jack, W. (2016). "The long-run poverty and gender impacts of mobile money", Science (New York, N.Y.), Vol. 354 No. 6317, pp. 1288-1292

Synovate. (2007). *Federal Trade Commission*. 2006 Identity Theft Survey Report. RetrievedJune 2019 from https://www.ftc. gov/sites/default/files/documents/reports/federal-tradecommission-2006-identity-theft-survey-report-preparedcommission-synovate/synovatereport.pdf

Synovate. (2007). Federal Trade Commission – 2006 Identity theft survey report. Retrieved Jun 2019 from https://www.ftc.gov/sites/default/files/documents/reports/federal-tradecommission-2006-identity-theft-survey-report-preparedcommission-synovate/synovatereport.pdf

Tan, T. M., & Rasiah, D. (2011). A review of online trust branding strategies of financial services industries in Malaysia and Australia., Advances in Management & Applied Economics, *International Scientific Press, 1(1), 125-150.*

Tashakkori, A. & Teddlie, C. (2003a). Handbook of mixed methods in social & behavioural research, *Sage, California.*

Texas Identity Theft Coalition. (2010c). Module 2: Emotional Impact of Identity Theft. Retrieved from https://www. ovcttac.gov/downloads/identitytheftnetwork/ toolkit/TrainingMaterials/Module_2_ EmotionalImpactOfIdentityTheft.pdf

Tembely, M. & Musa, S. M. (2017). Mobile Banking. *International Journal of Advanced Research in Computer Science and Software Engineering*. ISSN: 2277-128X(Volume 7, Issue-6)

Troy, L. (2008). Apple iPhone passcode work-around, digital forensic lab, Fort Worth Police Department, Viewed February 26, 2013, http://mobileforensics.files.wordpress.com/2008/02/iphone_passcode_workaround.pdf.

Tsai, W., Huang, B. Liu, J. Tsaur, T. & Lin, S. (2010). 'The application of web ATMs in E-payment industry: A case study', *Expert Systems with Applications,* 37(1), pp. 587-597.

Upadhyay, P. & Jahanyan, S. (2016). Analyzing user perspective on the factors affecting use intention of mobile-based transfer payment. Internet Res. 26, 38–56.

Usman, A. K., MSc, & Shah, M. H. (2013). Strengthening E-banking security using keystroke dynamics. *Journal of Internet Banking and Commerce, 18(3), 1-11*

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.

Weber, R. H., & Aline D. (2010). "Legal Issues in Mobile Banking." *Journal of Banking Regulation 11,* no 2 (2010): 129 -145.

Wilks, T. J. & Zimbelman, M. F. (2004). Decomposition of fraud risk assessments and Auditors' Sensitivity to Fraud Cues. Contemporary Accounting Research, 21(3), 719-745.

Withers, S. (2008). Whoops! iPhone passcode bypass a cinch, viewed November 28, 2013 Retrieved from: http://www.itwire.com/content/view/20273/53/

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.

Yankson, P. W. K. (2012). Landlordism and housing production in Greater Accra Metropolitan. In: Ardayfio-Schandorf, Yankson, PWK & Bertrand, M. (Eds.). *The mobile city of Accra: urban families, housing and residential practices.* Daker, Senegal, CODESRIA

Yin, R. (2014). Case study research: design and methods. *United States of America: SAGE*

Zahra, S. A., Priem, R. L., & Rasheed, A. (1975). "The antecedents and consequences of top management fraud," *Journal of Management, vol. 31, no. 6, 2005, pp. 803-828*

www.graphic.com.gh/news/general-news/mtn-sanctions-3-000-agents-for-mobile-money-fraud.html

www.myjoyonline.com/opinion/2017/October-23rd/mtn-mobile-money-fraud-an-inside-job.php

The composite budget of the awutusenya east municipal assembly for the 2014 fiscal year".

APPENDICES

Appendix A

Letter of Introduction

UNIVERSITY OF EDUCATION, WINNEBA
FACULTY OF SOCIAL SCIENCE EDUCATION
DEPARTMENT OF SOCIAL STUDIES EDUCATION
P. O. Box 25, Winneba, Ghana
+233 (020) 2041096
socialstudies@uew.edu.gh

22nd November, 2021

TO WHOM IT MAY CONCERN

Dear Sir/Madam,

LETTER OF INTRODUCTION: MR. SAMUEL AMOABENG (200026582)

We write to introduce Mr. Samuel Amoabeng to your outfit to assist him conduct his research. Mr. Samuel Amoabeng is pursuing Master of Philosophy (M. Phil.) in Social Studies Education in the Department of Social Studies Education of the University of Education, Winneba.

As part of the requirements for the award of M. Phil. in Social Studies Education, he is undertaking a research on the topic "*Mobile Money Fraud in Kasoa Township.*"

We would be very grateful if he could be offered any assistance he may need to enable him achieve the purpose of his study.

Thank you.

Yours faithfully,

Mrs. Margaret G. Nyala
***For* Ag. Head of Department**

Appendix B

UNIVERSITY OF EDUCATION, WINNEBA

FACULTY OF SOCIAL SCIENCES EDUCATION

DEPARTMENT OF SOCIAL STUDIES

Questionnaire for mobile money subscribers

This questionnaire is designed to gather information for research at the University of Education, Winneba. The interest of the researcher is to explore mobile money fraud in the Kasoa Township. I would be grateful if you could open up with appropriate and frank answers to the questions/statements. This research is purely for academic purpose and your responses will be treated with utmost confidentiality. In this regard, your name or any other form of identification is not needed.

Section A: Demographic Characteristics of Respondents

1. Gender

   a) Male b) Female

2. Age Group

   a) 18-29 b) 30-39 c) 40-49 d) 50-59 e) 60+

3. Educational level

   a) Informal Education b) JHS c) SHS d) Diploma e) Graduate

4. Which mobile money operator services have you subscribed to? (Select mostly used)

a) Mtn Mobile Money b) Vodafone Cash c) AirtelTigo Money

4.a) Which other mobile money operator services have you subscribed to?

a) Mtn Mobile Money b) Vodafone Cash c) AirtelTigo Money

5. How long have you been accessing mobile money services from your phone?

a) Less than 1y b) 1-3yrs c) 4-6yrs d) 7-9yrs e) 10yrs+

SECTION B

TYPES OF MOBILE MONEY FRAUD THAT IS PREVALENT IN THE KASOA TOWNSHIP

6. Have you ever received mobile money fraud attempts on your phone?

a) Yes b) No

7. If yes, about how many times? Select only one:
   (Daily/Weekly/Monthly/Quarterly/Yearly)
   a) Less than 5 ☐
   b) 5-10 ☐
   c) 10-15 ☐
   d) 15-20 ☐
   e) 20+ ☐

8. If yes, what category?

a) Text Message b) Voice Call c) Both calls & text messages

b) d) Other specify……

9. Which type of mobile money fraud attempts do you normally receive? (tick only one)

Types of Mobile Money Fraud	
Scam messages	
Emotional Scam	
Anonymous calls from fraudsters	
Cash-out- Fraud	
Vendor Pin Fraud (*Agents who hand over phone for customers to punch numbers are victims*)	
False Promotion (The business scam)	

Fortuitous Scam (Goods from abroad)	
MNO Fraud (*Telco staff/agents make unauthorized transfer of funds*)	
Other specify: ……..	

10. Have you ever been defrauded? a) Yes b) No

11. About how many times have you been defrauded?

a) Once b) 2 times c) 3 times d) 4 times e) 5 times

12. Through which of the momo fraud type?

Types of Mobile Money Fraud	
Scam messages	
Emotional Scam	
Anonymous calls from fraudsters	
Cash-out- Fraud	
Vendor Pin Fraud (*Agents who hand over phone for customers to punch numbers are victims*)	
False Promotion (The business scam)	
Fortuitous Scam (Goods from abroad)	
MNO Fraud (*Telco staff/agents make unauthorized transfer of funds*)	
Other specify: ……..	

13. In total, about how much have you lost through mobile money fraud?

Specify…….

SECTION C

FACTORS THAT PROMOTE MOBILE MONEY FRAUD IN THE KASOA TOWNSHIP.

14. If Yes to ques. 10, provide one major reason why it was successful.

……
……
……
……
……

15. If No, provide one major reason why it was unsuccessful.

……
……
……
……
……

16. Which of these do you think is the major factor that leads to mobile money fraud?

(Please tick only one factor)

Factors of Mobile Money Fraud	
Motive/ Pressure (Greed, Financial need e.t.c)	
Opportunities (Weak internal control system)	
Rationalisation of committing the fraud	
Capabilities/ skills/ abilities of the fraudster	
Other specify……	

SECTION D

EFFECTS OF MOBILE MONEY FRAUD ON KASOA INHABITANTS.

Please read the question and thick one major effects of mobile money fraud on you.

1. In what way does mobile money fraud affect you? (inhabitants of Kasoa)?

EFFECTS	
Mental and physical trauma	
Treat to business survival	
Destroys business relationships	
Loss of customer trust	
Erosion of business trust	
Increases vulnerability	
Discourages Investors	
Other specify: …….	

SECTION E

Interview Guide

This questionnaire is designed to gather information for research at the University of Education, Winneba. The interest of the researcher is to explore mobile money fraud in the Kasoa Township. I would be grateful if you could open up with appropriate and frank answers to the questions/statements. This research is purely for academic purpose and your responses will be treated with utmost confidentiality. In this regard, your name or any other form of identification is not needed.

1. Have you ever received mobile money fraud attempts?
2. If yes, what category?
3. How do mobile money subscribers become victims of mobile money fraud?
4. What do you think are some of the factors that promote momo fraud?
5. How does mobile money fraud affect the inhabitants of Kosoa Township?

The percentage of the age distribution above confirms that of Ghana's population by age group. For instance, 18-29, 30-39 and 40-49 year age groups dominated the respondents for this study. The same way Ghana's population distribution for adults is also being dominated by 15-49 year group.