UNIVERSITY OF GHANA

COLLEGE OF HUMANITIES

THE EFFECT OF MOBILE PAYMENT TECHNOLOGY FRAUD PERCEPTION ON CUSTOMER INTENTION TO CONTINOUSLY USE THE SERVICE: A STUDY MODERATED BY GENERATION X, Y, AND Z FROM A DEVELOPING ECONOMY

ALFRED PAA GYAISEY

DEPARTMENT OF OPERATIONS MANAGEMENT

AND MANAGEMENT INFORMATION SYSTEMS

OCTOBER 2023

UNIVERSITY OF GHANA

COLLEGE OF HUMANITIES

UNIVERSITY OF GHANA BUSINESS SCHOOL

THE EFFECT OF MOBILE PAYMENT TECHNOLOGY FRAUD PERCEPTION ON CUSTOMER INTENTION TO CONTINOUSLY USE THE SERVICE: A STUDY MODERATED BY GENERATION X, Y, AND Z FROM A DEVELOPING ECONOMY

BY

ALFRED PAA GYAISEY

(ID NO. 10637829)

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON, IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF A DOCTOR OF PHILOSOPHY IN INFORMATION SYSTEMS DEGREE

DEPARTMENT OF OPERATIONS AND

MANAGEMENT INFORMATION SYSTEMS

OCTOBER 2023

DECLARATION

I hereby declare that this work is the result of my research done under supervision and has not been presented by anyone for any academic award at this or any other university.

27/10/2023

……..……..

Alfred Paa Gyaisey

(10637829)

Date

27/10/2023

…RICHARD BOATENG……

Professor Richard Boateng

(Lead Supervisor)

Date

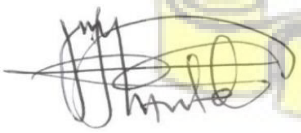
27/10/2023

……

Dr. Acheampong Owusu

(Co–Supervisor)

Date



30/10/2023

……

Professor Anthony Afful-Dadzie

(Co-Supervisor)

Date

ABSTRACT

The issue of mobile payment technology fraud or mobile money (MM) Fraud is relatively new in the context of the general concept of traditional fraud, as it is almost two decades old. Although fairly new, the subject of MM Fraud is of particular interest to the MM service as the service has been a revolutionary tool in transforming financial service delivery on the African continent and in developing economies (DE) across the globe. However, the subject of fraud, although is of interest to service providers, is yet to gain much traction in information systems (IS) research due to a number of reasons. The following has been ranked among the possible reasons: first, researchers' constant preoccupation with the success story of MM service in enabling financial inclusion regardless of geographical location, second, the persistent focus on making MM service technology adoption easy and to gain wider reach and then third, the general lack of focus from investment into research to understand the subject matter. This neglect has possible ramifications on customer trust and future sustainability and viability of the service. This thesis, hence, examines the possible effect of the perception of mobile payment technology fraud on customer intention to continuously use the service in the context of a developing economy and moderated by customer's or user's generation.

In this thesis, four key objectives were therefore spelt out to be achieved. The first objective was to *"undertake an empirical examination of the current perceptual state of MM service users"* in the face of incessant fraud attackers. Second, the researcher sought to *"examine how this current perceptual state of users affect their possible avoidance behaviour"* due to fraud attacks. The third objective was to further *"examine the effect of user's possible avoidance behaviour on their future continuous use of the service"*. Then finally, the possible *"moderating effect of MM service users'*

generation group on the relationship between their threat perception and avoidance behaviour". The purpose is to provide both practical and theoretical understanding of the issue of MM fraud and its potential effect on the sustainability of the service. Three main theories were used as a basis in order to achieve the purpose, the Technology Threat Avoidance Theory (TTAT), the Generational Theory, and the Theory of Intention to Continuously Use a Technology. By adopting a positivist paradigm, a quantitative research approach through a survey method was adopted to test 21 hypotheses using data collected from 384 mobile payment technology or mobile money users in Ghana.

In achieving the first objective, data from respondents were empirically examined based on concepts of rate of subscription or registration, specificity of use, and frequency of use. Ownership of social media account served as prelude to familiarity with modern technology. The research found ownership of social media account to be eighty-two per cent [82%] depicting high rate of technology familiarity among respondents. The rate of subscription or registration was found to be above ninety six percent [96.4%], and the rate of specificity of use was i.e., whether a user actually uses mobile payment system or MM for transactions, recorded over ninety six percent [96.6%]. In addition, regularity or frequency of use recorded above six percent [6.3%] for low, thirty percent [30.7%] for moderate, and sixty three percent [63%] for high. It was empirically established that the current perceptual state of MM is a positive one as there is still high patronage of the service.

To achieve the second objective, six constructs were used to examine users threat perception: perceived security threat, susceptibility threat, severity threat, perceived effectiveness, and self-efficacy. With respect to perceived security threat, the study found that perceived security threat has an effect on the avoidance behaviour of the MM user. The higher the perceived security threat,

the more likely a user will avoid using the service. Regarding susceptibility threat, the study established that the more users felt susceptible to MM fraud attacks, the more likely they are to avoid using the service. For severity threat, the study found that there was a negative relationship between the severity of the threat and avoidance behaviour, thus the more severe MM fraud attacks maybe on the user, the less likelihood of they avoiding the service. For self-efficacy, the study established that when self-efficacy among respondents is high the level of avoidance reduces. With regards to perceived effectiveness, it was also established that the higher the perceived effectiveness of MM fraud preventive measures, the lower or less likely the avoidance behaviour. Overall, it was established that based on the stated constructs, perception of MM fraud no matter how much or the nature of it has a consequential effect on avoidance behaviour.

For the third objective, the study established that the higher the avoidance behaviour today, the less likely it is that users will continually use or return to use the service in the future. As a predictor to the future patronage of the service, the continuous use of the service provided an insight into the future sustainability or viability of the service in the face of current fraud issues.

For the final objective that sought to examine whether there will be differences in the relationship between threat perception and avoidance behaviour among users when put under various generational cohorts. Users were grouped under three generation cohorts i.e., Generation X, Y and Z, and were examined on each of the six constructs. Overall, the study did not find a significant effect of a user's generation on the relationship between their threat perception and avoidance behaviour. Differences were established through a multi-group analysis among the three generations although findings were not significant.

In all, the study found that the issue of MM fraud perception, did not significantly affect the behaviour of users to avoid using the service. This was an interesting finding as it was in contradiction to TTAT's position that the threat associated with a technology will cause avoidance from the user. However, it also partially supports the TTAT's assertion that in the event where the technology cannot be avoided, the user will adopt a coping strategy or mechanism to minimize the possibly negative effect or pain associated with using the said technology. In the event the technology is avoided by the user, the study found that avoidance today was a good predictor of the user's intention to continuously avoid using the technology in the future.

The findings of this study, makes contribution to research, theory, policy, and practice in the following regard. First, this study makes major contribution to research by expanding the MM research from financial inclusion and economic gain to the issue of fraud and sustainability of the service in the long term. Theoretically, the study introduces and incorporates the concept of generation differences to the TTAT when studying technology adoption and use, as well as establishing whether the TTAT applicability and adaptability to the specific technology of mobile money payment due to it near indispensability. It further contributes to the postulation of that current avoidance behaviours distinct to future continuous use. Regarding policy contributions, this study provides an empirical evidence and confirmation on the level of subscription or patronage and degree of use of the service. With the service experiencing great success, the need for drastic measures to be taken to deal with the constant issue of fraud and its consequential effect in the long term cannot be overemphasized.

DEDICATION

This thesis is dedicated to God Almighty for bringing me this far, to my dear mum Elizabeth Abena Amoawah Baiden of blessed memory, to my beloved wife, Faustina Paa Gyaisey, my lovely children Lisa Paa Gyaisey and Austin Brain Paa Gyaisey.

It is also dedicated to Collins Amoako Addae and Comfort Owusu for all their support.

I also dedicate it to my church, Gospel Ambassadors Church and the general overseer Rev. Ebenezer Yamoah Ghansah, as well as to the Kaneshie Branch (Living Faith Centre), my associate Pastor Benjamin Arhin and special mention to my leaders Mr. Asamoah Otoo and Anthony Kwame Boateng.

ACKNOWLEDGEMENT

Many have contributed in diverse ways to this PhD thesis, both directly and indirectly; and I would like to thank them for their support and encouragement.

First, I am thankful and grateful to the Almighty God for granting me the grace and opportunity to go through this PhD work. Secondly, I express my profound gratitude to my supervisor, Prof. Richard Boateng for his confidence and trust in me to carry out this PhD work. I am also thankful to him for his guidance, constructive criticism, availability, advice and prayers. May God richly bless him.

To Dr. Acheampong Owusu, my co-supervisor, I say a big thank you for all the support and guidance that you gave me throughout my period of study. I really appreciate your support, Sir. And also, to Prof. Anthony Afful-Dadzie for your immense support and encouragement.

To all the participants and respondents who made this research possible, I say thanks. To my able research assistants Elizabeth Adjei, Evelyn Boabeng and Angela Pokuah Adjei, who helped me in administering my questionnaires. Finally, I say thank you to my family and friends whose support and encouragement helped me carry out this PhD. God richly bless them all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AVE	-	Average Variance Extracted
BBC	-	British Broadcasting Corporation
BBM	-	Bank Based Model
BMGF		Bill and Merlinda Gate Foundation

BoG	-	Bank of Ghana
CGAP	-	Consultative Group to Assist the Poor
DV	-	Dependent Variable
FDI	-	Foreign Direct Investment
FTT	-	Fraud Triangle Theory
FDT	-	Fraud Diamond Theory
GSMA	-	Global System for Mobile Communication Association
HTMT	-	Heterotrait – Monotrait
IMARC	-	International Market Analysis Research and Consulting
IntentCU	-	Intention to Continuously Use
INTERPOL	-	International Police
IV	-	Independent Variable
KYC	-	Know Your Customer
MENA	-	Middle East North Africa Region
MGA	-	Multi Group Analysis
MM	-	Mobile Money
MMI	-	Mobile Money Interoperability
MMS	-	Mobile Money Service
MNO	-	Mobile Network Operator
MTN	-	Multimedia Telecommunication Network
OTC	-	Over – The – Counter

PDA	-	Personal Data Assistants
PerEff	-	Perceived Effectiveness
PIN	-	Personal Identification Numbers
PLS	-	Partial Least Squares
PLS–MGA	-	Partial Least Squares Multi Group Analysis
PLS–SEM	-	Partial Least Squares Structural Equation Modelling
PerST	-	Perceived Security Threat
SelfEff	-	Self–Efficacy
SevT	-	Severity Threat
SIM	-	Subscriber Identity Module
SMS	-	Short Message Service
SSA	-	Sub–Saharan Africa
STK	-	SIM Tool Kit
SupT	-	Susceptibility Threat
TTAT	-	Technology Threat Avoidance Theory
UNCTAD	-	United Nations Conference on Trade and Development
USSD	-	Unstructured Supplementary Service Data
VIF	-	Variance Inflation Factor
WAEMU	-	West African Economic and Monetary Union
WAP	-	Wireless Application Network

CHAPTER ONE

INTRODUCTION

1.1 Background

The mobile phone innovation has enjoyed tremendous success after its invention and has consistently been a springboard for other innovations such as development of apps and access to the internet, as well as becoming extremely useful in areas such as education, healthcare, agribusiness, general commerce and all forms of economic activities. Mobile phones have now become a major tool for economic growth across the world as it is used for business transactions, receipt and payment of money for goods and services, etc through its mobile payment technology (Uswitch, 2021; Macwan, 2017). Looking in hindsight, the world's first mobile phone would be considered a strange piece of art which possibly perhaps served just one purpose: to make and receive calls, whereas today's version of the mobile phone is a great technology. By having a modern-day version of a mobile phone, one could have the entire world in his palm at any given point (Macwan, 2017). By checking the internet, going on social media, doing research, sending, and receiving instant messaging, be it text, voice or video, emailing, tracking of one's valuables such as cars, connecting it to security cameras at home, offices, and many more, the use of mobile phone is immeasurable (Uswitch, 2021). In fact, a mobile phone that can only make a call in this modern dispensation, would be seen as laughable to say the least. There is no denying the fact that the mobile phone technology has made tremendous impact on our daily lives.

Technology, which can be put simply as anything that helps us to do something easily, also brings changes to ways of life in the process of making work easier and comfortable (Cobla & Osei – Assibey, 2017). Depending on the nature or type of the technology, it is usually expected that the advent of such, will influence the user's way of living by making them more efficient as well as

increasing their productivity (Maurer, 2012). The world has gone through phases of technological advancement: from the stone age to the time when man made his first trip to the moon. In all, the introduction of mobile phone technology is one that has arguably been the most transformational on the global scale, penetrating the life of almost everybody on earth. It has aided in communication and has allowed for the creation of some more technologies, as well as allowing for the easy use of some pre-existing technologies and others that have come after it (Jack & Suri, 2011). As it has become a necessity to life, one needs no further proof to posit that the mobile phone technology has definitely come to stay and that the future will bring further improvement to this technology (Andrianaivo & Kpodar, 2012).

The adoption and use of mobile phone have also grown tremendously both on the global scale and among developing countries especially in Sub-Saharan Africa (SSA). There are a host of factors that have aided such growth within the SSA region and provides encouraging signs for the continent as Africa already has much catching–up to do. This growth has placed the developing world at a leading position of mobile phone adoption (Andrianaivo & Kpodar, 2012; Fanta et al., 2016).

By leveraging on the platform provided by the mobile phone technology, a number of services have managed to reinvent themselves and incorporate mobile phone technology into their operations to either allow for efficiency, reaching a wider population, easy access, or reducing cost, among others (World Bank Report, 2012). The financial sector for example, is one that has hugely benefited from the advent of mobile phone technology. One of the main benefits for example is that its adoption and use have been considered as a great opportunity and easier mechanism to curb the gap in infrastructure in the financial sector in the developing world (Andrianaivo & Kpodar, 2012). The banking industry had played a huge role in being the major

intermediary for almost all financial transactions or most activities that required sending or receiving money. Although the banking industry is still relevant even after the advent of MM, their key role of being virtually the only means of performing financial transactions have dwindled as the MM service have provided a much easier and convenient means of undertaking almost every form of financial service provided by the commercial banks (Kennedy & Konjaang, 2016).

In the year 2013, the Bill and Melinda Gates Foundation reported that a large number of the global population were outside of the formal financial sector (David-West, Umukoro, & Muritala, 2017). In their estimation, over 2 billion of the global population suffered some form of financial exclusion or were not receiving the full plethora of financial services (BMGF, 2013). Given that the benefits of expanding access to quality but cheaper financial services undoubtedly increase the speed in ensuring societal well–being and growth, increasing access through the use of mobile phone technology provides an even bigger opportunity for developing countries (David – West, Umukoro, & Muritala, 2017). According to the 2015 GSMA report, countries within the West African Economic and Monetary Union (WAEMU) still ranked lowest when it comes to financial inclusion on the continent of Africa (GSMA Report, 2015). To put it further, it was recorded that only 34.5% of this region's adult population have a formal account with a commercial bank. Reasons for this low rate could be attributed to several of factors which includes the low rate of adopting digital platforms by the people even with the high rate of mobile phone and internet penetration (GSMA Report, 2016). To address this challenge, a number of banks started building infrastructure and platforms for internet banking. A lot of investments have gone into advertising their online platforms to increase its appeal among its customers and the general public, although it impact has been checkered. Although internet banking could address a number of challenges such as reducing the number of clients who visit the bank and brings financial services to the

doorstep of clients, leveraging on customers using their mobile devices to access pure banking services still seems to appeal to just a few.

In the past decade however, the narrative has seen a dramatic shift as the use of mobile phone to provide financial services has grown bigger and become more relevant. Interestingly, this didn't come through the banking sector but rather the telecommunication sector. By creating a financial service enabling platform on our mobile phones, the telecom sector has achieved what the banks have struggled to achieve. Africa's telecommunication companies have ensured that money is now moving faster among the population. This technology, Mobile Payment Technology System, has been termed "Mobile Money" (MM), an innovation that has pushed even further the financial inclusion agenda particularly on the African continent (GSMA, 2015). Before the inception of MM on the continent, different means had been employed to save, send, or receive money, however, the MM innovation has provided an easier and more convenient route to achieve these purposes, and its popularity on the continent is now well known. Given the great success the service has enjoyed, it is safe to assume that, even those who initiated MM on the African continent could not envisage what has become of the service barely two decades after it was introduced (Matheson, 2016). The service has fast spread all over the continent and across the world with the number of subscriptions having grown over million times and the value of the service now reaching billions of dollars (GSMA, 2021). In each African country that the mobile money service has been initiated, the service growth has been tremendous, whether in the rate of subscription or in value of transactions. For an initiative that may have been valued a few dollars, Africa's mobile money economy is worth $459 billion by the end of the year 2020 (GSMA, 2021).

Mobile money fraud issue has been of great concern on the continent. Across the continent, the crime is being perpetrated almost everywhere with each country that uses the service having their

own fraud concerns to deal with (Botchey et al., 2020). Countries such as Kenya, Uganda, Zambia, South Africa and Ghana, all have had varying experiences with fraud issues (Gilbert, 2021; BBC Africa, 2018). However, earlier, he had received a call but immediately terminated.

1.2 Research Problem

Since the inception of MM, studies on this technology have grown steadily as the technology has received increasing attention in academic research (Narteh et al., 2017). It was apparent, after review of literature, that the issue of MM is gradually gaining traction within the academic space as studies are been conducted on the subject matter and the role it has played in Africa's financial space and across the world. Some studies have defined exactly what MM is within the telecommunication and financial space, and the growth the service has enjoyed (Asongu & Asongu, 2018; Botchey, Qin & Hughes–Lartey, 2020). Further, although not limited to these, available literature also covers a wide range of relevant themes such as adoption/use and financial inclusion (David-West, Umokoro, & Muritala, 2017; GSMA, 2015; Senoua, Ouattarab & Houensouc, 2019;), eradication of poverty (Gurbuz, 2017; Matheson, 2016; Van Hove & Dubus, 2019), major provider of employment, easy access to social services, interventions, and support (Mugambe, 2017), and impact on health, education, and lifestyle (Cobla & Osei-Assibey, 2017; Mitrega-Niestrój, Puszer, & Szewczyk, 2018). The following are however gaps that have been identified by this research and so has been a motivation for this study.

First, it is important to emphasize that the differences in the specific issues related to MM service is enough proof that different perspectives are still dominant on this subject. Almost every country on the African continent where MM operates has had its share of fraud issues (Gyaisey & Owusu, 2022). However, studies in relation to MM fraud have barely received the required research attention with focus rather on other aspects of the service as has been established above. The

problem faced by stakeholders within the MM space regarding fraud attacks has been of great concern (CGAP, 2017). The popularity and growth of the service has made it the cash cow for fraudsters and cybercriminals with the issue of money laundering through mobile money now being of great concern. The agenda currently by stakeholders has been on how to reduce this threat and also how to minimize it effect (CGAP, 2017; Baganzi & Lau, 2017). In the context of Ghana, although the problem is widely known among users of the service, little attention has been given to the problem in terms of academic research. Specifically analyzing how this menace have affected the general perception of MM service users is nonexistent, with recent few sporadic studies focusing on controlling the MM fraud (Akomea–Frimpong et al., 2017). Review of literature suggests that, the issue of MM fraud is indeed a big problem, and the continent loses millions of dollars annually to both local (country specific) and international (across Africa and the world) fraudsters and cybercriminals (Busuulwa, 2016; Laryea, 2016; CGAP, 2017; Akomea–Frmpong, 2019). Empirical evidence on the nature and typology of fraud occurring within the service, strategies adopted by fraudsters, among others, are lacking (Merritt, 2011; Subex, 2017; Akomea–Frimpong, Andoh & Akomea–Frimpong, 2020). Given that such issues possess both current and future threats to the service, providing an empirical perspective to the problem was a great motivation for this study.

Secondly, examining IS theories in relation to the MM fraud attacks is an area that is yet to be explored (Kim, Mirusmonov, & Lee, 2010; Shaw, 2014, Sanchez-Prieto, Olmos-Miguelanez, & Garcıa-Penalvo, 2016). With regards to theories related to the subject of MM, studies that have been conducted have used different theories for examination of issues based on the focus of those studies. The MM concept is one that also cuts across several academic divide such as finance, economics, health, agriculture, information systems and technology. As a result, theoretical

frameworks that have served as bases for research from these backgrounds have also varied greatly. The TTAT, for example, has it primary focus on how users of a technology react to threats associated with the said technology. It primarily examines a technology users' behavioural strategy in the face of threats and as a result examines the users threat perception against their possible avoidance or non-avoidance behaviour. The theory has mostly been used widely to prove or disprove the likely behavioural pattern of a technology user and have proven robust in established findings (Liao, Palvia & Chen, 2009; Avornyo, Fang, Odai, Vondee, & Nartey, 2019). However, given that technologies differ in terms of its relevance to the social infrastructure, overly generalizing the applicability or robustness of the theory against every technology could be erroneous as in the case of MM technology.

Third, it is important to emphasize that the concepts of avoidance and continuous use are distinct. As has been stated, the TTAT greatly emphasizes the manifestation of avoidance behaviour from the threat and coping appraisal themes. These themes are the foundation of the TTAT and are gained from the Technology Acceptance Model (TAM). As a result, in an attempt to test the concept of continuous use, researchers have adopted the underlying themes of the TTAT and TAM as measures for continuous use. These constructs such as Perceived Usefulness, and Perceived Ease of Use, have dominated the prediction of continuous use. For example, Avornyo et al. (2019) conducted a study on the factors that affect the intention to continuously use of mobile banking in two cities in Ghana (Tema and Kumasi). In their study, 295 customers of banks in the aforementioned two cities were examined on intention to continuously use mobile banking service based on Perceived Usefulness, Perceived Ease of Use, among other factors. Their study found that Perceived Usefulness positively affected intention to continuously use the services whiles perceived ease of use did not affect intention to continuously use the mobile banking service. Other

studies conducted by Jusuf et al. (2017), Yuan et al. (2014) and Zhou and Liu (2014) also established that perceived usefulness and satisfaction significantly affected the intention to continuously use mobile banking service. Whiles Albashrawi and Motiwalla (2017) have also established that perceived usefulness had a positive impact on satisfaction, a critical preceding element that predicts continuous use of mobile banking. Yuan et al. (2014) further analyzed that both perceived risk and perceived task-technology fit respectively had negative and positive effect or impact on the continuous use of mobile banking technology. It is however important to state that in all of these factors, avoidance motivation or behaviour has not been included in such examinations. The focus has primarily been on the perceived factors stated above without giving cognisance to the fact that such factors first precede avoidance motivation or behaviour, after which avoidance impacts either continuous or discontinuous use. Literature on a distinction or interconnectedness of avoidance motivation or behaviour, and continuous usage demonstrated in the above review is still grey. As has been established, a number of studies have primarily focused on avoidance behaviour as the final destination of an individual's conclusive decision on a technology for a number of varied reasons. However, the question beckons whether avoidance today does automatically lead to discontinuous use of a technology or otherwise.

Finally, establishing the existence or nonexistence of differences among different generation cohorts on their MM threat perception and related avoidance behaviour is arguably yet to be attempted in information systems research (Jiří, 2016; Desai & Lele, 2017). The generation concept which has necessitated the need to identify differences in the behaviour of a group of people, has become even more critical in academic research. Review of literature suggest the generation concept has widely been used in research that covers other areas of academia (Bittner et al, 2013; Schäffer, 2015; Andrea, Gabriella, & Tímea, 2016; Jiří, 2016). From an IS perspective,

this evidence further lays bare the need for IS academics to shift focus onto the subject of generations as it is a good predictor to behavioural patterns in technology use. Aside the fact that generation studies are lacking, technology is constantly changing as there are innovations springing up regularly, incorporating studies on generation groups in relation to technology adoption and use provides insight into the behavioural patterns of such group of people in a fast-changing technology driven world.

The Generation concept has grouped people into cohorts of Baby Boomers, Generation X, Generation Y, and Generation Z, with little differences in the specific periods among different scholars (Tari, 2011; Jiří, 2016; Dill, 2015). This study adopted the generation x, y and z categorization for examination. The MM technology and it related fraud concerns is a peculiar problem as this form of technology is quite different from previous ones. Outside the traditionally established banking and financial service delivery, this is the only technology that provides access to value or money with just any kind of mobile phone, with no need for the internet. Studies have established that there are differences with regards to how and when technology is adopted among different groups of people and as a result have gone further to categorize people under the diffusion of technology theory (Straub, 2009). Other studies have proven further that, the behaviour of people in the face of threat differs (Ein-Dor, 2014). The question then arises whether the threat of fraud regarding MM service will elicit different responses among users.

1.3 Research Purpose

The main purpose of this study is to make an assessment of the current state of MM fraud within the Ghanaian MM ecosystem and then further initiate a theorisation process by testing the TTAT with respect to the MM technology and in relation to the generational group concepts. These in turn will further aid in explaining the future viability of the service based on continuous or

discontinuous use of the technology. As has been established, empirical examination of current MM fraud situation in Ghana is non-existent, hence, decision making on the subject matter is more speculative in nature. This empirical assessment attempt is necessary to prove and or refine existing theories on technology adoption/use to aid in academic studies and research, and help policymakers/practitioners for countrywide policy directions and on–field execution respectively.

1.4 Research Objectives

The study therefore seeks to achieve the following objectives:

1. To perform an empirical examination of subscription and patronage rates of the MM service given cognisance to the current fraud situation in Ghana.
2. To examine the effect of users' threat perception on their avoidance behaviour towards the MM service.
3. To examine the effect of users' avoidance behaviour on their continuous use of the MM service.
4. To ascertain the moderating effect of users' generation in relation to their threat perception on their avoidance behaviour towards the MM service.

1.5 Research Questions

The study sought to seek answers to the following guiding questions:

1. What are the rates of subscription and patronage of the MM service given cognisance to the current fraud situation in Ghana?
2. What is the effect of users' threat perception their avoidance behaviour towards MM service?
3. What is the effect of users' avoidance behaviour on their continuous use of the MM service?

4. What is the moderating effect of users' generation in relation to their threat perception on their avoidance behaviour towards the MM service?

1.6 Significance of Research

The significance achieved by any research just as in IS, can be viewed in three broad perspectives; policy, practitioner and academic perspectives, of which this research is no exception. In academia, the concept of mobile payment technology specifically defined in this study as "mobile money" is relatively new. Being close to two decades since its inception, this technology has gained traction in various discussions on local, national and international platforms. However, the issue of fraud in relation to this technology in recent times have caused a shift in perspective from adoption and use of the technology to user safety and security. First, this study is important to properly understand and conceptualize the issue of mobile money fraud especially in the context of Ghana and to provide basis and perspective in understanding the general situation of mobile money fraud on the continent. Second, this conceptualization is important to properly situate or consolidate the theoretical underpinning of MM and specifically fraud related to the MM service. Third, the study will provide a deeper knowledge on the issue of fraud among MM service users, their perception of threat, security and safety. In the field of practice, this study is particularly important because factors such as fraud, security and safety are most critical in money related services provided by any institution. For services provided that relates to money, it has been established that trust is the most important factor between the service provider and the customer. This study will help practitioners understand the perception of consumers in relation to the issue of fraud, and the relevant safety or security measures preached by service providers. It will provide information on the level of confidence that mobile money users have in the service through the examination of their threat perception. This will inform service providers on the necessary strategies to adopt to

either improve or consolidate customer trust in the service. The study is also significant as it will help reveal the avoidance behaviour among users of the service in the face of all the fraud issues, and the potential future ramifications. On the policy point of view, the importance of this study cannot be overstated. Evidence from the central banks of countries whose citizens are major users of this service suggests that the service provides a huge wind fall in terms of revenue generation accrued to the governments through taxes, fees and charges as well as foreign remittances. Ensuring it survival and improvement for both now and the future cannot be rehashed enough.

1.7 Synopsis of Chapters

Chapter one of this study presents the introduction of the study. It includes the background, the research problem, research questions and objectives. The other part of the work is organized as follows:

Chapter two of the study speaks to the concept of mobile money and how it works. This chapter establishes a distinction between the mobile money service and other payment technologies that could be operated using the mobile phone. The chapter also speaks of key players and major stakeholders within the mobile money ecosystem.

Chapter three presents the growth of mobile money among some specific countries on the African continent, describing it inception and growth within almost two decades. The chapter also addresses the issue of mobile money fraud and it effect on the confidence of customers or users and being an existential threat to the service.

Chapter four speaks to the theoretical underpinnings of the study whiles in this chapter, a presentation is done on the theories that underpinned this study. Theories that were used which included the Technology Threat Avoidance Theory, Fraud Theories, Protection Motivation

Theories, among others, were contextualized and used as a bases in developing the framework of the research.

Chapter five presents the conceptual model or framework of the study and the development of hypothesis. This chapter also describes how constructs from the underpinning theories were used in developing the framework of the research, as well as in addition to literature review, helping in the formulation of hypotheses.

Chapter six discusses the methodology employed for the study. This chapter discusses the various reasoning and paradigms in academic research and establishes the paradigm that underpins this study. The chapter also throws more light on research design employed, the methods used, how data gathering instrument was developed, sample size, study population and sampling techniques and strategies that were used.

Chapter seven presents the results and analysis of the study. This chapter presents the demographic information of respondents, provides the descriptive of all the constructs that were used in the study. The chapter also makes a presentation on structural modelling analysis, multi group analysis as well as examining the moderating effect of the various generations in the study.

Chapter eight of the study presents the discussion of the study. In this chapter, results that were obtained after testing of the stated hypotheses are discussed in relation to other studies that have been conducted on the subject of mobile money and mobile money fraud. The chapter presents the study's contribution to theory and body of knowledge, its relevance to practice and how it provides suggestions for policy directions.

Chapter nine presents the conclusion, recommendations and suggestion for future studies. This chapter provides insight into how the study provides a general perception of mobile money fraud

threat among mobile money service users and how their perception informs their decisions on continuous use or avoidance. It provides other limitations that the study encountered and how future studies can address them.

CHAPTER TWO

LITERATURE REVIEW

2.1 Chapter Overview

This chapter presents the concept of mobile payment technology (Mobile Money). This chapter defines mobile money in the context of other payment technologies, key stakeholders or players within the mobile money ecosystem, how mobile money works, and major telecommunications networks which offer the service in Ghana and Africa.

2.2 Defining Mobile Money

Attempts have been made to define what mobile money is. In some jurisdictions, the name M–Commerce have been used interchangeably with Mobile Money to mean the same thing. Depending on the jurisdiction or the geographical location, one may come across either of the stated terminologies. The table below provides a summary of some definitions of the concept.

Table 2.1: Definitions of M-Commerce Confused to be Mobile Money

M-Commerce as:	
Technology	M-commerce refers to access to the internet via a mobile station or device such as a cell phone or a PDA (McDonnel, 2020).
	It is the use of mobile handheld devices to communicate, inform, transact and entertain using text and data via connection to public and private networks (Vrechopoulos et al., 2003)
	The use of mobile handheld devices to communicate, interact via high-speed connection to the internet (Zeng et al., 2003)

	The use of wireless technology to provide convenient, personalized and location-based service to customers, employees and partners (Yasar, 2022).
	Using smart phones and handheld computers with wireless connections to place orders and transact business over the web (Wu & Wang, 2005)
Product	M-commerce is a commercial application offered on the electronic medium of business transaction being deployed on a platform (Ayo et al., 2007).
Service	M-commerce is any transaction with a monetary value that is conducted through a mobile communication network (Durlacher, 2002).
	Business transaction conducted while on the move (Kalkota & Robinson, 2001).
Interaction of technology, product, and service	The buying and selling of goods and services using wireless handheld devices such as mobile phones and Personal Data Assistants (PDAs) (UNCTAD, 2002).
	The buying and selling of goods, services and information without any location restriction by mobile devices which uses a wireless connection to establish communication between all the necessary parties to complete the transaction (Jonker, 2003)

However, the concept of MM in the context of Africa is different. According to a report published by Interpol in 2020, the concept of MM is defined as a "digital financial service in which an individual uses a mobile phone handset to access a financial service or initiate a financial transaction" (INTERPOL, 2020). To throw further light on the phenomenon, Mobile Money

Transfer (MMT) has been defined as any form of financial service that Mobile Network Operator (MNO) give to their customers or subscribers that allows them the opportunity to transfer money electronically in a form of digital cash through their mobile network channels (Adedoyin et al., 2017). This definition is more relevant for this research as it is more reflective of the nature of the service in Africa. The service involves transferring cash either from a subscriber to another subscriber or from an agent to a subscriber through mobile channels (Shen, 2014). Unlike official banking services that requires a bank account, a relationship which is almost contractual, the mobile money service rather do away with the cumbersome processes involved with a bank. Rather, the "customer" uses his/her mobile phone or device to initiate a transaction using an electronic money. The idea of mobile money is somewhat different in the West or developed countries, where the concept is viewed as a continued form of banking services where one can enact a transaction on their bank accounts without visiting the banking hall and by the use of mobile devices (Adedoyin et al., 2017). Until recently, obtaining a bank account in a number of developing countries was a challenge for both individuals and businesses. This led to a high rate of financial exclusion of the masses in accessing financial services (Demirg¨uc¸-Kunt et al., 2017).

The introduction of mobile money transfer technology has become highly and significantly strategic to the unbanked and underbanked. Given the numerous definitions given to the service, what constitute a Mobile Money Services (MMS) has become contentious (Ayo et al, 2007). Regardless, it is generally accepted that MMS usually includes, consultation of account holders balance, storing of electronic cash, transfer of money and making of payments by the use of mobile phones (Shen, 2014; Adedoyin et al., 2017; Demirg¨uc¸-Kunt et al., 2017). Defining what constitute mobile money depends on a number of factors hence varies based on institutions (INTERPOL, 2020). The World Bank's 2017 Financial Inclusion Index reports' definition of a

mobile money account is limited only to financial services that can be accessed without the user having an official account with a formal financial institution ((Demirg¨uc¸-Kunt et al., 2017). In their estimation, anybody who operates a mobile money account that in one way or the other is linked to their financial institution is regarded as having an official account with the financial institution, a situation which connotes a reference to mobile banking.

The mother umbrella which represents the interest of all mobile network operators in the world, the Global System for Mobile Communications Association (GSMA), rather views mobile money in the opposite form. According to them, mobile banking should be considered as a subsection of mobile money as it is a financial service provided by a nonbank institution such as Mobile Network Operators (MNO) (GSMA, 2012). Hence, the term mobile money just connotes the use of mobile phone to access financial services, regardless of the model used in deploying the service, or the type of financial transaction (GSMA, 2012).

The varying opinion on the scope of the mobile money service could be attributed to jurisdictional differences in laws and regulations. For some countries, services which involves money transfer are solely handled by the banks or other formally established financial institutions. In some other jurisdictions, the operations of telecommunication networks or MNO would yield the introduction of such a service (GSMA, 2018). As such, there are two main models of mobile money: bank-based model (BBM) and the MNO based model or third parties (Ahmad, Green, & Jiang, 2020). In the MNO model, the, telecommunication network partners a bank to hold the electronic money as they themselves cannot issue money. In such situations the MNO can be given a license or certification to be able to issue electronic money from the state or the regulatory body (Ahmad et al., 2020; GSMA, 2018). There are negatives and positives associated with each model. One main

advantage of MNO model is that MNOs have proven over time that they can build and manage long chain of agent networks especially in remote and rural areas.

These MNOs have also built strong brands through their well-grounded marketing strategies and the trust they have built in their large customer bases of being able to provide such services (GSMA, 2016). The model adopted by the banks also have it advantages. Due to their financial backing, there is greater guarantee and assurance given to financial regulators in terms of fiscal discipline, well-structured security, trusted and proven processes, among others (Ahmad et al., 2020). One other model that is not very much popular but do exist is a combination of the government, the banks and the MNO. In such cases the MNO or cell phone company who provides the communication service is partnered by an interbank clearing system which is sponsored by the government. The interbank systems operate the payment processes between banks and among the accounts in a bank. The system currently operating in Ghana, for example, is associating the mobile money services by MNO with a bank or a nonbank financial institution or service provider or operator (GSMA Connected Women, 2020). With such structure, the mobile money service provider engages the cash in/cash out payments which is done through their agents. However, they go further to provide other services such as savings & loans, insurance services, cross border and transnational remittances, among others, due to their association with insurance companies, remittance companies, etc. In other instances, banks in partnership with MNOs, may use the technical infrastructure such as the Unstructured Supplementary Service Data (USSD) as the conduit, to provide some form of mobile money services in order to attract a different group of customers who may be unbanked (GSMA, 2018; GSMA Connected Women, 2020).

Africa's development of mobile money was a rather an interesting one. After the inception of M-Pesa in Kenya in the year 2007, many MNO plying their trade on the continent saw the service as

an opportunity to increase their revenue streams due to the increasing number of mobile phone users (Baba, 2010). Currently, the benefit of the service to the MNOs and the banks is staggering. Governments across the continent also saw the service as a great tool to bridge the gap of financial inclusion of large sections of their populace who were previously deprived of such services (Demirg¨uc¸-Kunt et al., 2017). Currently, all the models of the MM service, i.e., bank-led, MNO-led and hybrid models are all operational on the continent and enjoying great success.

2.3 Key Players of Mobile Money Ecosystem

There are various models of MM service delivery as has been established previously. However, a typical MM cycle always involves several stakeholders who play different roles and derive various benefits from the whole mobile money ecosystem. Depending on the jurisdiction of operation, the MM ecosystem may have four (4) key players as depicted in Figure 2.1.

2.3.1 The User

The User(s) is made up of the individual MNO subscribers who access the service through their phones (Jenkins, 2008; Merritt, 2010). They create account basically by providing authentic personal information and is enrolled unto the platform on which they are allowed to make deposits and withdrawals which attracts charges termed commissions. A user is an individual, business or anybody that uses the MM service. Users are those that basically rely on the service to send or receive cash and depend on the service to make payments for goods bought or receive payments for goods sold (GSMA, 2012; GSMA, 2013). As a business, their operations may revolve around the service, where they deliver products to clients either in the country or across in other countries and receive payments through the service. The MM service in Ghana for example allows for users to be able to purchase instruments such as government securities, and engage in online shopping, among others (Botchey et al., 2020).

2.3.2 Agents

Agents are the intermediaries between the customer (user) and the service provider. Agents play major role as they take users through the registration processes to get their SIM cards registered to get access to the service, by so doing they create accounts for customers (Jenkins, 2008; Merritt, 2010; Botchey et al., 2020). They also receive cash from customers and deposit unto their electronic wallets as well as assist them in sending money unto the wallet of other users. The agent also assists customers to withdraw electronic money from thegeneral cohortsir wallets by receiving electronic money unto their wallets and giving the customer cash in return and may also assist customers to rectify wrong transactions and also receive instructions from the service provider to be implemented (GSMA, 2012) By receiving instructions from the service provider and implementing them on the field, the agent serve as a representative or the face of the service provider.

2.3.3 The Mobile Network Service Provider

The service providers are the telecommunication companies who provide the mobile money service, in addition to their voice and data services (Botchey et al., 2020). They are responsible for building the system, both hardware and software and ensure the MM service runs smoothly. They are also responsible for the implementation of all systems that assures customers of the safety of their funds, which is a critical part of the mobile money value chain (IMARC, 2022). They are also responsible for meeting all the requirements of regulators within the jurisdiction they operate. They provide the network connectivity and the SIM cards which serves as the platform for creating the electronic wallet and register customers unto the mobile money wallet through their agents (GSMA, 2012; IMARC, 2022).

2.3.4 Banking Institution

The third player in the MM service are the banks or financial institutions (Merritt, 2010; Tagoe, 2016). The e-wallet created on the customer's SIM card is the intermediating link between the customer's funds and a float account held by a commercial bank in the name of the telecom company (GSMA, 2012). Every mobile money operator i.e., network, has an account with a commercial bank that houses cash deposits of customers and agents in a float account. In Ghana, for example, the management of this account is established in the E-Money Guidelines from the Bank of Ghana (BoG) (GSMA, 2015). In recent times, these banks have also created the platform for customers who save with them to be able to connect their mobile money accounts to their bank accounts held by these banks.

2.3.5 Regulatory Bodies

The MM service falls within and forms part of the financial sector of every country's economy and so are regulated by government financial sector policies and requirements usually through the central bank (GSMA, 2015). In the event where such policies are not available specifically for the mobile money service, they are responsible for creating such regulations. The central bank along with other regulators such as the communication authorities form the central regulatory bodies. In Ghana, for example, the Bank of Ghana is responsible for setting the regulatory framework to guide this activity (Tagoe, 2016). This led to the establishment of the E-Money Guidelines in 2015 by the BoG to regulate activities of telecom networks and banks.

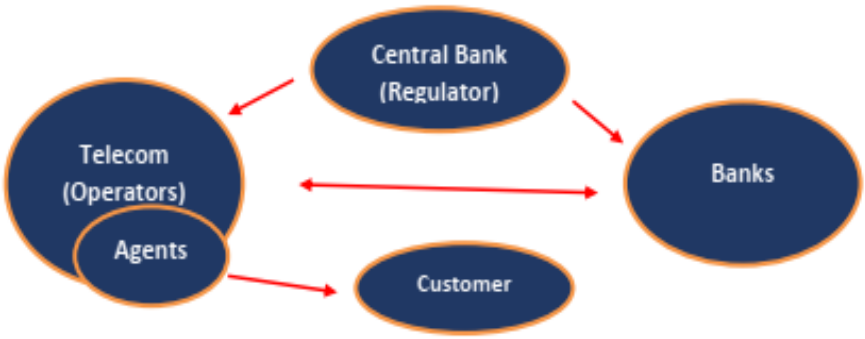


Figure 2.1 Mobile Money Service Players Conceptual Framework

Source: Author's Construction

Table 2.2 below presents the key players in the mobile money ecosystem as have presented, depicts their respective roles in the provision of the service and the benefits or incentives these players enjoy based on the roles they play in the MM value chain

Table 2.2: Key Players in the Mobile Money Ecosystem

Actor(s)	Role(s)	Incentive(s)	References
Customer or Mobile Money User	Customers of the services are registered individuals or organizations that use the service based on their needs.	They are able to conveniently send or receive remittances or perform financial transaction at a cheaper cost, anytime they need it and can be done almost everywhere they are.	GSMA (2012), GSMA (2015), Merritt (2010), Jenkins (2008), Botchey et al. (2020)
Telecommunication Companies or Mobile Network Operators (MNO)	In an MNO based mobile money model, MNOs provide mobile money services in partnership with banks or through obtaining e-money issuer licenses. They use their existing mobile phone service customer base and communication infrastructure as a competitive advantage. In a bank led mobile money model, MNOs provide the mobile infrastructure and communication services. An MNO ensures compliance with telecommunication regulations and policy within the country.	Provides new revenue stream as customers pay charges for the use of the service. MNOs with wider coverage gets to attract more subscribers as they would have a wider reach, invest in infrastructure and other security related technologies.	Botchey et al. (2020), IMARC (2022), GSMA (2012)
Bank/financial institution with	In an MNO based mobile money model they may act as segregated/trust accounts for MNOs. They enable the exchange of money between different parties. In a bank led model, they deliver	Banks or other financial institution can leverage mobile money platforms to reach new customers in	

banking license and infrastructure	mobile money services in partnership with MNOs of which they use the technical infrastructure. They also provide oversight and ensure compliance with national financial regulations and policy.	traditionally underserved areas at much lower cost.	Merritt (2010), Tagoe (2016), GSMA (2012), GSMA (2015)
Regulatory institutions across different sectors	Key regulators usually include Central banks for the financial sector and telecommunication regulators for the communications sector. They set up the regulatory framework under which mobile money service providers operate.	Driven by the need for national development, regulators would like to see more people served by formal financial and communication services.	GSMA (2015), Tagoe (2016)
Agents	They familiarize customers with products and services, guide and support them in their transactions. They may also enroll new customers. They facilitate cash-in (converting cash into mobile money) and cash-out (issuing cash on demand) hence ensure convertibility between mobile money and cash. The agent activity can be a full-time endeavour, or a side activity carried out in addition to their main enterprise. An agent may serve several mobile money service providers. MNOs have developed extensive	Agents earn commission on various transactions carried out by mobile money users	GSMA (2012), Merritt (2010), Jenkins (2008), Botchey et al. (2020)

	agent networks to sell airtime and other products while those of the banks tend to be limited to urban or highly populated areas.		

2.4 How does Mobile Money Work?

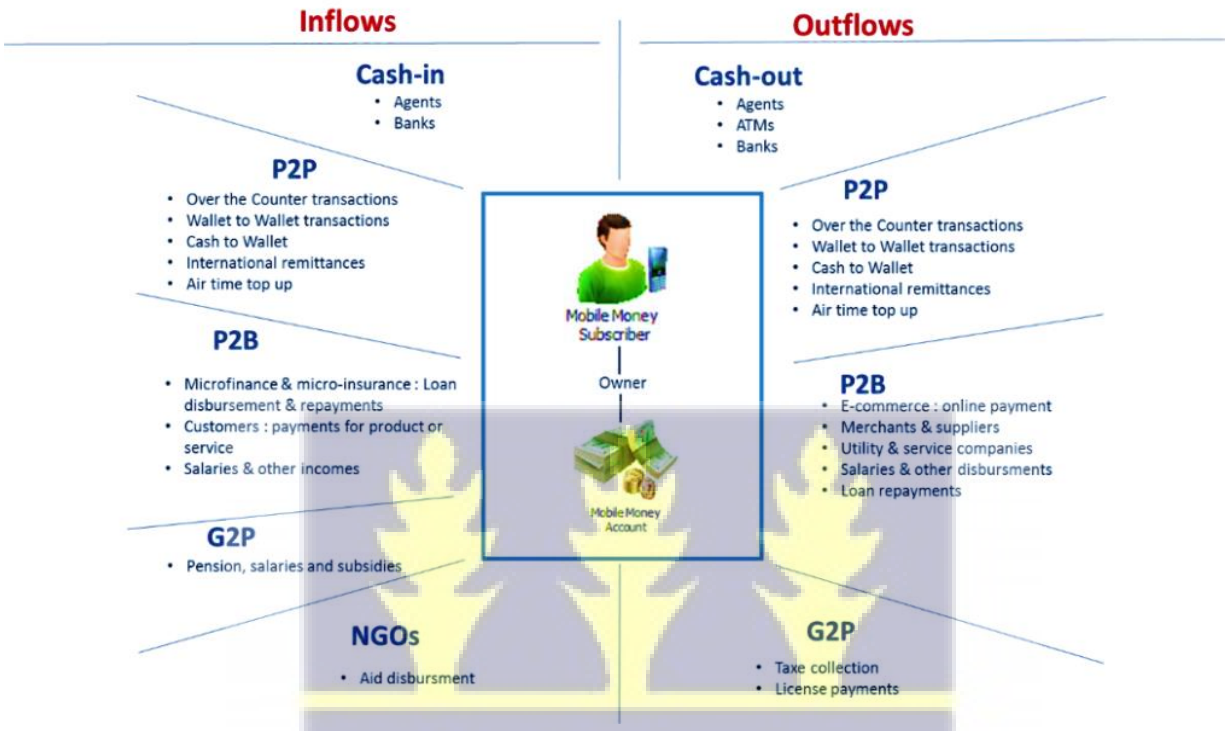
The mobile money service can be completed on any mobile phone device, even for a phone that is least in terms of features and technological advancement. To be able to use the mobile money service, a customer needs to be registered unto the service usually by the aid of an agent (Lake, 2013). The registration process is first and key, as it is part of the requirements usually by regulators, which is referred to as Know Your Customer (KYC) and may vary depending on the country. The process concludes with activation of the service on a person's SIM after completion of the registration process and may involve dialing some specific numbers or short codes to verify the completion of the registration process (Powers, 2022; Purnell, 2022). After the activation of the SIM, the customer generates a personal identification number (PIN) to their account, which is now their "wallet". For a customer to load cash unto their wallet, they would have to visit the network operator's agent or an operators' point of sale. At the agent, they deposit cash and in return gets an electronic money onto their e-wallet (Lake, 2013). The customer immediately receives a notification when the process is completed by the agent as a confirmation to the success of the registration. The message may contain the business registration name of the agent, the balance on the wallet, the date and time of the transaction and the transaction ID, etc. This process averagely may take 3 to 5 minutes, and sometimes less depending on the speed of the agent. This process is termed Cash-In or Deposit (Lake, 2013; Powers, 2022).

To make a withdrawal, the user visits an agent to exchange electronic money for physical cash. The withdrawal process is initiated by the customer on their wallet and then completed by the customer by approving a notification on their phone by entering their secret PIN. This point completes the process of transferring electronic cash from the wallet of the customer unto that of the agent in exchange for cash. This process usually comes with a fee charged on the customer,

and an instant notification on the phones of both the customer and the agent: a process referred to as Cash–Out or Withdrawal (Purnell, 2022). The notification may contain the details of the transaction just as in the Cash In process. The process of mobile money is secured through the customers use of his/her PIN in all transactions except cash deposits or loading electronic money. Some minor weakness includes customer's PIN not being masked and that makes them exposed to the agent or any other person close by when a transaction is going on. Also, this PIN is a four-digit number which can potentially be guessed by using social engineering, especially in situations where users use obvious numbers such as date of birth as their PINs.

2.5 Types and Flows of Transactions

There are several types of transactions that one can perform using their mobile money wallet. The drastic growth of the service has ensured that a host of other institutions have incorporated part of their service unto the mobile money platform, a situation which was not so at the incubation stage of the service. This has helped in the growth of the service making it almost indispensable. The MM service is made up of two broad parts: Cash-In (Inflows) and Cash-Out (Outflows) (INTERPOOL, 2020) as is depicted in figure 2.2 below. The Cash-In part involves a user or customer depositing electronic cash unto their MM wallet typically by visiting an agent. The customer visits an agent who takes the customers physical cash and credit the customers MM wallet. The Cash-Out part on the other hand involves or refers to a customer making a withdrawal from their MM wallet, also typically by visiting an agent. Other aspect of the service also includes Person-to-Person (P2P), Person-to-Business (P2B), Government-to-Person (G2P) among others (INTERPOL, 2020), as depicted in figure 2.2 below.



Cash-In: The process by which a customer credits his account with cash. This is usually via an agent who takes the cash and credits the customer's mobile money account.

Cash-Out: The process by which a customer deducts cash from his mobile money account. This is usually via an agent who gives the customer cash in exchange for a transfer from the customer's mobile money account.

P2B: Person to Business transaction

P2P: Person to Person

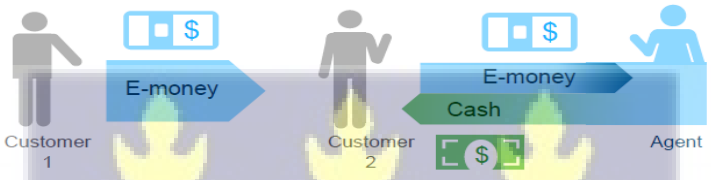
G2P: A payment by a government to a person's mobile money account.

Figure 2.2: Mobile Money Service Outlook

Source: INTERPOL (2020)

Cash–In, Cash–Out, and Person to Person (P2P) is the commonest form of transaction in Sub–Saharan Africa (SSA), the Middle East and North Africa (MENA) regions. There are two main types of P2P transactions. The Wallet–to–Wallet type (Figure 2.3) and Over-the-Counter

Transactions (OTCs). Wallet to Wallet involves a direct transaction between users without an agent. An OTC transaction on the other hand involves an agent where the sender of receiver does a cash transaction with an agent who executes the transaction on behalf of the user (GSMA, 2018; INTERPOL, 2020).

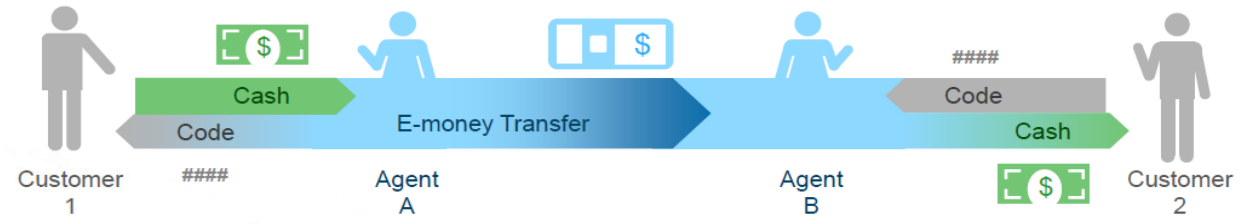


Transfer: Customer 1 sends e-cash from their wallet to customer 2, a service that could be free or attract a minor charge.	Cash-out: Customer 2 receives funds into his/her wallet free of charge. They may choose to keep the E-money or cash it out. To cash-out at an agent the customer pays a fee to the MNO whiles the agent earns a commission

Figure 2.3: Wallet-to-Wallet Transaction
Source: INTERPOL (2020)

The OTC transactions provides good benefits for both a subscriber and nonsubscriber. However, for a customer who many are not able to maneuver the wallet menu interface, it is of greater benefit. In all, there are many forms or types of OTC transactions and that, whichever form or type that is undertaken in any country may be as a result of national legislation.

The figure 2.4 and 2.5 below demonstrate two other forms of OTC transactions.



Cash Payment: Customer 1 gives cash to Agent A and pays a transfer fee after which the Customer then receives a code from Agent A.	Transfer: Agent A transfers the cash to another Agent B, anywhere for "pickup" and gets a commission.	Disbursement: Agent B who receives the transfer is served a code from the recipient (customer 2), gives out cash, and gets a commission	Receipt: Customer 2 picks up cash from Agent B at no fee or cost.

Figure 2.4: Cash to Cash OTC Transaction
Source: INTERPOL (2020)

Cash Payment: Customer 1 goes to agent with cash to either deposit on their wallet or on the wallet of another subscriber and may pay some fee for the service.	Transfer (deposit): Agent A makes a deposit unto the account of customer (Customer 2), using his (Agent) own account	Cash-out: Customer 2 receives funds into their wallet free of charge but pays a fee to withdraw cash from Agent B, who earns a commission.

Figure 2.5: Direct Deposit OTC
Source: INTERPOL (2020)

2.6 Channels to Access Mobile Money

The nature of the MM service platform is one that is driven by a menu and provides the user a number of options based on which they can make a transaction. These platforms are initiated through the use of codes and varies based on the method used to send commands to the servers of the network operators. The use of the USSD accounts for 90% of transactions in Africa hence making it the most dominant on the continent. The use of the USSD have its own characteristics

and advantages as with other channels (TRA India, 2013). Using the USSD appears to be the best option, most convenient and suitable due to it compatibility with almost every kind of phone. It is faster and easier to use compared to sophisticated ones. The use of the USSD is more secure as it's based on session and that at the end of each session, there is no trace of the transaction, as there is no data of the transaction left on the phone after termination of each session (GSMA, 2018). The UUSD is Short Message Service (SMS) based and as such, customers receive an SMS after every transaction. The danger associated with that is when a user's phone ends up in a wrong hand as it may give a full detail of transactions enacted by the owner. However, the use of a PIN for transaction gives some level of security for the owner in the interim. Nonetheless, Kenya's M-Pesa for example has avoided the use of the USSD method and adopted the SIM Tool Kit (STK) method in addition to encrypted SMS (GSMA, 2018). Despite the frailties with the USSD method, Tanzania's M-Pesa was built with the USSD technology as compared to Kenya's STK. MM in Tanzania started a year after Kenya's. Unlike the USSD, the STK technology breaks down the transaction process into bits or a stepwise logic method that allows the users to follow the steps to get a transaction done. Coupled with it not given SMS feedback, it also avoids the use of complex sequences and keywords, although a bit slower (GSMA, 2019). The USSD, regardless, remains the fastest easily suitable for more complex transactions. The use of nickname has also been employed by some of the operators who use the USSD technology, like Airtel Money in place of a mobile number as an indication for the recipient of the transaction. Aside ensuring privacy and security, the use of nicknames can be viewed as a business name, something that becomes easier to memorize (Comviva, 2019). Over time, the mobile money platform has increasingly become more compatible with a number of access platforms or channels. Platforms such as Virtual Imaging Platform (VIP), Wireless Application Protocol (WAP), STK and other mobile applications

(Comviva, 2019). There is a broadening of the scope of the mobile money service due to the adaptability of the service. Before the advent of 3G, GSM networks were well known for the porousness of their security especially in terms of encryption and authentication algorithms (Baraka, 2013). This porousness, as a result of a lack of end-to-end encryption, made information sent through either SMS or USSD vulnerable to interruption. These security issues have been addressed in newer and current generation of mobile phones mostly above the 2G. Even with the associated shortcomings of the 2G technology, 2G mobile phones and technology has well over 50 percent representation in SSA and 0ver 30 percent in the MENA region as of 2018, regardless of the gradual rise in 3G and 4G adoption in these regions (GSMA, 2019)

2.7 Benefits with Mobile Money Service

Recognizing the potential of mobile-based financial services in bridging the financial inclusion gap and promoting good health and well-being, the SDGs are committed to accelerating the adoption and uptake of mobile money. This is due to its potential to increase financial inclusion, root out corruption, mitigate financial risk, and provide economic benefits to individuals and households (GSMA, 2014, 2017, 2018; Mitrega-Niestrój, Puszer, & Szewczyk, 2018).

2.7.1 Help Establish Financial Resilience

Ahmad, Green, and Jiang (2020), opine that m-money can contribute to the economy especially through its impact on financial inclusion. M-money can increase the speed and reduce the cost of payments. It can enhance security by reducing the transport of cash; increase transparency through digital accounting and therefore reduce corruption; and it can provide an entry point into the formal financial system, and so help promote increased saving and self-insurance against small adverse shocks (Demirg¨uc¸-Kunt et al., 2017).

A lot more families who uses mobile money service particularly those in the SSA region a now being able to quickly respond to unforeseen situations due to their access to mobile money: this is a finding that has been established by a number of studies (Demirg¨uc¸-Kunt et al., 2017; Purnell, 2022). Individual family members who use mobile money can rely on quick support by receiving cash from family and friends in situations of negative unexpected events such as death, sudden illness, disasters, accidents, among others, which needs intervention from others. Households are able to send support even when they are geographically far from each other at lower cost and convenience (Purnell, 2022). A study conducted in Kenya using a difference-in-difference technique proved that the ability of households to deal with situations due to access to mobile money was very strong and sizeable. Families that use Kenya's version of mobile money, M-PESA, were far abler to respond quickly to the needs of family members in difficult or negative situations. In addition, these families did not have to adjust their spending on food and other basic needs at the expense of their response to the situation. This is so, primarily due to the fact that mobile money helps in the sharing or risk among the family community regardless of one's location (Van Hove & Dubus, 2019). Each member of the family can send their contribution easily. Other studies have also found, using the same difference-in-difference methodology, that families in Kenya who used the M-PESA were able to still keep up with family spending even when they spent more health-related issues, after examining the effect of mobile money o health shock issues (Van Hove & Dubus, 2019). Contrary though, families who were not using M-PESA had to sacrifice their non-food needs and sometimes the education of their children in order to be able to foot their health expenses. Other studies conducted in Mozambique and Uganda which used a randomized control sample trial produced very similar results (Wieser et al., 2019), and also in

Bangladesh and Tanzania where the difference-in-difference approach and instrumental variable estimation techniques were also used respectively.

2.7.2 MM Improves Savings

With it benefit of facilitating resilience, the mobile money service has the added advantage of encouraging savings from its users (Van Hove & Dubus, 2019; Powers, 2022). A study conducted in Kenya, for example, found that mobile money accounts of women easily although securely, used in the allocation and labelling of money for savings. By identifying or labelling specific accounts in an attempt to encourage women to save with such accounts so they could use it in emergency situations and savings, yielded very positive results (Matheson, 2016; Van Hove & Dubus, 2019). In addition to have a one vs one plans or goals for savings coupled with a weekly reminder on savings goals through SMS resulted in an increase in savings. This accumulated money helped women greatly in their response to unplanned and expected expenditure, making them less reliant on loans and other means or networks for financial support (Matheson, 2016). By using instrumental variables, researchers in Kenya also found that households were able to save more due to the use of mobile money (Gurbuz, 2017). There was between 16 to 20 percent chance that households that used mobile or M-PESA were more likely to save, and their average savings increased by an average of 18% as compared to those who do not use mobile money. This savings amounted to US$2.7 to US$3.7 for each month.

2.7.3 MM Enhances Transparency and Formalization

The system that controls the mobile money service processes is electronic in nature, with the service itself thriving on information. This electronic system takes record of every transaction both to the service provider, the intermediary institutions and the customer. This allows for transparency and an improvement in the security of the service (Purnell, 2022; Matheson, 2016). The transparent

nature of the service allows government and stakeholders to monitor funds transfer, foreign remittances, and all transactions which can improve revenue generation through tax collection. Another advantage of a well-established mobile money economy is that it could help in formalizing the economy (Aron & Muelbauer, 2019), helping in the integration of the informal sector and the unbanked into the financial inclusion agenda of a country. This will help the government greater a stronger link with users by creating social protection schemes, innovative avenues for tax collection, and the execution of other government agenda (INTERPOL, 2020).

2.7.4 Occupation Decision and Long Run MM Effect

The ease and safety of receiving cash through mobile money even from distant social networks by users have been found to greatly influence users and household choices and decisions on employment (Jack & Suri, 2016). By using the difference-to-difference approach, the study conducted in Kenya on the long run effect of M-PESA found that there was considerable change in occupation especially among women to the higher access to mobile money (Voorhies, 2016). Researchers found that an estimated number of about 185,000 women changed their occupation from agriculture to engage in small-scale retail businesses as due primarily to the ease of access of M–PESA (Jack & Suri, 2016; Voorhies, 2016). Although this may not be a positive consequence to the agricultural sector, it provides government new information to take strategic decision for the now and the future. Similar results were found in other jurisdictions, such as Uganda, where the ease of access to mobile money has caused the youth to shift from farm based work to self-employment (Aron & Muelbauer, 2019) and in Mozambique, has also led to significant migration of the youth from rural areas to the urban environment where income levels are higher basically because there is a belief that, after hustling the urban areas, mobile money gives them the opportunity to easily and safely send remittances to their families (Batista & Vicente, 2018). The

latter was because mobile money increased individuals trust that they could easily and safely remit money to their families in the rural areas.

2.7.5 MM Eradicating Poverty among Women

Studies in Kenya have confirmed that access and ease of use of mobile money helped to increase the savings and the per capita consumption of households leading to reduction in poverty. Data presented suggests that this increase in savings and per capita consumption of households helped to move over 196, 000 households out of serious poverty, a number that represent 2 percent of Kenyan households (Jack & Suri, 2016). A follow-up study was conducted in 2014 which assessed the long-term effect for households that, relatively, saw an increase in access to agents between 2008 to 2010. The findings revealed that the impact was largest among families or households whose head was a female, a finding that brings to the fore the amplification of the impact of technology when given to women who were leaders of their households (Mitrega-Niestrój, Puszer, & Szewczyk, 2018). Researchers then asserted that women may enjoy more financial independence, especially in households headed by males and where the females play a secondary supportive role. The number of agents that could be identified in a particular area or community, referred to as agent density, was a major factor to this (Matheson, 2016). The more agents that were available in a specific area, the higher the number of women (study found to be about 3 percent) took up retail business activities instead of farming (Matheson, 2016).

2.7.6 Necessary Requirements for Strong Mobile Money Economy

Having established the importance of mobile money service in both the short term and long term, i.e., its ability in reducing the level of poverty and its ability to reduce the effect of negative situations regardless of the context, there is no argument of it immense benefits. However, having

noted the benefits, these benefits do not come in a vacuum as there are necessary ingredients needed for these benefits to be realized (GSMA, 2013). These may include:

- A strong and well-developed agency networks that will deliver the service such as providing cash out services.
- Easy registration and use of MM technology made simple and trouble-free.
- Investment in infrastructure from the beginning; and
- A strong regulatory body and framework environment to manage the technology.

The beginning phase of mobile money requires that potential users will have access to mobile phones and basic understanding and appreciation of the service and the ability to use the service or product (GSMA, 2013; GSMA, 2018). Before rolling out the service in Mozambique, for example, there was the need for intensive mobilization process which included the dissemination of information to both agents and individuals, a major and important step in ensuring the success of the service.

2.8 Risk and Challenges with the MM Service

The service, after its inception and with all it associated benefits, also have major challenges. After close to two decades of the mobile money service operating on the African continent, the services have achieved tremendous growth as it has become the most popular means of assessing financial services on the continent. Its growth has been exponential and continues to achieve new heights year-on-year. The service however has been bedevilled with several risk factors and challenges that needs immediate attention and solutions. These challenges and risk concerns are now well known (Gaber et al., 2012; Lake, 2013; Otieno et al., 2016) as it has received some attention from academic to practice.

2.8.1 Wrong Transactions

One challenge with the MM service is when an agent or a user makes a transaction to a wrong number and need a reversal of the process to retrieve their monies. If a transaction goes wrong, for example, if a deposit or cash transfer goes to a wrong number, the customer usually has two main options: either to call the receiving number to resend the electronic cash back to you or you call the MNO to take action on the account that received the cash (Muthoni, 2020). This block is, however, only successful when the wrong recipient hasn't withdrawn the money which he/she received. In most cases, the recipient will not retransfer the money back to the sender, so the best option always is to call the service provider (Muthoni, 2020). In a situation where a customer loses their phone or SIM through theft, due to the ability of some thieves or fraudsters to be able to unlock the wallet, the best immediate option is to call the MNOs to take necessary measures. Sometimes this reporting process can be cumbersome as a customer calling a MNO's customer care line may be made to stay on for very long before being attended to. Usually, calls from agents are responded to quicker and so it is best to make an agent call a help line. In some instances, a customer may not even know what to do and that may lose their funds.

2.8.2 Infrastructure Challenges

Setting up mobile money system and infrastructure is capital intensive and requires significant capital investment upfront by the network operator. With the continent having only 25 percent broadband connectivity as at the end of 2018 (World Bank, 2019), there is a serious limitation with the service being able to properly integrate with other digital financial products even right from the beginning. The MM service relies heavily on SMS – based technology making it more difficult in linking mobile money with digital based financial services that relies on the internet (Otieno et al., 2016).

2.8.3 Operational Risks

The risk of operating mobile money is one that really exist, especially on the agent and the customer. As a system, minute loopholes create opportunity for fraud to be perpetrated. Review of literature shows that there is evidence of data breaches due to poor encryption of communication (Otieno et al., 2016; Gaber et al., 2012). This makes operators vulnerable to attackers who may steal valuable data or money from user's accounts.

2.8.4 Regulatory Challenges

Another key area in the mobile money ecosystem is the issue of regulation. One of the major issues with mobile money from the beginning for a number of countries, is which part of the financial space it belongs. Especially as the service or product was the initiative of telecom network whose license do not cover financial activities (Gaber et al., 2012; Lake, 2013). And so, a lot of companies in the private sector and policymakers are still struggling with creating the appropriate regulation for the service (Nyaga & Ogollah, 2015). Designing the appropriate MM platform coupled with linking it with other digitally established identification systems to enable spread of the service to other far places are all hurdles that needs crossing.

2.8.5 Regulating the Mobile Money Service

In Ghana for instance, MTN holds the largest number of money subscribers, followed by Vodafone and then AitelTigo. On regular basis, telecommunication networks send text messages to it customer to be on alert against any fraud attacks. All the networks have been embarking on a campaign to educate the public on mobile money fraud. MTN, given that it has highest number of subscribers, has led the way in sending messages and engaging in public education strategies to reduce mobile money fraud (Tamakloe, 2019) The tremendous rise in mobile money among emerging markets and developing countries has been considered to be the most significant factor

that has contributed to the increase in financial inclusion among countries with emerging markets. The service has opened up the financial space by providing reliable and yet cheap services to the informal and the unbanked. Like the M-PESA in Kenya and Tanzania, such innovative and smart MM services have transformed into major platforms that helps in movement of cash worth billions of dollars every year. However, the MM service, in the past few years have become the major target and channel for fraud and other financial crime activities (Nyaga & Ogollah, 2015).

2.9 Chapter Summary

Chapter two of this study sought to explain the concept of mobile money. In this chapter, various definitions of the mobile money service were given, the key players in the mobile money value chain and their roles. The chapter also spoke on how the mobile money service work and the different forms of transactions that characterize mobile money. The chapter concludes on the nature of mobile devices that can use the mobile money service.

CHAPTER THREE

MOBILE MONEY GROWTH AND THE ISSUE OF FRAUD

3.1 Chapter Overview

As has been noted in the previous chapter, the use of mobile technology for receiving remittance and for business transaction has now become the main driver of economies in developing countries especially, Africa. This chapter on literature review presents the concept and development of mobile money in Africa, on its growth over the years and emerging challenges.

3.2 Overview of Mobile Money in Africa

Globally, remittance through the use of mobile technology and the agenda to ensure a cashless society has already taken center stage, especially among developed economies. Given that emerging economies of sub-Saharan Africa (SSA) lag behind in terms of technological advancement as compared to the West, countries in the SSA region have devised means of ensuring that it citizenry, although they may lag behind technologically, can partake in any form of transactional activity without any hindrance and are also finding ways to use their second and third generations (2G and 3G) mobile phones for financial activities (Bold, Porteous, & Rotman, 2012; Donovan, 2012, Ehrbeck et al., 2012).

The idea of mobile money is no more alien to most countries on the African continent. The concept is very much popular among the citizenry whether they use mobile phones or not, as well as telecommunication networks, experts in software engineers, programmers, technology or even in the academic field (Narteh et al., 2017; Asongu & Asongu, 2018). The popularity of mobile money on the continent is emphasized by The African Report which posited that the mobile money service or product is expected to grow beyond 500 million subscribers in the year 2020. Based on the

report, the services grew by more than 50 million new accounts created on the continent in the year 2019, marking a growth of 12% in the number of registered users from the 2018 figure (Velluet, 2020). Although the adoption of the service was a bit slow at the beginning, studies have suggested that the popularity of the service on the global scale became more evident after the two summits in the years 2008 and 2009 dubbed "Mobile Money Summits" (Suri & Jack, 2016; Maurer, 2015; Gosavi, 2017). With its fast-paced growth on the continent, the service was projected to reach over 450 million users or subscribers by the year 2017. This growth estimation was anticipated alongside transaction value reaching in excess of $721 billion (Shen, 2014). There are currently over 150 services in operation across 72 countries with most of these countries in the SSA region. A region, which in the year 2012, had double the number of mobile money transfer users than holders of Facebook accounts.

3.3 Growth of Mobile Money in SSA

The growth of MM in the SSA region has been tremendous. Available data suggest over 135 different MM implementers were recorded in the year 2017, with accumulated accounts opening of over 338 million (GSMA, 2017). By the end of 2018, SSA alone accounted for more than two thirds of the world's MM transactions with total value in excess of US$25 billion (GSMA, 2019). The mobile money service has been considered to be the most revolutionary technology that has helped in bridging the gap of financial inclusion, making financial services available and accessible in remote regions. Even with the lowest form of mobile phone technology, users are easily and quickly able to send cash or remittances to friends or relatives, or even transact business at almost no or very little cost without the use of a bank account (Parekh & Hare, 2020). One major advantage with mobile money is that people from low resource settings or relatively poor and unbanked population, where usually there is a family and friends support system even when they

are far from each other, enjoys the benefit of this technology most (Nevin & Omosomi, 2019). In the year 2018, SSA alone received remittances in excess of US$48 billion. Nigeria alone accounted for more than 50% of the total SSA remittances received in that year, with a record US$25 billion (Cooper & Esser, 2019). To put it in perspective, this amount injected into the Nigerian economy was almost four times more than the combined total of revenues received from foreign direct investment (FDI) and official development assistance (Nevin & Omosomi, 2019). Before the advent of mobile money in SSA, families and friends devised ingenious ways of sending cash support to their relatives. Some sent money through bus drivers, passengers traveling their route, or some even hid them in foodstuffs or goods to be retrieved upon delivery. This was the case for countries such as Kenya, Nigeria, Ghana, etc. putting away the issue of insecurity, these processes were also costly and caused serious delays (GSMA, 2013). The anxiety associated with the process, as to whether the money will reach the said destination, was demining enough. This situation is now a thing of the past as mobile money has provided the needed solution.

3.4 Mobile Money Service in Ghana

The year 2021 marks 15years since M-Pesa was launched in Kenya. The mobile money industry then was only hoping to make improvement with time. To the dismay of many, the industry has now made great strides with more than half a billion mobile money accounts registered by the end of 2016, with global reach of over 170 million active accounts holders (GSMA, 2016). The advent of mobile money has bridged the gap between financial service delivery and the unbanked populace. Going beyond this process of financial inclusion by reaching the unbanked, mobile money, according to the GSMA 2016 report, contributes to 11 of the 17 United Nations Sustainable Development Goals. Through this, the service has reduced the inequality that existed between the haves and the have nots, by creating the enabling grounds for households to lift themselves out of

poverty and empowering the underserved segments of the population. In addition, mobile money has become one of the main drivers of economic growth in emerging markets or growing economies, mainly through the formalization of payments, delivering transparency, and boosting the flow of money throughout economies. Digital finance, including mobile financial services, is projected to have the potential of adding US$3.7 trillion in various economic activities annually by the end of 2025 (AFI, 2016).

The impact of mobile money on the Ghanaian financial space is no different from the global experience. In 2016, the Bank of Ghana reported that the service had a growth rate of 737.4 percent between the years 2012 to 2016, in terms of the volume of registered mobile money transactions (Diniz, Albuquerque & Cernev, 2014).

In Ghana just like other jurisdictions, the main use of mobile money is to transfer value from one person to another person (P2P), for payment of goods and services such as buying airtime, paying for utility bills, Gold and DSTV bills, salaries of some workers, taxi fares, micro-credit, savings and micro-insurance. The ability of the MM platform to store money has led to the quarterly payments of interest on these floats. Total float balance was GH¢1,257.40 million at the end of December 2016 compared to a float balance of GH¢547.96 million at the end of December, 2015, reflecting a growth of 129.5 per cent (Bank of Ghana, 2016). Total interest paid to holders of electronic money wallets in 2016 amounted to GH¢24.79 million (Bank of Ghana, 2017). This payment of interest has certainly even made the service more attractive. In 2016, BoG gave approval for four (4) electronic- money issuers' modalities for the payment of interest on float accounts to electronic money holders. Total interest paid to holders of electronic money wallets in 2016 was GH¢24.79 million. This was the first time in 2016 that interest on mobile money float were distributed successfully since its inception in 2009. This was in accordance with paragraph

10(5) of the Electronic Money Issuers Guidelines (2015) (Bank of Ghana, 2016). Various reports have been quite clear on the impact mobile money has had on national and global economies. Future projections have made the prospect of mobile money and mobile financial services even more appealing with projections exceeding $3.7 trillion to the global economy. When mobile money was first introduced in Ghana in 2009, it took a while to gain much traction as compared to other African countries due to the Bank of Ghana's restrictive 2008 Branchless Banking Guidelines. Five years later, however, the bank of Ghana revised 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 (Bank of Ghana, 2016). Shortly after, new players like the telecommunication giant MTN began heavily investing in creating awareness, educating customers and recruiting agents and merchants. According to a Summary of Economic and Financial Data published by the Bank of Ghana in March this year, there are now 14.7 million active mobile money accounts and 235, 000 active agents.

3.4.1 MM Service Providers in Ghana

Between 3 to 4 million Ghanaians living in the diaspora are estimated to be sending remittances back home through mobile money (Nicco–Annan, 2020). Currently, one of the easiest platforms that thrives on mobile money to send remittances to families back home from across the world is WroldRemit. As has been stated, a 2019 World Bank report described Ghana as the country with the fastest growing mobile money economy. According to the Ghana Interbank Payment and Settlement Systems (GhIPSS), after the introduction of Mobile Money Interoperability (MMI) in 2019, it grew by 358% in the first quarter of 2020 (GhIPSS Report, 2020). Due to the convenience that comes with the mobile money service, subscribers visit to commercial banks have been

reduced, thereby doing away with long queues at commercial banks. It has provided job opportunities for numerous youths who work with service providers as agents and has aided the financial inclusion agenda across a number of African countries.

3.4.2 MTN Mobile Money

Mobile Telecommunication Network (MTN) being the largest communication service provider in Ghana, was the first to introduce mobile money into Ghana and operates the largest mobile money service called MoMo, in Ghana (Nicco–Annan, 2020). With their slogan or tagline, "Everywhere You Go", it is the only communication service provider that has the widest reach in the country, priding itself as being almost everywhere in the country. The popularity of mobile money in Ghana is entirely as a result of the work done by MTN, now bosting of over 23 million voice subscribers amounting to 57% of the market share (Paul, 2020). The service provider has also partnered with a host of remittance business such as WorldRemit which helps any subscriber to receive foreign remittance directly unto their phones, anywhere in Ghana (Nicco–Annan, 2020). To register for MTN mobile money in Ghana, all that a customer needs to do is to take any of their national IDs: Ghana Card (ECOWAS Card), Voter ID, Driver's License or Passport to any MTN mobile money agent who will take them through the registration process. After capturing the data of the customer, the customer will receive a message alert on their phone confirming the success of their registration or otherwise.

There are some advantages that a person gets when he/she subscribes to MTN (Paul, 2020; WorldRemit, 2022):

- The company has kept true to their slogan "Everywhere You Go" and so with their numerous agents scattered across the country, it is much easier to perform a transaction

anywhere and everywhere. In Ghana, it is not a strange to locate an agent just by walking about 100 meters or even less.

- Secondly, the brand MTN is widely recognized and has public appeal among Ghanaians. It has enjoyed some goodwill from the people of Ghana as it is now so difficult meet a Ghanaian who doesn't use MTN.
- MTN has strong global partnerships that makes sending and receiving money across the world much easier as compared to other service providers.

On the other hand, due to the large number of people hooked unto the network, any break in the service affects large section of the population and can bring a lot of services to a standstill. This can be very frustrating leading to customers having other service providers as their second option.

3.4.3 Vodafone Cash

Aside MTN, Vodafone cash, the mobile money service provided by Vodafone Ghana is the second fastest growing mobile money service in Ghana. Launched in 2015 (Paul, 2020), almost a decade after MoMo was introduced by MTN, Vodafone Cash has introduced various incentives that have made their service more attractive. Although it doesn't have the widest reach in the country, it commands over 21% of the market share (Paul, 2020) and prides itself as being the only service provider that charges absolutely no cost and any transfer, whether from Vodafone number to another Vodafone number, or from Vodafone to any other network. This incentive has gained traction in the Ghanaian mobile money ecosystem, causing a rapid growth in the number of subscribers unto the service, as sometimes the charges with MTN mobile money can be a little expensive (Gujral, 2020). The service currently has a little over 2 million subscribers and has good presence in some rural areas. By introducing other addon initiative such as their Farmers Club, the

service has good appeal among some rural folks. Using Vodafone cash comes with some benefits such as (Gujral, 2020)

- No charges on transfers of any amount for as many times as one wants to all networks.
- All transactions are initiated by the subscriber alone and so nobody can have access to subscribers' number or accounts information.
- As with MoMo, Vodafone Cash allows subscribers to pay all utility bills, school fees, broadband services, etc, using their Vodafone wallet.

The service is however challenged with poor network service in rural areas or remote towns leading to customer complaints.

3.4.4 AirtelTigo Money

The final mobile money service provider in Ghana is the AirtelTigo Money. AirtelTigo was formed in 2017 by two communication service network providers Airtel and Tigo. The two companies, in the year 2017, joined to become one network called AirtelTigo (Nicco–Annan, 2020). Before their merger, the two companies operated separate mobile money services, Tigo Cash and Airtel Money, which after their merger came together to form AirtelTigo Money. Compared to MTN and Vodafone, AirtelTigo enjoys a little over 20% of the market share (Paul, 2020), and has over 2000 network locations and more than 400 retail points all over Ghana. The network provides a number of services.

AirtelTigo provides certain benefits for its customers which includes (Nicco-Annan, 2020)

- Subscribers on the network can send money to friends and family on the AirtelTigo network free of charge.

- Customers sending Ghc 100 (US$17) from their AirtelTigo wallets to other networks will also not pay any charges.
- New subscribers can register AirtelTigo Money via their WhatsApp line.
- Receiving foreign remittance to the tune of GHc500 or more comes with free international calls to the customer (Nicco-Annan, 2020)

Using the service also comes with its own challenges.

- Challenges with service networks in remote areas
- Less popular and so less public appeal

3.5 Mobile Money Fraud

There is no denying the fact that the mobile money service has security features that are questionable and hence have created loopholes in the system. These loopholes coupled with poor level of knowledge among users of the service has opened opportunity for cybercriminals and criminals (Gilman & Joyce, 2021; Akomea-Frimpong et al., 2020) of all types to have a fill day to perpetrate their crimes, causing subscribers to lose millions of monies and creating a disincentive in getting the unbanked and those excluded from financial services to get access into the FinTech community (Botchey et al., 2020). There is a general lack of research into mobile money fraud, partly because systems for detecting such frauds are unavailable or yet to be developed as this technology is quite new to the Western World. Being able to detect mobile money fraud has become a huge task (Botchey et al., 2020).

There are a number of fraud categories that have been identified in the MM ecosystem which includes: Agents and Third-Party Fraud on Customers and Fraud against Agents. These fraud

issues have caused significant losses in the sector both for the agents and users (Gilman & Joyce, 2021). The number of people affected with these fraud situations is markedly high and has caused significant economic losses. There could be a potential reduction in subscription and continuous usage of the service as result of fear or having actual experiences with the increasing cases of fraud associated with it (Akomea-Frimpong et al., 2020). Such situation may have rippling effect on other riskier and more complex nonpayment services. Inability of stakeholders to clump down on the issue of fraud, whether internal or external, can cause a reduction in the perceived benefits that customers enjoy and badly affect the major strides made in the financial inclusion agenda (Rao & Vasudevan, 2021). Furthermore, the issue of fraud can also affect the confidence of regulators in allowing more space for further innovative services that could be added to the mobile money service due to a potential lack of trust in the control measures put in place by service providers to mitigate the risk of fraud (Akomea-Frimpong et al.,2020; Gilman & Joyce, 2021). It is therefore important for service providers to put in place appropriate control measures that will ensure a balance between managing risk and other business objectives.

A comprehensive study was conducted by CGAP in the year 2015 on the issue of mobile money fraud among six leading mobile money markets in the world: Ghana, Kenya, Pakistan, Rwanda, Tanzania, and Uganda. The study examined the issue of reported fraud from customers as well as other key industry stakeholders and made the following recommendation: there is the need to begin engaging policy makers and very key risk issues related to the service and it relevant policy responses; putting in place mapping strategies for good practices in detecting and mitigating fraud attacks; and organizing workshops and training for industry and its agents, and the government regulatory bodies on the current fraud issues (CGAP, 2015). This can be done also by collaborating

with the global mobile industry association, the Global System for Mobile Communication Association (GSMA).

3.5.1 MM Fraud Situation in Kenya

The east African country, Kenya, is credited as being the first country in the sub region with the initiative of mobile money, with a popular name M–Pesa as stated earlier. Users of M–Pesa have been experiencing issues of fraud with individuals giving their accounts of scams perpetrated on their wallets which has been widely reported in the country (Gilbert, 2021).

In a story published by BBC Africa, an M–Pesa user shared his experience of losing his SIM card entirely. He claimed of receiving a message via text, suggesting that his SIM card was been swapped and that he was required to send his personal code although he had not asked for a new SIM card or had not called Safaricom's customer help line to make any complaint (BBC Africa, 2018). However, earlier, he had received a call but immediately terminated it. After receiving the text from his service providers, he figured out that the earlier call he terminated must have been an attempted fraud, as the caller posed himself as a customer service representative from Safaricom (Safaricom, 2022). According to him, "it was a brief call, and I did not give any of my details" and called Safaricom immediately to inform them of his suspicion that a fraud attempt was being made on his number. Sammy claimed, that although he did not give out any details to the caller and even went ahead to report the incident to Safaricom, he still lost his number and account until after three days. He shared the whole experience in a tweet a summarized in figure 3.1 below:

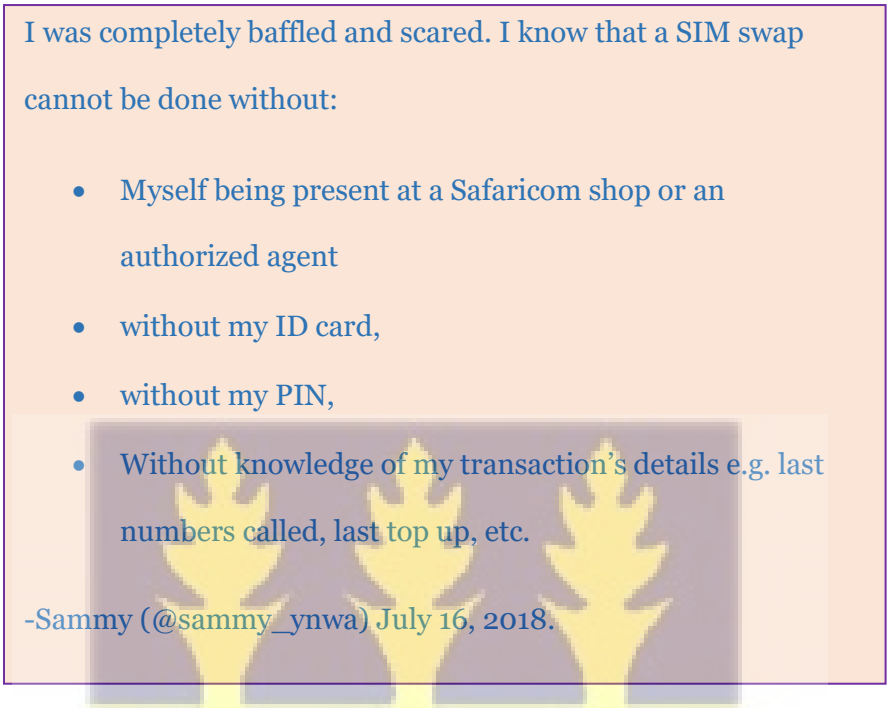


Figure 3.1: A victim sharing their story on twitter

Source: Author's Creation

The situation in Kenya is not very surprising, as globally, it is the country in the lead with the largest number of mobile money subscribers (Boston Consulting Group, 2020). The country with a population above 47 million has almost half of its population using the M-Pesa to transact business or pay for nay service. With such large numbers, issues of SIM fraud could be rampant causing public consternation. Mobile money service providers in Kenya haven been able to form partnerships with institutions such as banks, insurance firms, which has given customers the opportunity to transfer money into their bank accounts from their wallet and vice versa. According to William Makatiani, an expert from Serianu, a consulting firm in the cyber security space, incidence of mobile money scam has become more common now and will keep rising.

3.5.2 MM Fraud Situation in Uganda

Uganda is one other country which has sustained a substantial shock to it mobile money ecosystem quite recently (Aheebwa, 2022). After a security breach on the systems used by a consumer finance aggregation firm, Pegasus Technologies, the whole of Uganda's mobile money sector came to a halt as the country's telecommunication and banking sectors were thrown into utter confusion. The attack on Pegasus Technologies, according to MTN Uganda caused a total loss of $3.3 million as the situation affected bank to wallet transfers (Kafeero, 2020). Pegasus Technologies owns the right to provide bills and other financial solutions to a number of firms. Based on reports by local news outlets, the perpetrators orchestrated the act by using over 2,000 SIM cards to gain access into the system that manages mobile money in Uganda. After hacking into the Pegasus Technology system, they issued instructions to the banks to make transfers amounting to several millions of dollars to telecommunication companies who later transferred these unto the over 2,000 SIM cards all over the country (Kafeero, 2020). After what was described in joint statement as an "unprecedented technical challenge" by the two telecom giants of Uganda, MTN and Airtel, mobile money service was completely suspended indefinitely.

As the mobile money service has been growing in Uganda, a barrage of attacks is to be expected. Data from the Bank of Uganda revealed that, in the year 2019 alone, transactions worth over $20 billion was conducted through the mobile money system (Aheebwa, 2022). MTN Uganda commands the lion share of the country's total subscriber base, with over 80% of the total number of subscribers. This percentage translate into over 11 million subscribers for MTN alone. MTN Uganda insist that only mobile money service that passes through Stanbic Bank of Uganda, Sendwave and MTN to Airtel transactions. Sendwave, for example, is a payment service provider that has operations in six other African countries namely Ghana, Uganda, Tanzania, Kenya,

Nigeria, Liberia and Senegal (Sendwave, 2022). As a result of this MTN Uganda performed an upgrade on their system, during which all data, voice and mobile money services suffered hiccups. Afterwards, customers were assured by the affected banks and telecoms that their account balances were still intact and were assured of improved security and better service provision (Kafeero, 2020). Stanbic Bank Uganda, in response, has also suspended all transactions the happens between the telecom companies and the commercial banks.

Uganda has a vast majority of its citizens not having official bank accounts and as a result, the convenience of mobile money service has been a great tool helping the unbanked and rural dwellers accessing financial services at a very low cost (Aheebwa, 2022). The service is used in almost every sector of the country's economy and in some rural areas, the only available option to send and receive money. According to annual Ugandan Police Crime and Road Safety report of 2019, the country lost over 41 billion Ugandan Shillings or $11 million due to cybercriminal activities such as SIM Card Swapping and hacking of digital financial accounts (Kafeero, 2020).

3.5.3 MM Fraud Situation in Zambia

Issues of mobile money fraud in Zambia has also been widely reported with the menace constantly on the rise (Nyambe, 2022). There are constant reports of people receiving messages purported to be coming from the MNO which later turns out to be fraud attacks. A victim sharing her ordeal claimed she received a text message on her phone that read "I'm requesting you to send that money in this number" with a phone number added to the message. After she speaking to her son and telling him that she will be sending her some money, Mulenga quickly assumed the message was from her son directing her on which specific number she should send the money to. She later sent 2,000 Zambia kwachas (about $168) to the said number. She later discovered that the message was from fraudsters as the money never got to her son (Phiri, 2019). Although she reported the incident

to the police, the fraudster could not be traced as the mobile number was no longer active (Phiri, 2019). There is no denying the fact that mobile money has now become a major player in the financial space on the African continent and has become a major revenue stream for telecoms that provide the service (Nyambe, 2022). According to the 2017 GSMA report, sponsored by Bill & Melinda Gates Foundation, there were more than 338 million registered MM accounts across SSA (GSMA, 2017). This figure is a substantial rise from the previous year, where 286 million accounts were registered, representing 17.13% increase. SSA had a total transaction value a little less of $20 billion (GSMA, 2017). According to the Bank of Zambia, there was 67.5% rise in the volume of mobile money transactions in the year 2017 alone (Phiri, 2019; Gilbert, 2021). In terms of value, this percentage translated to approximately 7.3 billion kwachas (about $612), which is double the figure recorded for 2016 (Phiri, 2019). With such tremendous growth, it is not surprising that the sector has become the prime target for criminals, and expert opinions suggests that crimes such as scams that targets individuals who uses their SIM cards to perform a transaction has gone up greatly. The Zambia Information and Communication Authority has been issuing warnings to mobile money users to desist from sharing personal information or their contacts on social media sites and endeavor not to share their PINs with anyone. After suffering a scam, one Richard Sakala claimed:

> "*I concluded that the thieves are just using psychology, because they know that at one point or another someone might be sending money".*

Although he still uses the service as it has almost become a habit for him, plus the convenience the service brings:

> *"I still use it despite losing such a large amount", says Mulenga, the woman who meant to send money to her son. "I am just more careful now"* (Phiri, 2019).

3.5.4 MM Fraud Situation in South Africa

Loses in Africa in relation to mobile money, according to Evina, an anti-fraud firm based in Paris, is certainly set to go up beyond the $4 billion recorded in 2020 to $5 billion by the end of 2021 if proper measures are not put in place to effectively deal with the looting of the continent through the virtual scramble for the continent (Gilbert, 2021; Businesstech, 2021). With the apparent gap in infrastructure and social amenities on the continent, activities of such nature continue to leave the continent in tatters. According to Lofti, CEO of Evina, as reported by Businesstech (2021), there are two main forms of mobile money fraud that is currently impacting the service:

- Clickjacking: This technique involves a fraudster intercepting a legitimate click by the mobile money user, where unknowingly to him/her, redirects them to a different website where important information about their financial details could be stolen.

- Malicious Apps: These are apps specially designed with malware embedded in them. As a user downloads or updates the apps on their phones, the app gathers and sends sensitive information to fraudsters at a separate source where the information is used to defraud the user.

Evina posits that, with fraud rate of about 27% happening in the Middle East and African Regions, 60% of this fraud rate is attributed to clickjacking whilst malicious applications accounting for 19% (Businesstech, 2021). Clickjacking, he claimed, has existed for a while and is a very basic form of fraud, whereas the malicious app technique is rather a more refined form of fraud being perpetrated. In South Africa for example, one out of three mobile money subscription is for fraudulent purposes. According to him, the tools needed to combat these crimes are already

available to us. By using the same tools which we already use to protect millions of mobile money users across the world, these fraudsters can be stopped (Businesstech, 2021).

3.6 Types/Categories of Mobile Money Fraud

The nature of mobile money service and it risk factor characteristics, makes the type of fraud that has bedeviled the service quite different from that which is experienced by banks. Overall, all types of fraud perpetrated with mobile money impact three main groups: Service Providers, Agents and Subscribers/Consumers (Subex, 2017). Various forms of fraud have been perpetrated against the mobile money service since it was first introduced. These fraud activities have been orchestrated by cybercriminals or individuals with the sole purpose of looting monies from people's accounts, thereby derailing the confidence users have in the service. These scammers engage in such acts in order to gain excessive advantage of all the stakeholders in the mobile money value chain: mobile money service providers, agents and subscribers (Merritt, 2011; Subex, 2017). Scammers invest a lot of planning into such acts and sometimes gets support from cartels across the world with the purpose of enriching themselves. They take a long time to plan, by critically observing the system with technical assistance either from themselves or some fraud cartel and try to identify loopholes that they can take advantage of (Maurer, 2012). Three main types or categories of mobile money fraud has been established by literature:

3.6.1 Subscriber or Customer-Affecting Fraud

Subscriber or Consumer-affecting fraud is the type of fraud that has the consumer as the main target. It is a very broad category of fraud with different variations and differs with regards to the market. Users or subscribers of a particular network or mobile service provider, usually register their SIM cards to be able to use mobile money service offered by their network. They are taken through registration processes where they are asked to provide certain information before they can

be registered. In Ghana for example, the first critical requirement is that a person who wishes to register must have been 18 years or older. However, there are some who also register unto the service with the aim of duping or deceiving other subscribers to steal money from them. This is the commonest form of mobile money fraud especially in Ghana (Akomea–Frimpong, 2020). Fraudsters who have subscribed to the service use all manner of strategies to deceptively get their subjects to initiate certain procedures that will help them get access to their accounts or falsely but smartly deceive them into making certain transfers to them. Almost 50% of subscribers may have been subjected to these deceptions. They manipulate people to get their SIM cards, PINs, mobile money codes and other important information that they can use to steal money from subscribers (Akomea-Frimpong, 2020).

In Uganda and Rwanda for example, the topmost consumer-affecting fraud they face have been listed as follows.

- There is Identity theft which rises out of fraudulent SIM swaps used in transferring data and information from the SIM wallet of the subscriber unto the SIM wallet of the fraudster which gives the fraudster access to the wallet and the bank account details of the customer.
- The use of scams through social engineering, false promotions, service provider impersonation and phishing. Fraudsters pose themselves as though they are employees of the mobile money service provider and tells customers that they are prize winners of some promotion, and so for customers to redeem their prize, they need to make some cash payment through transfer unto a number given to them by the fraudster.

- The problem of network down time. A situation that gives fraud perpetrators the opportunity to engage in over-the-counter transactions and offline SIM swaps, can only be reconciled through verification only after there has been network reconnection.

- Customer PINs ending up with Agents. These may not always lead to fraud as it may not have been done with such intent. However, it still leaves customers or subscribers exposed to potential fraud risks.

- Agents perpetrating OTC fraud on Customers. This may happen when, for example, agents overcharge customers for direct deposit transactions or may take fees or charges for services that must be free of charge.

- There are also losses that happen as a result of transfers sent to wrong people who may refuse sending it back or refunding the money.

Available data suggest that the commonest fraud concern raised among the above listed is agents asking for customers PINs, although, this may have been done initially without the intent of fraud. The second on the list are cases of overcharging by agents for direct deposit transactions or charging for typically free services. However, interestingly, network down time was the topmost concern of customers, and was reported by over 50% of customers who were sampled. It was also interesting to further note that, regardless of the numerous challenges that customers faced, only 11 percent of these issues were formally reported to the service providers or the police. This was mainly due to the fact that customers had no idea or information on what to do or where to formally report such incidents, and also due to the ineffectiveness of the resource channels provided by the service provider. Wallet-based customers have been identified to make more official complaints through formal complaint channels as compared to OTC customers (Mazer & Garg, 2015). Lack

of reporting by customers poses a challenge in gathering accurate data in fighting the perpetrators of fraud crimes.

3.6.2 Employee and Agents Fraud

The second category of fraud is the Agent-Affecting Fraud. there are specific frauds that are targeted at agents, making them also vulnerable. In an Agent Network Accelerator Survey conducted by Helix Institute of Digital Finance revealed that more than 50% of mobile money agents in Uganda, and over 40% in Tanzania have had a fraud experience within the past 12 months (Bersudskaya, Khan, & Kuijper, 2016). Agents in Uganda recorded the highest rate of fraud in the East African region (Bersudskaya et al., 2016). In Ghana for example, there are over 240,000 registered mobile money agents scattered across the country. Unfortunately, some of these agents in connection with some employees of the mobile money service providers also engage in some fraudulent activities. These employees work in hand with some agents sometimes to dupe customers or to create dummy accounts and PINs or passwords which they use to transfer monies to enrich themselves. In 2017, for example, mobile money service providers initiated the arrest and prosecution of over 3,000 agents who connived with some subscribers and employees to rob mobile money operators and some customers of huge sums of monies (Mustapha, 2017). Some employees have also been implicated as they worked with some agents to dupe customers. Such incidences occur due to poor internal control measures and porousness in the system (Mustapha, 2017).

The most common fraud that affected agents was the loss of float from the account of the agent due to unauthorized use from someone or scams through MM service provider staff impersonation by fraudsters through which they get access into float accounts of agents. Sometimes, agents suffer fraud from customers as well, such as, withdrawal reversal fraud or the use of fake currencies to

make deposits. The survey revealed that fraud was the primary concern for most agents in the East African mobile money market as is depicted in figure 3.2 below:

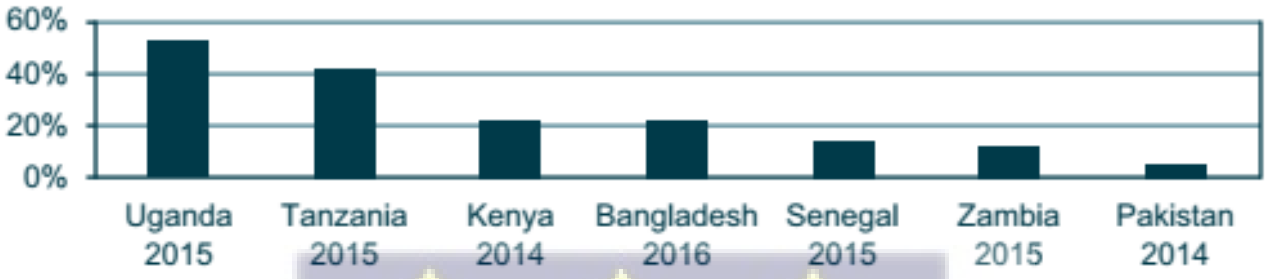


Figure 3.2: Percentage of Agents who have suffered fraud in the past year
Source: Bersudskaya et al. (2016).

3.6.3 Systems/Internal Fraud

The third category is fraud orchestrated and perpetrated by insiders within the MNO company. Such fraud cases usually result in much more significant financial losses for the service providers. It further disrupts customer or subscriber confidence as they will feel at risk of losing their monies, thereby putting the service provider's financial integrity into disrepute. It is reported, for example, that MTN which is one of the largest telecom companies operating in Africa and by far the largest operator of mobile money service in Uganda, lost over US$3.4 million as a result of fraud by an employee in 2011 (Morawczynski, 2015). In Rwanda, a neighbor to Uganda, similar fraud case was recorded with telecommunication company Tigo of which the company lost US$700,000 as a result in the year 2014 (Mugisha & Ainembabazi, 2014). The problem of internal fraud could be attributed to a number of factors such as a lack of adequate internal controls that creates loopholes for data hacking, lack of adequate audit processes, poor corporate governance structures, lack of whistle blowing mechanisms, among others.

Operating mobile money service requires the installation and use of advanced technology that will ensure smooth coordination and security of the process. There are more complex algorithms that are available to mobile service operators to perform a variety of activities, however such systems

are mostly expensive. Modern day cybercriminals operating the cyberspace are very sophisticated and have support from international cartels who provide financing and the technical expertise for these fraudsters to perpetrate their act. Machines with the highest form of security features require huge capital injection making it affordability difficult for some MNO. Some service providers may have outmoded machines which cannot compete with the sophisticated nature of the mobile money service (Vlcek, 2011).

3.6.4 Mobile Money Fraud in Ghana

The issue of MM fraud is not new in Ghana anymore. Annan (2017) provided a list of the types of MM fraud currently being perpetrated in the country.

1. Anonymous calls and text messages from fraudsters: Subscribers usually receive calls or text messages from strange or anonymous numbers who are usually fraudsters claiming to have wrongfully sent or deposited money to the wallet of the subscriber which needs to be sent back to them. These claims are usually false when the recipient of the call checks their account balance. They may try to manipulate the subscribers by claiming to assist them reverse the transaction.
2. False promotion: Some subscribers are also duped by fraudsters who call to deceive them of winning some form of promotion from their network provider. For the subscriber to redeem their promotion prize, they may have to transfer certain amounts of money to some numbers, which later turn out to be false. Fraudsters also send fake text messages that may be generated by a computer to agents and so may seem true. Agents are sometimes instructed by the text message to initiate certain transaction processes which may lead them into making transfers that later turns out to be false (Provencal, 2017).

3. Scam: In some instances, fraudsters call subscribers and pretend to have received some funds or goods from overseas and so the subscriber would have to send them money before the goods can be delivered to them. Sometimes they demand for specific amounts as charges to be sent to some different number to retrieve the goods from relatives of friends who live in the US or Europe or some foreign country.
4. False Cash Out SMS: In other cases, mobile money merchants may receive messages asking them to authorize a transaction of which the physical cash is issued by the merchant to the fraudster without the equivalent e-cash (Provencal, 2017).

3.7 MM Fraud Risk Factors and Vulnerabilities

To be able to find the appropriate measures in curbing the issue of fraud, it is most important to establish the various risk factors, which either alone or put together, makes the MM service liable and susceptible to fraudulent act or money laundering. By establishing this, it is also important to define and properly analyze the types of fraud associated with the service (Buku & Mazer, 2017). Extant literature has identified the following indicators and risk factors:

3.7.1 Product Risk

The mobile money service is one that thrives on speed, convenience, security and portability, making the service a far more preferred option compared to the bank in developing countries (Estrin, Pelletier, & Khavul, 2019). However, by these same qualities, the service becomes liable or easy target for scammers and fraudsters as it has almost no checks and balances compared to the service provided by traditional banks hence making the service porous. By incorporating a lot more products to that originally provided by service providers such as insurance, mobile savings, bank to wallet transfers and international remittances, the service becomes more exposed to attacks (Cassara, 2019).

3.7.2 Channel Risk

The channel through which the mobile money service is executed also provide some risk to the stakeholders. One of the critical elements of mobile network operation is the fact that it is ubiquitous; the same critical factor that the mobile money service rides on (Transparency International, 2018; Estrin et al., 2019). This leaves almost no room for piloting for new and inexperienced service providers who want to enter into the mobile money market using this channel.

3.7.3 Agent Risk

The use of agents also serves the service provider and the subscriber some risk. Having a large agent base makes it almost impossible to establish infrastructure for proper supervision and oversight to ensure compliance with laid down procedures especially in rural areas (Estrin et al., 2019). Even in the cities, absolute monitoring and evaluation is almost impossible.

3.7.4 Customer and Compliance Risk

Unlike in the west, a host of countries where mobile money service has become the easiest tool towards financial inclusion have large part of its population either unbanked or illiterate (Transparency International, 2018; Cassara, 2019). There are poor identification systems that makes it difficult to ensure proper Know Your Customer (KYC) due diligence is followed to the later. This makes it difficult to track criminal activities or even get reliable data for strategic security planning.

3.7.5 System and Delivery Risk

Delays caused by system down times provide fraud opportunities (Cassara, 2019). There is the potential for individuals having system access rights to abuse them especially when there aren't enough checks and control mechanisms. Being able to establish a comprehensive transaction

monitoring mechanism may border on the service provider's ability to put in place an automated fraud management system that can screen transaction activities to detect fraud (Cassara, 2019).

3.7.6 Regulatory, Supervision, and Enforcement Risk

In markets where there is no proper laid down regulations that cover mobile money operations, there is the potential for this leading unauthorized activities or proliferation of unrelated mobile money products or unlicensed agencies who will provide such services. Such situation can be good breeding ground for cybercriminal activities such as fraud, money laundering and other crimes (Transparency International, 2018).

3.7.7 Customer Protection with The Use of MM

Consumer protection can be defined as the practice of ensuring the safety of buyer's commodities whether goods or services, and the entire public against inimical activities in the marketplace (Bongomin & Ntayi, 2020). Usually established by laws, the aim of these protective measures is to counter and possibly prevent business owners to engage in practices specified by these laws, with the aim of misleading the customer or gain undue advantage in the market over their competitors (Bongomin & Ntayi, 2020).

Three main dimensions of customer protection has been established when it comes to mobile money (GSMA, 2016; Ramos et al., 2016):

- Basic protection rules
- Ensuring safety of customers' funds
- Deposit Insurance of Customers

The basic rules of protection chiefly ensure transparency in relation to (Ramos et al., 2016):

a) Service Prices

b) Ensuring customers have access to the terms of the service and

c) Making available avenues for dispute resolution.

It is also worth noting that each region or country has its own approach to protection and so there exist some variations. Available data suggest a wide gap between the level of protection enjoyed by the users of mobile money service in one country compared to another country. Based on the criteria listed previously, Figure 3.3 below according to INTERPOL (2020) provides a pictorial view of the level of protection enjoyed by customers within specific regions: Central African Police Chiefs' Committee Organisation (CAPCCO), Southern African Regional Police Chiefs' Cooperation Organisation (SARPCCO), Eastern African Police Chiefs Cooperation Organisation (EAPCCO), North Africa and West African Police Chiefs Committee (WAPCCO). Member countries in the SARPCCO are lacking grossly when it comes to basic rules of protection for mobile money services users, with some other regions being better.

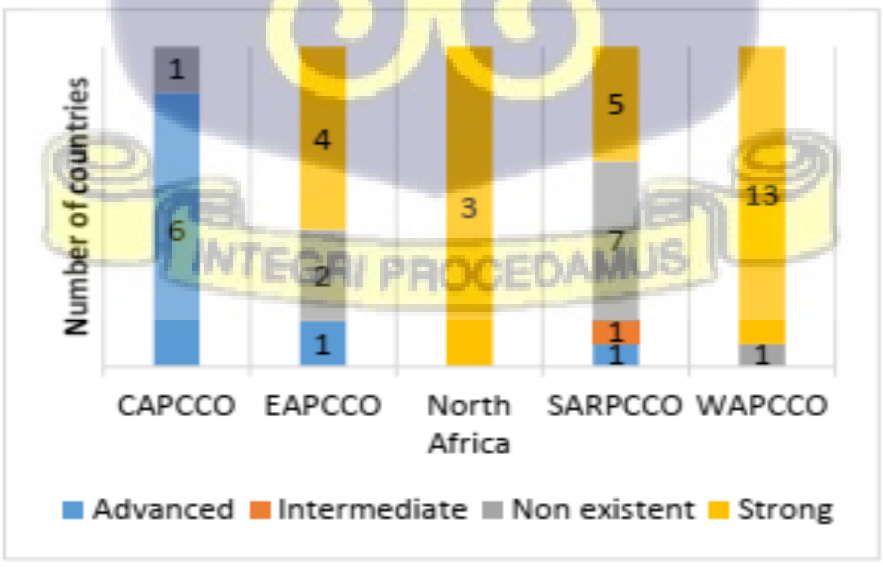


Figure 3.3: MM Customer Protection Regulations in different African Regions.

Source: IINTERPOL (2020).

When it comes to ensuring the safety of mobile money users funds, the situation becomes even more dire. Data available to the GSMA, suggests that all mobile money service providers on the African continent are mandated by law to ensure the absolute safety of the deposits of customers (GSMA, 2018). This regulation is set in such a way that there is 100% liquid assets or cash that can be given immediately to customer when the demand comes. To put it simply, all mobile money service providers must ensure they can provide in cash, 100% of their electronic money liabilities as well as all commercial banks who provide mobile money service in any form must be properly regulated (GSMA, 2018). There is another mechanism that have been put in place in the event that there is default or bankruptcy on the part of the service provider, which is the insurance of user's funds. In the traditional scheme of things, this approach is used for commercial banks, to ensure they are able to pay customers either in part or full in case the banks are unable to pay their debts when it is due. In similar fashion, such approach is used as a hedge for mobile money depositors.

3.7.8 How to Protect Yourself

There are diverse ways that scams, or fraud happens, and investigations are still ongoing to device more strategies to deal with the menace. However, there are still a number of things that customers or subscribers could do to halt a possible fraud attempt on them; at least those that are within their control to halt (BBC Africa, 2018; Prosper, 2022). Kenya's National Communication Authority and the Central Bank gave out some guidelines that can help customers halt any fraud attack on their mobile money accounts. Their guidelines are almost the same as those provided by MTN Ghana and across the continent by other service providers (Prosper, 2022; MTN Ghana, 2022):

- Never give out personal information
- Don't give out your PIN under any circumstance
- Delete requests for financial information or passwords

- Be suspicious of unsolicited messages or calls
- Report immediately any suspicious attempts on your SIMs to service provider

Safaricom, operators of MTN, also advised customers to protect important information such as passwords, dates of birth and national identity numbers. They also publish their customer care number and specific numbers, which will be the only number that MTN will use to call any subscriber in any circumstance (BBC Africa, 2018).

3.8 Chapter Summary

This Chapter speaks to the issue of mobile money growth in Africa and the problem of mobile money fraud. A presentation is made on how fraud issues are gaining grounds on the continent, the types of fraud that is been perpetrated on the service and the possible risk factors exposing the service to these fraudulent activities. The possible consequence of these reports of fraud is also addressed.

CHAPTER FOUR

THEORETICAL UNDERPINNINGS

4.1 Chapter Overview

In this chapter of the study, the theories considered for the study are presented. The theories considered for the study defined the underlying constructs and the basis on which examination, analysis and understanding are derived. Theories discussed include the Fraud Triangle theory, the Technology Threat Avoidance Theory (TTAT), the Generation Theory and the Concept of Continuance Use.

4.2 Theoretical Framework

4.2.1 The Fraud Triangle

Studies on fraud have established theoretical underpinnings to fraudulent activities. Although not particularly related to MM service, issues related to fraud in general cuts across economic, technological and structural fabric of society. For example, the fraud triangle by Donald Cressey (Cressey, 1986), in addition to other theories, puts in summary the entire issue of fraud.

In discussing the issue of fraud in MM service, the study discusses the Fraud Triangle, Fraud Diamond and Fraud Pentagon. The issue of fraud has been a major concern for many years especially as technological advancement has enabled perpetrators of such crime to become more sophisticated in their trade. The cost of fraud has never reduced and has had grave negative consequences on countries, institutions, businesses and individuals. The coast of fraud goes beyond the monetary value as it causes loss of confidence of investors in businesses or even the financial markets (Peterson & Buckhoff, 2004; Rezaee, Crumbley & Elmore, 2004). Discussing the issue of fraud in all of it variant form is not new as many studies and reports have extensively focused on it causes and impact (INTERPOL, 2020; Akomea–Frimpong et al., 2019; Gee &

Burton, 2019). In general, it has been accepted that in our fight against fraud, much attention should be placed on prevention rather than cure. This is because in terms of cost, it is far cheaper and easier to prevent fraud than to fight it after its occurrence (Gee & Burton, 2019). After it has occurred, most monies involved in the fraud may not be recoverable, coupled with the time needed for investigation and pursuing it in the court of law. In fraud cases involving governments and multinationals, it is almost impossible to track all the culprits involved.

Thanasak (2013), opined that for a fraudulent act to be curbed and it associated consequences reduced, it is immensely important that first, an understanding is made on the causative factors that leads to fraudulent activities. In effect, it is important to understand who these fraudsters may be, the nature of fraud they commit, how these frauds are committed, when such frauds take place and the major motivation behind what they do i.e., committing fraud. Among the theories that have been used or cited in an attempt to explain fraud, prominent among these are first, Cressey's (1950) Fraud Triangle Theory (FTT), and Wolfe and Hermanson's (2004) Fraud Diamond Theory (FDT). In both theories, proponents sought to establish the elements that influence fraud perpetrators in committing such acts. Dorminey et al. (2010), established that FTT originates way back from the works of Edwin Sutherland (1939). Edwin, in his own description of fraud coined the term white-collar and during those times, Cressey was one of Sutherland's students.

In 1950, Cressey conducted a study that sought to probe further, in an attempt to establish on the possible factors that leads or motivates people to violate the trust imposed on them by other people by perpetrating fraudulent acts or any other unethical activity. Cressey established two criteria for behaviours that the subjects must meet: (1) a person who had accepted a position of trust in good faith, and (2) must have violated the trust. Over a five-month period, Cressey interviewed 250 criminals. A theory which became known as FTT, the theory is made up of three main components

required for fraud to happen: (i) Perceived Pressure, (ii) Opportunity, and (iii) Rationalization. The above three components are put in other words as follows: i) financial problem(s) that were difficult or near impossible to share, ii) when there is the opportunity to commit the trust violation, and iii) trust violator trying to rationalize their act (Abdullahi & Mansor, 2015).

Cressey (1950) defined financial problems that were difficult to share or non-shareable financial problem as a situation where a person or persons violates the trust imposed on them when they incur financial problems which they consider as something which cannot be socially sanctioned and a such must be resolved secretly or through a private means. With regards to Perceived Opportunity, he said this happens when the individual in whom trust has been imposed, tends to find a way of solving the financial problem by using the trust imposed on them and being aware that it may be difficult for them to be caught (Abdullahi & Mansor, 2015). After taking the perceived opportunity, a lot of fraudsters rationalize their act with the claim that they are first time offenders having no criminal record, who see themselves as ordinary and honest people who have been unfortunately found themselves in a bad situation. In the end, this helps them in giving justification to what they have done and making it acceptable to themselves. Interestingly, Cressey (1950) discovered from his respondent through interviews that they knew what they were doing was very wrong and illegal but yet were kidding themselves in thinking otherwise. Cressey's (1950) hypothesis, over time, has been referred to as "the fraud triangle", (Figure 4.1) which is seen as a triangle with each side representing each of the three constructs identified (Wells, 2011).

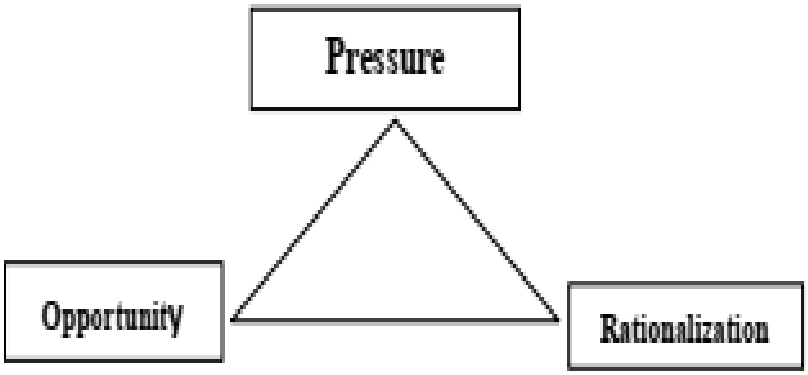


Figure 4.1: Donald Cressey Fraud Triangle

Source: Cressey (1986)

In his work, Cressey split up the Non-Sharable Financial problems into six different parts:

- Difficulty with debt repayment,
- Personal failures that have created problems
- Major uncontrollable incidence that causes businesses to fail or retrogress e.g., inflation or recession)
- When the trust violator isolates themselves from others who can provide support
- Gaining social status by living above their means
- Poor employer-employee relations such as poor treatment at workplace.

Other studies have corroborated the work of Cressey (1950) although they defined components of Cressey's (1950) fraud triangle differently with distinct examples. For example, according to Lister (2007), first, pressure or the motive to commit fraud should be considered as the main cause of the fraud act but did asset that the fact that these pressures are present does not necessarily mean they will commit fraud. He posited that there are three forms of pressure: pressure to pay for personal lifestyle, structure of employment compensation causing pressure, or the financial interest

of managements, and other external pressures e.g., financial stability of the business, commitments from business financiers, expectations from the market, etc.

Second, Lister (2007) defined Opportunity, representing the second side of the triangle as essentially "the fuel that keeps the fire going" or the drive that maintains or makes the pressure active. In his opinion, motive can only be perpetrated if there is an opportunity to perpetrate it. In other words, the absence of opportunity, no matter the presence of motive, will make the motive null and avoid. Some examples of opportunities that Lister considered to influence fraud includes managerial turnovers, duties not being segregated, or too complex organizational structures. Third, is the rationalization component. Lister (2007) considers rationalization as the oxygen that keeps the fire burning. In his opinion, one can study the culture of an organization and based on that, be able to tell the personal values of the individuals within it, whiles using auditors as an example.

A study by Vona (2012) also reasoned that, the presence of personal and corporate pressures is the leading cause of the motive to commit fraud. This motive to commit fraud is spurred on by the pressures that influences the perpetrator, either through sheer opportunity or rationalization. Among other things, he believed that the position a person holds in an organization plays a major role to commit fraud and that there is a direct correlation between the opportunity that leads to committing fraud and the person's ability to conceal it (Vona, 2012; Vona, 2021). In effect, the ability to understand the opportunity that leads to the perpetration of fraud helps auditors, for example, to know the scheme or type of fraud a person can commit and how the risk of fraud increases due to poor and ineffective control measures implemented by management.

Albrecht et al. (2010), asserted that the motive or pressure can take different forms. He claimed that the pressure can either be non-financial or financial e.g., falling sales, personal financial losses, inability of one's business to compete with other major players in the market, debt owed by the

person, greed, living above ones means, unable to meet financial forecasts, and unexpected financial commitments. Other non-financial forms of pressures may include the following: motivation to make reports look better than actual performance, challenges of beating the system, work frustration, etc. Albrecht et al. (2010) posited that, top managers or executives who believed any act of fraud will be caught and severely punished, never committed fraud even in the face of serious pressures. In terms of rationalizations executives gave to commit fraud, some few thoughts were presented. For example, the need to keep the stock price high, we are not the only business that uses aggressive accounting methods, or we are doing this for the good of the business, among others. In terms of perceived opportunity to commit fraud, some of the examples mentioned were: ability to bypass measures of fraud detection, poor organizational governance structure, board of directors who are weak, inability to discipline those who commit fraudulent acts, lack of audit trial, etc.

In addition to financial and non-financial pressures, Murdock (2008), added other forms of pressures such as social and political. According to him, lack of discipline or other habitual weaknesses such as addiction to drugs, gambling habits, are the root causes of non-financial pressures. In addition, the root cause for social or political pressures is the fact that individuals seek to protect their reputation or social status and so cannot envisage themselves failing.

Rae and Subramaniam (2008) also submitted that personal financial pressures and greed were chief determinants or factors in committing fraud among employees. They defined opportunity as a recognized weakness in a system that employees can take advantage of, and rationalization as the justifiable reasons employees give when they commit fraud due to a lack of personal integrity on their own part of other moral reasons. It is evident from the above studies presented that each researcher had their unique way of defining motives or pressure. However, they all agreed in

principle that pressure or motives was the first step in committing fraud. In all, it showed a strong support for the work of Cressey (1950) and how widely it has been accepted. In 1987 for example, the Commission of the Treadway Committee reviewed issues of fraud in reporting financials, whether alleged or proven, after which their report supported the findings posited by Cressey:

> *"Fraudulent financial reporting usually occurs as the result of certain environmental, institutional, or individual forces and opportunities. These forces and opportunities add pressures and incentives that encourage individuals and companies to engage in fraudulent financial reporting and are present to some degree in all companies. If the right, combustible mixture of forces and opportunities is present, financial reporting may occur" (1987, p.23).*

In 2002, SAS No. 99 supported the use of Cressey's fraud triangle by mentioning that:

> *"Three conditions generally are present when fraud occurs. First, management or other employees have an incentive or are under pressure, which provides a reason to commit fraud. Second, circumstances exist—for example, the absence of controls, ineffective controls, or the ability of management to override controls—that provide an opportunity for a fraud to be perpetrated. Third, those involved are able to rationalize committing a fraudulent act. Some individuals possess an attitude, character, or set of ethical values that allow them to knowingly and intentionally commit a dishonest act. However, even otherwise honest individuals can commit fraud in an environment that imposes sufficient pressure on them. The greater the incentive or pressure, the more likely an individual will be able to rationalize the acceptability of committing fraud" (AU316.06, Paragraph .07).*

The International Auditing Standards Board, in the year 2009 issued a revised version of their guidelines to international auditing standard and practices (ISA 240): The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements. The revised guidelines stated that:

> *"Fraud, whether fraudulent financial reporting or misappropriation of assets, involves incentive or pressure to commit fraud, a perceived opportunity to do so and some rationalization of the act" (Ref: Para. 3).*

Some examples were provided for the three fraud risk factors in the revised guidelines. In terms of pressure to commit fraudulent reporting of financials, the document cited that, this is possible to happen when managers are under some pressure, either from sources within the company or outside the company, in order for them to achieve certain set targets which are sometimes unrealistic. When it comes to perceived opportunity, the guideline stipulate that such a situation may exist when the individual who has violated the trust is in a key position of trust or is previewed to certain specific frailties in internal control measures. With regards to rationalization, the standard mentioned that there is always a possibility for trust violators to rationalize their wrongdoing. The standard therefore required all team members in an audit group to have a discussion on the susceptibility of the company to possible fraud, requiring all audit team members to make a consideration of both internal and external factors affecting the company that may serve as a pressure incentive for fraud either by management or any other individual, give an opportunity for fraud to be committed, and establish the existence of a culture that gives management or other key individuals to seek or attempt to rationalize perpetrating fraud. It is important to point out that, although the audit regulators supported Cressey's fraud triangle, other works that have been mentioned (Albrecht et al., 1984; Wolfe & Hermanson, 2004; Kranacher et al., 2010; Dorminey

et al., 2010) suggested that the model is not enough for fraud detection and prevention. Wolfe and Hermanson (2004), proposed a reviewed form of Cressey's (1950) fraud triangle and opined that for fraud to be properly detected and prevented, there was the need to add one more element to the three. In their opinion the three components of the FTT, thus, Pressure, Opportunity and Rationalization, is incomplete unless the perpetrators of fraud have the Capability to execute the act. They called theirs the Fraud Diamond Theory (FDT), made up of Pressure, Opportunity, Rationalization and Capability (Wolfe & Hermanson, 2004). The addition of capability to the fraud triangle has been supported by other works as an improvement to the FTT (Thanasak, 2013; Gbegi & Adebisi, 2013).

4.2.2 Technology Threat Avoidance Theory (TTAT)

The Technology Threat Avoidance Theory (TTAT) has been largely used to explain how users of a technology would avoid or mitigate the threat associated with the technology (Liang & Xue, 2010; Carpenter et al., 2019; Marikyan et al., 2021). In situations where the threat is avoidable, the user of the technology uses an avoidance strategy to avoid the threat whiles still enjoying the use of the technology. On the other hand, if a threat is not avoidable, the user of the technology adopts an emotion – focused strategy to deal with the consequences or the effect associated with the threat (Liang & Xue, 2009; Agarwal et al., 2000). Regardless of the fact that the threat of MM fraud attack is one that is avoidable, year on report suggest that the problem is constantly on the rise. Unfortunately, review of literature suggests that very little has been done in research to ascertain the empirical cause to the continuous rise in fraud attacks.

Available evidence suggests that in the MM value chain, the customer or end-user of the service is the one most at risk (Akomea–Frimpong et al., 2019). Stakeholders within the value chain, especially telecommunication companies, have tried frantically to put in place systemic measures

to curtail the activities of fraudsters but have achieved very little results. However, given that the end–user is the most at risk stakeholder and usually the main target when it comes to fraudulent attacks in the MM value chain, the onus now lies on the end-user to shoulder most of the responsibility in the prevention of these crimes (Yu et al., 2022; Lahiri et al., 2021). Without strong empirical evidence to explain the reasons for the continuous rise in MM fraud attacks, little will be achieved in attempts being made to curtail this problem.

One of the critical elements in dealing with a threatening situation is the perception of that threat. If an individual does/does not consider a situation to be threatening, they wouldn't be willing or motivated to take any necessary steps to avert such threat (Liang & Xue, 2009; Liang & Xue, 2010; Yu et al., 2022; Lahiri et al., 2021). Hence perception is critical. By using the TTAT as governing theory, this study will seek to appraise end–user' perception of the threat and their own coping abilities in relation to mobile money fraud attacks. In the adoption of technology, the Technology Threat Avoidance Theory (TTAT) propounded by Liang and Xue (2009 has served well in projecting the underlying factors that could prevent technology adoption. It explains why and how individual technology users avoid threats (Agarwal et al., 2000). These threats are basically malicious information technologies of which when the technology users become aware, decide on a strategy to deal with. The basic tenet of this theory is that technology users go through threat appraisal by perceiving their susceptibility to these threats and then how severe the threat may be (Carver, 2006). Users then juxtapose these findings to their ability to deal with the threat (Self-Efficacy) through Action Taking (Bagchi & Udo, 2003).

According to Liang and Xue (2009), TTAT as a dynamic and positive feedback loop, as depicted in figure 4.2, can be used to explain the avoidance behaviour of Information Technology (IT) users through the coping and cybernetic theories. They assert that, the technology user engages in two

cognitive processes. It is after this mental or cognitive process to appraise the threat that a strategy is determined after which a decision is taken on possible cause of action. Depending on how serious a malicious technology threat is will determine whether the user may perceive it as a threat, and as a result may draw a response of coping strategy (Beaudry & Pinsonneault, 2005). The nature of the perceived threat will determine whether the user will adopt a safeguarding approach based on perceived cost and self-efficacy. If a safeguarding measure is decided by the user, it may take the form of a problem-focused coping measure, where the user may try to solve the problem, or emotion-focused coping measure may be adopted when the threat may not be very easy to avoid and so user tries to emotionally adjust or cope with the threat. TTAT's assumption of avoidance and acceptance behaviour of people is supported by literature as humans are naturally prone to avoiding negative stimulus but rather gets closer to a positive stimulus (Pavlov, 1927; Skinner, 1953).

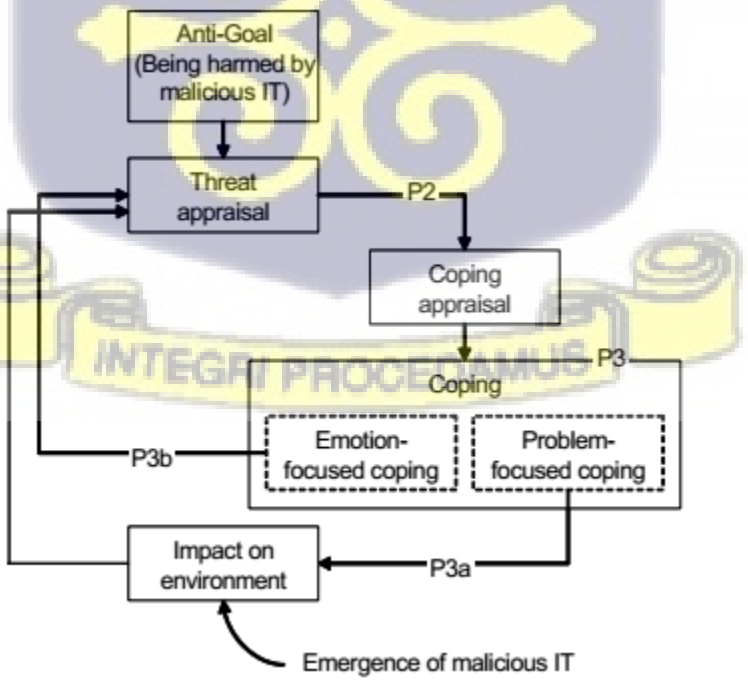


Figure 4.2: The Positive Cybernetic Loop

Source: Carver (2006)

The TTAT was considered as fit and relevant for this study this is because, the MM service offered by MNO is a new technology that aid in sending and receiving monies wherever one finds themselves. This technology has made it possible for users to receive foreign remittances all over the world directly unto their phones without visiting the bank. However, with the issue of fraud becoming increasingly prevalent, the service now faces significant existential threat and the confidence that users have may begin to dwindle.

4.2.3 The Concept of Generation X, Y, and Z

By its classical meaning, the term generation is in reference to the act of birthing one's offspring, a word which takes it root from the Latin term "*generāre" which means "to beget"* (Levickaitė, 2010). Over time, the word has garnered more diverse and an all-encompassing meaning referring to various stages or levels of evolution or alternatively seeing an improvement in technological developments. Scott and Marshall (2005), in their words define generation as a categorization of a specific age group. This specific age group may include all societal members who were birthed around the same time or during a specific historical event within that period. Depending on the specific area in academia, the term could vary in definition.

In Sociology for example, the term generation has been used to refer to a group of people relating in family or cultural patterns. Even by this definition, making a distinction between the family and cultural patterns is very critical, as in each context, the concept may vary in meaning (Scott Marshall, 2005). Before the 19th century, the term was used simply in relation to family relatives. However, the scope of its meaning has widened to refer to cohorts or groups born within the same date range, who came to share similar societal or cultural experiences. And so, form some cluster

of societal groupings. For example, in 1863, Emile Littré defined generation as "all men living more or less at the same time" (Wohl, 1979). After World War II, the term gained more prominence especially in relation to its impact on social change which has become clearer. In terms of family, the term generation refers to the average time usually between the first child of a mother and the first child of the mother's daughter. In the western world, this time length has been approximated to 25 years.

According to Gasset (1960), the concept of generation should be seen as a change and a task that needs solution. He opined that the term has some relationship with conflict. In the 20th century for instance, there has been a tall list of social or historical events that have been used to define generations. For example, there are those people who fought, and some who lost their lives in the first world war and so are referred to in Europe as the *Lost Generation* or *the Generation of 1914* (Wohl, 1979). War veterans from World War II are referred to as *The Greatest Generation*. These people were birthed around the years 1910 to the middle of 1920s who formed the youths and adults in the period of the *Great Depression*. Those who were too young to join the forces and service in the period of the second World War are called the *Silent Generation*.

After the silent generation, came the baby boom. After World War II, the world experienced a massive growth in population to about the year 1960. These are the *Baby Boom Generation*. This generation created a demographic bulge which played a major role in remolding society as they moved through society. In their college and teenage years, these group formed a central part of the 1960s counterculture, a group that played pivotal roles in major social issues and values such as racial and gender equality, environmental stewardship, etc (Strauss, 1991). Aside the Baby Boom Generation, there have been three main categorization of the generations that have come after. Specifically, these are Generations X, Y and Z.

4.2.3.1 Generation X

Generation X's are those who were born after baby boomers, describes a demographic, social, cultural social group in the Western culture and refers to people born in the 1960s and 1970s. The term was given in 1964 by American and British researchers Hamblett and Deverson (1964) who conducted a series of interviews with teenagers. Definitely conformist youth cultures (pros and cons racism, homosexual rights, Vietnam War; hippies) were defined by the term *Gen X*. *Generation X* was formed by contradictions, fetish, political flows, e.g., the phrase was picked up as the name of a punk rock band featuring Billy Idol (Coupland, 1989). The term *Generation X* was later popularized in 1991 after Douglas Coupland (1991) had published his novel spreading conformist ideas among Westerners. According to Coupland (1991), *Generation X* is a category of people who wanted to hop off the merry-go-round of status, money, and social climbing that so often frames modern existence. *Generation X* matured seeing the inception of the home computer, the rise of videogames, and the Internet as a tool for social and commercial purposes.

4.2.3.2 Generation Y

Generation Y which comes after the Generation X, is also referred to as the Millennium Generation. (Schäffer, 2012). The letter Y, in this generation group, stands for the word Youth. According to Krishnan et al. (2012), this generation is characterized by the following:

- They are highly adaptive and accept change easily. This generation does not like to plan too much for the future as they prefer living for today and now. They would rather enjoy themselves and have fun.
- This generation also came at the inception of various technological advancements; hence, they are technologically savvy and have great knowledge and very high qualification on

technology and digitization. With this, they can easily acquire new technological tools and IT devices and are adept at the use of them.

- This generation easily form virtual relationships and friendships, as most of their friendships are built on the internet of social sites. Adapting to people of different cultural background is not a challenge for this generation and prefer living the quick life.

For this generation, highly valued traditions are outmoded and hence do not hold on to them. They do not put much emphasis on family as they believe in being on their own and establishing themselves individually. Currently, Generation Y forms the majority of the world's working force, working together with a sizeable number of Generations Xs and a few Generation Zs. Most of Generation Ys hold bachelor's degrees and are very intelligent (Schäffer, 2015). They have interesting ideas of the workplace and the future of the working class in relation to positions and job opportunities. For this group, working in their preferred fields and enjoying what they do is highly important to them. Being free to express their creativity is critical, hence any form of restrictions of captivity will be opposed. They will not hesitate to step further. They can easily multitask, have multiple sides and can share attention (Schäffer, 2015). For this generation, money, success and career are most important as they believe these are extremely necessary to enjoy life (Tari, 2010), and their experience forms a major determinant in their decisions and subsequent actions (Bittner et al, 2013).

4.2.3.3 Generation Z

Generation Z is the group that comes after the Generation Y. As technology began among Generation Ys, Generation Z were hence birthed into technological advancement. They came at the time of digital transformation and so are referred to as the "net generation". They are sometimes also referred to as the "Facebook-generation". They are the "digital natives" or "iGeneration"

(Tari, 2011). This generation has values and norms that are entirely different and new to Generation Ys. Their language use, their expressions and mannerism are absolutely strange to the previous generation. They love to be on the internet almost every time, a situation that drastically influences their worldview and behaviours. Being able to socialize outside of the internet is extremely difficult for them, coupled with the fact that they don't understand the concept of struggling. They have a lot of bravery and won't hesitate taking the lead, are very practical and very intelligent but not as much wise. They are highly impulsive and always in the lookout for new challenges unlike their predecessors. Generation Zs are very agile, impatient and are not afraid of change. Due to the preference of the internet, this generation is well informed as they have a lot of information. However, they are also unable to solve problems without the internet as they will search for solutions to almost everything on the internet (Tari, 2011).

Forbes magazine put together a survey of which forty-nine thousand (49,000) respondents were interviewed from the Middle East, Europe, North and South America, Africa and Asia (Dill, 2015). After analyzing the data, the following postulations were made. That Generation Z can be considered as the generation that is truly global in their worldview. They are extremely high-tech and have grown up in complex environmental situations that have shaped their habits, educations, work and workplace expectations (Bencsik, Horváth-Csikós, & Tímea, 2016). They are the most professionally ambitious generation, having high level knowledge on technical situations and language expressions. It is hence projected that they will be an excellent workforce. Employers seeking to employ this generation must be clear on exactly what they want and must learn to effectively communicate to them to be able to fit them properly into the organizations culture, and even the community to derive the best from them in this digital age (Elmore, 2014). The study also revealed that, employees should be ready to accept that this generation will go their way or choose

a career path that they want and not to be pushed into something due to somebody's demands. This group is highly intrinsically motivated, have the tough spirit of entrepreneurs and would want to greatly influence the world. They prefer a good balance of life and work and enjoys stability most. Although intrinsically motivated, they are not highly optimistic as there are always concerns of unemployment, unlike the generation that came before them (Elmore, 2014).

Comparatively, although Generation Y and Z witnessed the digital age and are accustomed to it, they still have a difficulty of being able to merge their online life to their offline life. They are characterized with anxiety and nervousness and are in constant need of attention. They crave for feedback that tells them: they are incredible (Tari, 2011). These two generations are easily adaptive to technology; hence the use of smart gadgets and applications comes easily is quite widespread among them. They therefore live a much easier and faster life (Elmore, 2010). The age groupings of the above-mentioned generational cohorts, their personal life and workplace characteristics are depicted in Table 4.1 and 4.2, and Figure 4.1 which shows the generational timelines.

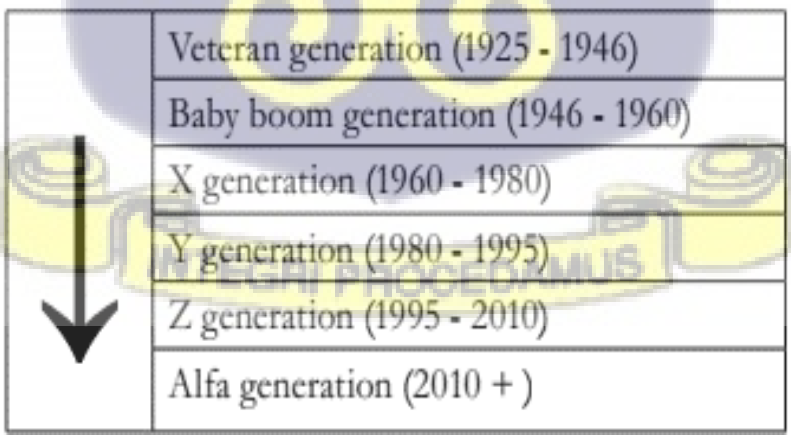


Figure 4.3: Generational Timelines

Source: Zemke et al. (1999)

Table 4.1: Generational Group and their Personal, Lifestyle and Workplace Characteristics

Views Toward	Veterans (1922 – 1945)	Baby Boomers (1946 – 1964)	Generation X (1965 – 1980)	Generation Y (1981 – 2000)
Core values	Respect of authority, discipline	Optimism, involvement	Skepticism, fun, informality	Realism, confidence, extreme fun, social
Family	Traditional	Disintegrating	Latch-key kids	Merged families
Education	A dream	A birthright	A way to get there	An incredible expense
Dealing with money	Put it away, pay cash	Buy now, pay later	Cautious, conservative, save	Earn to spend
Work ethic and values	Hard work, respect authority, sacrifice, duty before fun, adhere to rules	Workaholics, work efficiently, personal fulfillment, desire quality	Eliminate the task, self-reliance, want structure and direction, skeptical	What's next, multitasking, tenacity, entrepreneurial, tolerant, goal oriented
Work is …	An obligation	An exciting adventure	A difficult challenge, a contract	A means to an end, fulfillment
Interactive style	Individual	Team player	Entrepreneur	Participative
Communication	Formal	In person	Direct, immediate	E-mail, Voice mail
Feedback and rewards	No news is good news, satisfaction in a job well done	Don't appreciate it, money, title recognition	Sorry to interrupt, but how am I doing?, freedom is the best reward	Whenever I want it, at the push of button, meaningful work
Ideal leaders	Authoritarian commanders	Commanding thinkers	Coordinating doers	Empowering collaborators
Work and family	Never the twain shall meet	No balance, work to live	Balance	Balance
Special Interests	Want to feel needed, they are patient and loyal and expect loyalty in return	Look for future security rewards	Are most likely to excel at multitaking	Is amazingly optimistic. "We can do this". Sometimes this is detrimental to achieving success in the workplace.

Source: Cook (2015); Hammill (2005); Wasserman (2007)

Table 4.2: Generational Behavioural Characteristics of Different Age-Groups

	Baby – boom	X generation	Y generation	Z generation
View	Communal, unified thinking	Self-centred and medium-term	Egotistical, short-term	No sense of commitment, be happy with what you have and live for the present
Relationship	First and foremost personal	Personal and virtual networks	Principally virtual, network	Virtual and superficial
Aim	Solid existence	Multi-environment, secure position	Rivalry for leader position	Live for the present
Self-realization	Conscious carrier building	Rapid promotion	Immediate	Questions the need for it at all
IT	It is based on self-instruction and incomplete	Uses with confidence	Part of its everyday life	Intuitive
Values	Patience, soft skills, respect for traditions, EQ, hard work,	Hard work, openness, respect for diversity, curiosity, practicality	Flexibility, mobility, broad but superficial knowledge, success orientation, creativity, freedom of information takes priority	Live for the present, rapid reaction to everything, initiator, brave, rapid information access and content search
Other possible characteristics	Respect for hierarchy, exaggerated modesty or arrogant inflexibility, passivity, cynicism, disappointment	Rule abiding, materialistic, fair play, less respect for hierarchy, has a sense of relativity, need to prove themselves	Desire for independence, no respect for tradition, quest for new forms of knowledge, inverse socialization, arrogant, home office and-part-time work, interim management, undervalue soft skills and EQ	Differing viewpoints, lack of thinking, happiness, pleasure, divided attention, lack of consequential thinking, no desire to make sense of things, the boundaries of work and entertainment overlap, feel at home anywhere

Source: Bencsik and Machova (2016)

4.3 Technology Continuance Theory (TCT) or Theory of Continuous Use

After the invention of every technology, among other things, two things that are most critical is the adoption process of the technology and the continuous usage of that technology. The theory that explains continuous use of a technology, the Technology Continuance Theory (TCT), has serve a great deal of purpose. Propounded by Liao, Palvia and Chen (2009), this theory gives an explanation on how users of a technology could be predicted to either continue to use or discontinue using a technology. The TCT had its roots from the Technology Acceptance Model (TAM) propounded by Davis in 1989, the Expectation Confirmation Model (ECM) also propounded by Bhattacherjee in the year 2001, and the Cognitive Model (COG) also propounded by Oliver in 1980. It seeks to combine the above listed theories, which are among the most widely used theories in Information Systems and Technology research. The TCT consists of three main stages with the final part the IS continuous Intention. On the first, TCT is made up of Confirmation, Perceived Usefulness and Perceived Ease of Use. After a user of a technology has satisfied him/herself at this level, the stage is set for the next, which is Satisfaction and Attitude. The final conclusion after satisfaction has been confirmed and attitude towards the technology is formed determines the final stage which is the continuous use intention.

A number of studies have confirmed that, for any information system or technology to succeed, the first step is for the information system or technology to be accepted (Bhattacherjee, 2001; Bhattacherjee et al., 2008). After crossing the initial phase, the next most critical point is being able to maintain user's intention to continue using the technology. At different stages in the adoption process, users may have different demands from the IS or technology, a situation that affects each individual user differently in their decision to continue using the technology (Ambalov, 2018; Bhattacherjee et al., 2008). This is depicted in the Figure below.

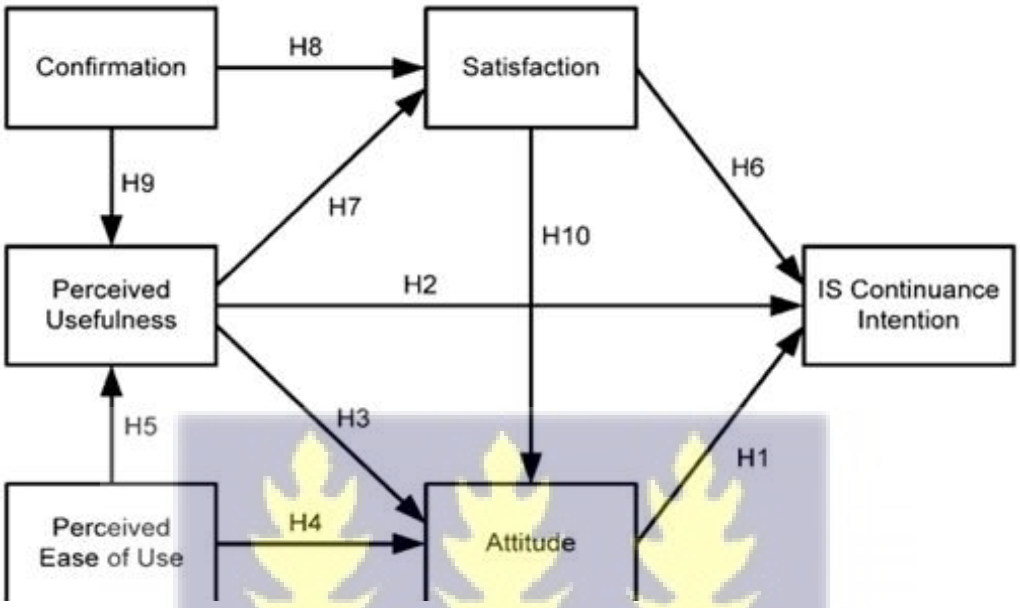


Figure 4.4 Technology Continuance Theory (TCT) by Liao et al. (2009)

Exploring user's intention to continually use the mobile money service in the face of consistent fraud issues, is one that is most critical for the survival of the service. This knowledge and information are highly critical, hence justifying the inclusion of the Technology Continuance Theory (TCT) in this study.

4.4 Chapter summary

The chapter four of the study presented the theories that underpinned the research work. This chapter's discussion centered on the TTAT, the Generation Theory, and the Technology Continuance Theory. Discussion also included the tenets of each theory, the justification for their inclusion as well as their role in the development of the research framework.

CHPTER FIVE

FRAMEWORK OF RESEARCH

5.1 Chapter Overview

In the previous chapter, presentation was made on the theories that were used for this study. In this chapter, the framework of research is presented. The constructs that were used for the study is presented and discussed, as well is the formulation of the hypothesis. The chapter concludes with a summary of discussions made within the chapter.

5.2 Development of Research Framework and Hypotheses

The primary purpose of this study was to investigate how users of mobile payment systems as a channel for transferring money are able to avoid the possible threat of fraud that has bedevilled the service, and how this avoidance behaviour affects their intention to continuously use the service. By this purpose, this study sought to appraise respondents' threat and coping perceptions and how these two affects their avoidance behaviour. The study went further to examine how respondent's avoidance behaviour affects their intention to continuously use the service. By using the Technology Threat Avoidance Theory (TTAT) as the main governing theory. The study further sought to examine how the threat and coping appraisal process is moderated by Generational theory. In all, this study aimed at making an important theoretical contribution to the TTAT, as well as how the various generations i.e., Generation X, Y and Z, go through the appraisal process and the possible difference in their avoidance behaviour among users of this service (Liang & Xue, 2010; Carpenter et al., 2019). The focus was to provide grounds for possible prediction of customer behaviour on their intention to continuously use the service and then help inform telecom operators and service providers on service improvement strategies and possible policy directions.

The various constructs of the study are governed by the Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009) built on the works of Maddux and Rogers (Maddux et al., 1986; Maddux and Rogers (1983), the Generation X, Y and Z theory (Levickaitė, 2010; Jiří, 2016), and the Technology Continuous Use Model (Liao et al., 2009). The TTAT measures coping strategies by examining or appraising perception of threat and coping mechanisms, and it effect on Avoidance Behaviour. As originally established in relation to security threat defined in the space of technology adoption, this theory is made relevant for this study by redefining the various constructs in relations to mobile payment technology fraud attacks.

To better understand and establish a strong basis for user's avoidance behaviour, the various constructs are moderated by the Generational Theory. The generational theory with three generational cohorts; X, Y and Z, will provide better appreciation of the relevance of these three generational cohorts in relation to the TTAT. The measure of respondents Avoidance Behaviour as the dependent variable, will then again serve as the independent variable to be used for examining their intention to continuously use the service in the face of fraudulent attacks. The variables to be used for the study are derived from the constructs and hence, the framework of research or the research model is depicted in the figure 5.1 below:

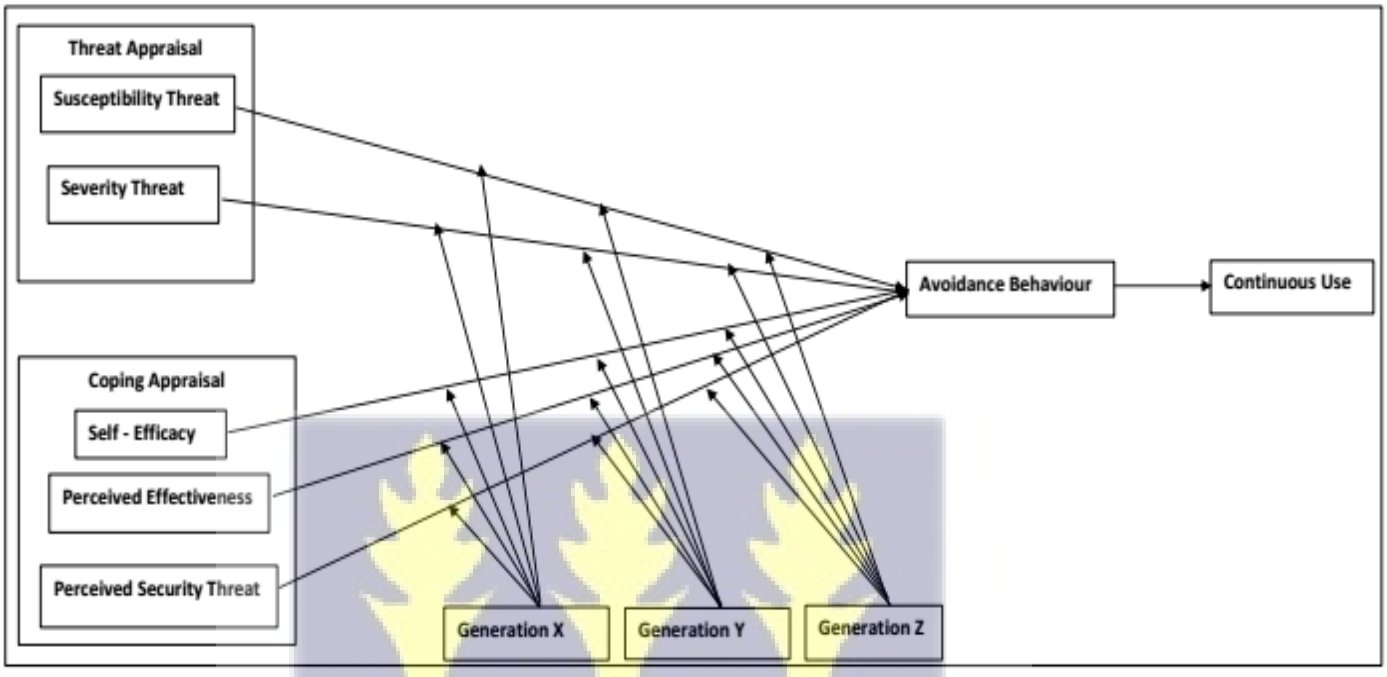


Figure 5.1: Research Model

Source: Author's Construction

5.2.1 Relationship Between Threat Appraisal (IV1) and Avoidance Behaviour

This study adopted two broad categorizations of Independent Variables: First is the Threat Appraisal which is made up of two main components; Susceptibility Threat (Perceived Susceptibility or Vulnerability) and Severity Threat. The second is the Coping Appraisal, which is made up of three components: Self-Efficacy, Perceived Effectiveness and Perceived Security Threat.

5.2.1.1 Susceptibility Threat

The threat appraisal process has two main components: Susceptibility Threat and Severity Threat. Susceptibility threat, also referred to as Perceived susceptibility or Vulnerability in some scholarly works, is an individual's independent assessment of a malicious IT or a negative situation and its likelihood of affecting them (Liang & Xue, 2009) or in other words a person's perception that a

criminal event with eventual negative consequences will most likely harm them or some asset or property they have (Clubb & Hinkle, 2015). Literature suggests that, for an individual to consider a negative situation as a threat, there has to be the potential that the negative situation is likely to affect them (Liang & Xue, 2009). Review of literature has suggested that an individual's assessment of their vulnerability or susceptibility to a negative situation or to a technology can influence their decision to either continue to use the technology or abandon it (Clubb & Hinkle, 2015; Liang & Xue, 2010). Although susceptibility threat has been widely used in IT adoption and use (Liang & Xue, 2010; Chen & Zahedi, 2016; Carpenter et al., 2019), it has not been used to explain mobile money adoption and fraud (David-West, Umukoro, & Muritala, 2017; Akomea-Frimpong et al., 2020), which is a major threat related to the service. This study is arguably the first of its kind to attempt such. Given that mobile money is a form of technology for payment and also issues of mobile money fraud are threats to users of the service, this study hypothesized that:

H1: Susceptibility Threat will have a direct effect on Avoidance Behaviour

5.2.1.2 Severity Threat

After an individual have assessed themselves of their susceptibility or vulnerability to a threat, they measure the possible severity of the consequences associated with the negative situation or the threat. This is called Perceived Severity or Severity Threat. According to Liang and Xue (2009), users of a technology only consider a possible threat when the severity of its consequence is great or serious. Other studies have suggested that the consideration of a severe situation is subjective and that it will differ among groups of people (Clubb & Hinkle, 2015), nevertheless, a technological threat whose consequence may be deemed more severe will affect the individuals desire and intention to avoid the technology (Akomea-Frimpong et al., 2020). Threatening situations such as violent criminal victimization may have severe outcomes such as physical

injuries to the body, psychological injuries, loss of money and other harms that may affect a person's quality of life or may potentially lead to death. Issues of mobile money fraud, aside one losing their money, also has the potential of causing severe psychological damage to the individual victim and has the potential of causing the victim to either switch networks or avoid using the service altogether. Based on the above, this study hypothesized that:

H2: Severity Threat will have a direct effect on Avoidance Behaviour

5.2.2 Relationship Between Coping Appraisal (IV 2) and Avoidance Behaviour

The second independent variable used for the study is the Coping Appraisal. The coping appraisal process in dealing with threatening situations with regards to the use of technology, according TTAT, is made up of three components: Self Efficacy, Perceived Effectiveness and Perceived Security Threat.

5.2.2.1 Self – Efficacy

The possibility for one to be successful in overcoming a threat is also dependent on the level of self-confidence that a user has. Termed as Self-efficacy under TTAT, this construct is defined as the technology users' level of confidence in being able to take certain safeguarding measures to curtail the threatening situation (Liang & Xue, 2009). It refers to the perception of a person that he can effectively deal with a criminally threatening situation and reduce it risk based on information he or she has (Clubb & Hinkle, 2015). Self-efficacy has been deemed a vital component of avoidance motivation leading to avoidance behaviour (Liang & Xue, 2009; Clubb & Hinkle, 2015). To be able to apply safeguarding measures against a threatening situation, sometimes the protective measure may require the user involved to consistently remember how to use the protective measure. Other situations may demand that the user possesses some special skill e.g., firing a gun. In some other instances, the person only needs to be alert and smart, and be able to

read gauge a situation to be able to identify potential threat, such as in the case of MM fraud. However, regardless of the format the threat may take, it is important that the individual believes that he or she possesses the necessary qualities or skills to deal with the threat (Clubb & Hinkle, 2015). Fraud related to MM is now well-publicized, that almost all users of the service should be aware of. Safaricom, operators of MTN across the African continent, has managed to spread as much information as possible concerning MM threat especially in Ghana. Studies have shown that there is higher motivation among individual technology users to apply safeguarding measures as their level of self-efficacy rises (Ng et al., 2012; Woon et al., 2005; Workman et al., 2008). As technology user's self-efficacy goes up, the more likely they are to use available safeguarding measures to avoid the threats (Liang & Xue, 2010). Due to the widespread nature of MM fraud and the rate of information given by operators, government and media, this study projected that the level of self-efficacy among users will be high. The study therefore hypothesized that:

H3: Self – Efficacy will have a direct effect on Avoidance Behaviour

5.2.2.2 Perceived Effectiveness

Protective mechanisms must be able to provide technology users the needed outcome of protecting them against malicious software. In the case of MM fraud, protective information and guidelines that have been provided to users by service providers must be effective in yielding the desired outcome. This concept is derived from the outcome judgement of Bandura (1982), which described the extent to which a well actionable behaviour, if effectively executed will lead to specific or particular outcomes. By executing such a behaviour against an IT threat, it is believed that the individual will reduce the potential negative ramifications associated with the IT threat. By applying it to MM fraud, it is believed that as a customer or MM user properly execute such a plan, it will be less likely for he or she to be defrauded. From TTAT's perspective, perceived

effectiveness is a subjective assessment of the effectiveness of the safeguarding measure to deal with the threat.

In the health belief model for example, this concept is akin to the concept of perceived benefits (Janz & Becker, 1984; Rosenstock, 1974) and in the protection motivation theory, the concept of response efficacy (Rogers, 1975; Rogers, 1983). When users of a technology believe that a safeguarding measure provided to curtail any negative consequences of a threat is effective, they are more than likely to adopt the safeguarding measure and use it. In the context of technology security, perceived effectiveness has been found to motivate users to use the provided safeguarding measures to deal with IT threats (Anderson & Agarwal, 2006; Ng et al., 2012; Woon et al., 2005). On the basis of the above, and in relation to MM fraud, this study hypothesized that:

H4: Perceived Effectiveness will have a direct effect on Avoidance Behaviour

5.2.2.3 Perceived Security Threat

The perception of security threat or perceived threat depicts how the user of the technology sees a potential threat. Perceived Security is the extent or how far an individual assumes a threatening situation as dangerous or harmful. For some literature, perceived threat is defined by combining susceptibility threat and severity threat. Thus, perceived does not exist, but by defining susceptibility and severity threat, we then establish perceived threat (Carpenter et al., 2019; Chen & Zahedi, 2016). However, other scholars have opined that although perceived security could be as a result of combining susceptibility and severity threat, perceived threat or perceived security threat can be measured on its own, as there is the possibility of a lot more possible factors which influences it such as gender, risk appetite, among others (Carpenter et al., 2019; Yu et al., 2022; Lahiri et al., 2021). In this study, the researchers opined that, in as much as perceived security

threat or perceived threat is influenced by Susceptibility and Severity, perceived security can be measured on its own as other literatures have indicated (Lahiri et al., 2021)

According to Maslow's hierarchy of needs, one of the basic needs of every man is safety and security; be it for themselves or any asset that they possess (Maslow, 1943). Based on the principle of hedonism, humans originally tilt towards pleasure as they avoid pain (Freud, 1915). And so, as the presence of IT threats has the potential of bringing unwanted negative consequences such as destruction of gadgets, financial losses, etc., when users perceive an IT threat, they are motivated to avoid it. Avoidance motivation is therefore defined as the degree to which IT users are motivated to avoid IT threats by taking safeguarding measures. As the threat perception intensifies, individuals are more motivated to get away from the danger. A number of studies have confirmed this relationship such as in the health sector (Tanner et al., 1991; Weinstein, 1993; Wimmer, 2018). As Liang and Xue (2009) posit, both malicious IT and diseases are somewhat similar. Just as disease causing agents enter into the human body and takeover the body's systemic functionalities, so do malicious software. Therefore, people's responses to health threats tend to be similar to their responses to IT threats. This same principle can be applied to MM fraud, in that, the presence of MM fraud also causes different degrees of negative consequences such as financial losses, depression and emotional instability and various other devastating consequences on users of the service. From the above presentation, this study also proposes that:

H5: Perceived Security Threat will have a direct effect on Avoidance Behaviour

5.3 Avoidance Behaviour as Dependent and Independent Variables

In this study, avoidance behaviour is operationally defined as the decisions and actions of mobile money users to avoid the use of the service due to potential or actual incidence of fraud attacks or attempt on them (GSMA, 2016; GSMA, 2017). Avoidance Behaviour played two key roles in this

study, first, as a dependent variable (DV) and then as an independent variable. As a dependent variable, it represents the effect of the independent variables (Boateng, 2016). The dependent variable, as intrinsically applied in its name, depends on the influence of the independent variables and/or their interaction(s) between the independent variable(s) threat appraisal and coping appraisal (Boateng, 2016). As an independent variable, avoidance behaviour directly influenced the intention of mobile money users to continually use or discontinue using the service. Mobile money users may potentially avoid using the mobile money service which may greatly affect their intention to continually use the services. The study postulates that:

H9: Avoidance Behaviour will have a direct effect on Intention to Continuously Use the Service

5.4 Generation X, Y and Z as Moderating Variable.

The Generation theory has been used in a number of studies, and as such it is not new to the academic field. Depending on which year period a person was born, one is most likely to fall within one of the three generation categories: Generation X, Y or Z. This is not to say, that there are no other generational groupings aside those stated. It is a fact that prior to these current generational groupings, others have existed, and possibly others will come after this group. However, within our current dispensation, these three groups are the dominant force.

A generation is defined primarily based on the age groups that people fall under or the years of their birth, however, review of literature suggest that various scholars have defined the different generational groups distinctively (Levickaitė, 2010). Regardless of the definition that is given, there is not much disparity in the year categorizations of their birth. Generation X has been defined by a number of scholars, after review of literature, as people born from the early 1960s to the year 1974 and are people who currently fall within the age range of between 46 – 60 years (Levickaitė,

2010; Howe & Strauss, 2000; Martin & Tulgan, 2002). Generation Y group, according to literature, are those born between the period of 1975–1989. People within this generational group are those who fall between the ages 31 – 45 years (Levickaitė, 2010; Glum, 2015; Holmes, 2011; Howe & Strauss, 2000; Martin & Tulgan, 2002). The final generational group is Generation Z. This group of people were birthed from the mid-1990s to the late 2000s and currently fall between age 30 years and below. These generations are unique in their behaviours and their overall view to life. Based on the period or dispensation of their birth, these three generational groups have distinct characteristics, for example, whiles generation Z are very knowledgeable as they will find answers to virtually everything on the internet, Generation Y, although technologically savvy, do not entirely understand how to properly find the balance between their life online and offline (Abdurrahaman, Owusu, & Soladoye, 2018). A number of studies have classified Generation Y-ers as people who are very sensitive. They care so much about things that will put information they consider to be personal out in the public, as compared to members of the Generation X who do not care much about their information being in the public domain. Generation Y members, although technologically savvy, find it difficult being persuaded to be in the online social space and are usually opposed to the use of conventional marketing strategies (Abdurrahaman et al., 2018). As has been stated, each of the generational cohort has its unique characteristics, and it is expected that these groups will differ in their perception of threats, and their approach in dealing with such threats. Differences among different groups is consistent with studies in other disciplines such as marketing. As with the case of market segmentation, different groups of people have different needs (LaTour & Rotfeld, 1997; Quinn, Meenaghan, & Brannick, 1992; Rotfeld, 1999). By applying the same principle, different groups have specific ways in identifying problems and devising solutions for them.

As has been stated, the Generation Theory has been used widely in a number of studies. Either used together or as distinct from each other, the generations have been predominantly used either as an independent variable or dependent variable (Levickaitė, 2010; Jiří, 2016; Bencsik, Horváth-Csikós, & Tímea, 2016; Desai & Lele, 2017). Further, no study was found to have examined the various generations and how they would behave or react on issue of fraud and security. In fact, very few studies have established that, for example, that millennials (Generation Ys) were the most careless when it comes to issues of privacy and security. No study was found that examined the three generation groups as moderators to the issue of mobile money fraud and specifically to the threat and coping appraisal of mobile money users in relation to their avoidance behaviours (Brewster, 2014). Therefore, for all generational groups, and independent variables, the researcher hypothesize that:

H6a: Generation X will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour

H6b: Generation X will moderate the direct relationship between Severity Threat and Avoidance Behaviour

H6c: Generation X will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour

H6d: Generation X will moderate the direct relationship between Perceived Effectiveness and Avoidance Behaviour

H6e: Generation X will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior

H7a: Generation Y will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour

H7b: Generation Y will moderate the direct relationship between Severity Threat and Avoidance Behaviour

H7c: Generation Y will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour

H7d: Generation Y will mediate the direct relationship between Perceived Effectiveness and Avoidance Behaviour

H7e: Generation Y will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior

H8a: Generation Z will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour

H8b: Generation Z will moderate the direct relationship between Severity Threat and Avoidance Behaviour

H8c: Generation Z will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour

H8d: Generation Z will moderate the direct relationship between Perceived Effectiveness and Avoidance Behaviour

H8e: Generation Z will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior

5.5 Intention to Continuously Use

Intention to continuously use or continuous usage was used as a dependent variable (DV) in this study. Mobile money user's decision to either continue using the service or discontinue it use was the end point of the user's avoidance behaviour. This construct was deduced from the Technology Continuance Theory. A number of studies have established that, factors such as Perceived Ease of Use, Perceived Usefulness, Self-Efficacy, etc., are critical determinant factor for an individual in adopting a technology. Teo and Zhou (2014) sought to provide explanation on the intention for a technology to be used through a structural equation modelling approach. They sampled 314 participants who were at various levels of training at a teacher training institute in Singapore, and established that factors such as attitude, perceived ease of use, perceived usefulness and self-efficacy significantly affected students' intention of using a technology (Teo & Zhou, 2014). As there are no argument on the above stated factors affecting an individuals' decision to use a technology, the issue of avoidance behaviour actually translating into or affecting the choice of using or not using a technology is still under exploration. Studies in fields of medicine and psychology (Ng & Lovibond, 2017; Ng et al., 2020) have established that an individual's avoidance intention affects their emotional state which directly affects their decision making and consequently their choices. The question of whether this situation applies to all forms of technologies is one that have served as a motivation for this study. Considering the mobile money transfer service has almost become an indispensable part of average Ghanaian, the question of fraud affecting avoidance behavior, and whether it will consequently translate into decision of not using again was worth exploring.

5.6 Chapter summary

This chapter made a presentation on the development of the framework of research as well as hypotheses that were postulated for the study. The framework of the study and the hypotheses were developed after review of both theories used for the study and relevant literature. Explanations were given on all the variables that were used as measures for the study. The next chapter presents the methodology that were put in place to achieve the objectives of the study.

CHAPTER SIX

RESEARCH METHODOLOGY

6.1 Chapter Overview

In the previous chapter of this study, the theoretical basis that underpinned the study were discussed out of which the conceptual framework that were adopted for the study was designed. This chapter makes a presentation on the methods that were adopted to help answer the research questions and achieve the setout objectives. This chapter discusses the research design which encompasses the types of reasoning in research, and the paradigms that available in information systems research. The chapter also speaks of the sources of research constructs as well as the questionnaire source matrix. It concludes by providing a summary of the chapter.

6.2 Research Design

In its simplest definition, research design is considered to be the framework that a researcher uses in conducting research (Malhotra & Birks, 2007). The purpose of a research design is to organize and structure research in a way and manner that will help answer posed by the research or the objectives set out to be achieved by the research. Scholars such as Zikmund (2003) posited that research design demonstrates a carefully structured plan laid down to provide direction and guidance in the execution of the research with the focus of achieving the stipulated objectives. Included in a research design are the steps or road map that it provides for data collection and analysis and tells the researcher of the necessary details of all the processes that will be used in getting the needed information out of which inferences can be drawn to inform decision making (Churchill & Iacobucci, 2009). The research design speaks of the paradigm of the research, the purpose, laid down strategy, and the methods for needed to gather required data.

With regards to the paradigm, this study was conducted from the perspective of the positivist, as it was based on well-structured methods through which responses that are quantifiable were sourced from respondents to aide in performing statistical analysis out of which inferences could be drawn (Gill & Johnson, 1997). Literature was reviewed after which statements of hypothesis were formulated and tested empirically. Analysis was done based on direct effects of threat perception on avoidance behavior, as well as the role of moderator variable generation theory. This study sought through empirical examine the effect of the threat perception of mobile money fraud attacks on the avoidance behavior of users, and the role of generation X, Y and Z, as a moderator. A survey method was used through, as it has been considered to be the favoured method in cross sectional studies (Creswell, 2014), a structured questionnaire which was developed based on review of theory and literature. Descriptive analysis was done on the sample, and quantitative approach used to measure the relationship between the constructs.

6.2.1 Types of Reasoning in Research

In order to understand the different concepts in philosophy, it is important to understand how theories and conclusions are found within the data i.e., the logic applied to the data to obtain results. There are two main types of reasoning when it comes to research, inductive and deductive. Other paradigms such as realism also refers to retroductive reasoning, but this is discussed elsewhere (Danermark et al., 2019).

Inductive Reasoning starts with observation, experimentation and measures, generalization and finding patterns in data and then theory development to describe the situation (Bryman, 2008). This process would consist of making repeated measures and observations until the researcher is confident that the findings describe the wider situation. Inductive reasoning forms a world view of a situation by joining it fragmented parts. By using inductive reasoning and it approach, we

consider collecting primary or secondary data, based on that analysis of the data is done to observe patterns that may lead to the formation of relationship which may lead to forming relationships, make generalizing analysis and/or defining theories or question them.

Deductive Reasoning follows the revers process: find a theory, make predictions/hypotheses based on this and then observe/experiment/measure to prove or disprove (Bryman, 2008). This form of reasoning views the situation from a universal perspective and then makes steps backwards to it fragments. This approach starts with forming a hypothesis and then test the hypothesis to either supported or rejected. The formation of hypothesis seeks to find a relationship between two or more situations and also seek to establish a cause-effect relationship. These two ways of reasoning forms the central core of research methods and it design.

6.2.2 Paradigms of IS Research

A research paradigm refers to the set of beliefs, values and techniques which is shared by members of a scientific community, and which defines what makes up knowledge, the apt way to acquire that knowledge, analyze it and the researcher's role in the research process (Kuhn, 1970). The ontology, epistemology, and methodology are the three dimensions that constitute a research paradigm (Guba & Lincoln, 1994). The ontology examines the physical and social reality beliefs about a research phenomenon (Orlikowski & Baroudi, 1991).

The epistemology refers to what constitutes knowledge and how it is validly generated, understood and used (Lewis & Ritchie, 2003). Methodology, however, refers to the framework used to conduct research in the context of a specific paradigm (Lincoln, Lynham, & Guba, 2011). Research methodology could be quantitative, qualitative or a mixed approach. Research paradigms in Information System has traditionally include Positivism, Interpretivism and Critical research which over the years have become the dominant paradigms (Orlikowski & Baroudi, 1991). As part

of the critical research paradigm, Critical realism (CR) has been developed as a more practical option to the stronger and more popular opposing scientific views such as positivism and Interpretivism (Mingers, Mutch & Willcocks, 2013).

6.2.2.1 Critical Realism

Compared to other philosophical positions, Critical realism is a fairly new approach to ontological, epistemological and axiological problems. Orlikowski and Baroudi (1991), asserts that, the primary focus pf critical realist paradigm is to attempt to critique the status quo, by exposing a deep-seated structural contradiction within social systems, and by doing so, help to transform these alienating and restrictive social conditions. The basic beliefs or principles of critical realism is that causal language can be used in describing the world (Bidet & Kouvelakis, 2008). Due to the fact that there are assumptions to all philosophical positions in research, the judgement of these philosophies can only be pragmatic, not specifically in the limited sense of the use of the word by pragmatists but rather in terms of our beliefs so they help in giving better explanations (Easton, 2009). One favourable and strong pragmatic argument of critical realism is that it is performative. In other words, critical realist behaves as though it was true, as if the world was real. They assume, for example, that there is a real world out there. However, there is no way that such an assumption can ever be proved or disproved, as social constructivists, pragmatists and even positivists are ready to argue (Easton, 2009). An assumption which is surely performative and primarily works, especially for the physical world. Sayer (1992), in his book established certain eight key assumptions of critical realism of which a selected few are presented as follows:

- That the existence of the world is independent of our knowledge of it, and that
- Our knowledge of the world could potentially be wrong and weighed down by theory. He also posits that the concepts of true and false fails to provide us a coherent view of the relationship

between knowledge and its object. Nevertheless, knowledge is not immune to empirical check and its effectiveness in informing and explaining successful material practice is not mere accident.

- He also asserts that the development of knowledge is neither through a wholly continuous process, such as the gradual accumulation of facts which is dependent on a stable conceptual framework, nor a discontinuous process, through simultaneous and universal changes in concepts. The world is differentiated and stratified, consisting not only of events, but objects, including structures, which have powers and liabilities capable of generating events. These structures may be present even where, as in the social world and much of the natural world, they do not generate regular patterns of events.
- Critical realism sees social phenomena such as actions, texts and institutions to be all dependent on concept. Hence, we do not only attempt to explain how they are produced or material effects but rather to understand, read or interpret what they mean. Regardless that they have to be interpreted by and from the perspective of the researcher's own derived understanding, basically they continue to exist regardless of how the researcher interprets them. A particular example of such applies to the social world where methods of social science and natural science have both differences and similarities.

Critical realism approach has been best suited to case studies as it has been the case of business to business (B2B) research due to the fact that critical realism provides the needed ontological and epistemological underpinnings and seems ideally matched to case research (Sayer, 1992; Bergin, Wells & Owen, 2008; Easton, 2009; Bidet & Kouvelakis, 2008).

6.2.2.3 Interpretivist Paradigm

Interpretivism, on the other hand, holds that there is an existence of multiple realities, thus reality is socially constructed (Walsham, 1995). Interpretivist researchers go beyond the observable actions of people in the context of social phenomena and understand the subjective meanings they assign to their actions and thereby interpret and understand the reasons behind those actions (Walsham, 2006). Generally, Interpretivism uses an inductive approach to research (Creswell, 2013). Interpretivism argues that truth and knowledge is subjective, culturally, and historically situated based on lived experiences and understanding of them. A researcher can never be completely separate from their own values and beliefs, and these will inevitably inform the way in which data is collected, interpreted and analyzed.

6.2.2.4 Contributors to Interpretivism

Just as with any other paradigm or philosophical propositions, the interpretivist paradigm has had major influences since its inception. Bryman (2008) asserts that there are four main approaches that has been used in interpretivist research: hermeneutics (Heidigger, 1962), Verstehen (Weber, 1947), symbolic interactionism (Mead, 1962) or phenomenology (Schutz, 1962).

Hermeneutics, basically associated with interpreting and understanding texts or documents, helps in building a deeper meaning to documents and hence by extension aiding research. Charambous (2010), for example, uses a hospital scenario in describing the essence of hermeneutics. His description of how assessment is done on patient documents such as folders, and through signs and symptoms could be regarded as a form of 'text' waiting to be interpreted and understand either by a nurse, physician or a healthcare provider of any sought.

Weber (1947), on the other hand, places much emphasis on the exploration of understanding and perception from research participant's or patient's viewpoint to enable a researcher to understand

why a phenomenon exist or why they believe the way they do. To contribute to Interpretivism, Bulmer (1979), presented three core principles of the idea of symbolic interactionism: Humans behave based on their own meanings, meanings are generated from social interaction and that meaning may be adapted based on an individual's perception of a situation or their experience of it. Aldiabat and Le Navenec (2013), for instance, adopted this approach as a way of understanding and working with older people who harbors suicidal ideations.

Finally, phenomenology as a contributor to Interpretivism, focuses on granting interpretation and description life experiences of people and is deeply informed by philosophical assumptions (Wilson, 2015). Interpretivism takes a relativist ontological perspective which suggest that reality is only knowable through socially constructed meanings, that there is no single shared reality (Ritchie & Lewis, 2003). Using another hospital scenario, for example, each patient in a hospital ward will have their own perspective and individual experiences of the care. Their formation of this perceptions and experiences will be informed by their personal interactions with other patients and staff, visitors and previous experiences. Hence, reality has many different representations (Ryan, 2018).

A researcher from the interpretivist paradigm opines that there is nothing as a worldwide and universal truth. Such investigators understand and explains or interpret happenings on the basis of his own outline of orientation and reference. They hold the view that uncommitted and indifferent impartiality is highly not possible and doable and that realism and/or practicality of framework and background is critical (Aliyu et al., 2014). These researchers often possess a relativist and a biased or subjective view of the world. Among the methods used in most cases by interpretivist researchers includes qualitative analysis, field experiments, idiographic experiments induction and exploratory analysis. Currently in research, the Interpretivism paradigm is arguably the most

significant substitute to positivism (Aliyu et al., 2014). This study was most influenced by the interpretivist because the viewpoint of the interpretivist is an ontological which and hence looks at reality or truth as a social construct of the mind's inner feeling.

6.2.2.2 Positivism

Commonly associated with experiments and quantitative research, positivism is considered a form of/progression of empiricism, first labelled as positivism by Auguste Comte in the 19th century. Philips and Burbules (2000), asserted that empiricism is one of two forms of foundationalist philosophy that believes knowledge should be objective and free from bias; that is, free from the values and beliefs of the researcher. Ontologically, positivist researchers believe that truth can be proven (or disproven), reality is not different for each person (e.g., patient weight is the same regardless of who measured it) and observations and measures tells us what reality is. Bryman (2008), suggest four key characteristics of positivism.

- Phenomenalism – only knowledge confirmed by the sciences can genuinely be warranted as knowledge.
- Deductivism – the purpose of theory is to generate hypotheses that can be tested for laws to be proven or disproven.
- Objectivity – science must be conducted in a way that is value free.
- Inductivism – knowledge is gained through gathering of facts that provide the basis for laws.

A Positivist opines that there is an existence of objective reality, and this reality is single and concrete (Kaplan & Duchon, 1988). A positivist researcher or investigator, for example, holds the opinion or the idea that there are permanent and unchanging rules or laws of causation and

associated happenings that the world or universe conforms to; that this rules/laws and its happenings exist in a complex and intricate manner that could be overcome by reductionism; and by deliberately asserting emphasis on impartiality, measurement objectivity and repeatability (Aliyu, 2014). The methods employed by positivist investigators and researchers includes the following: confirmatory analysis, nomothetic experiments, quantitative analysis, laboratory experiments and deduction (Olesen, Westerberg & Klingberg, 2004). The main purpose of the positivist researcher is to learn by the use of instruments about reality so as to discover and explain the general laws that govern reality to help describe, predict and control reality, usually by using deductive process to carry out such research.

This study used a positivist paradigm as it involved the scientific examination of social events and phenomenon through the verification of hypotheses and making deductive reasoning based on established hypotheses. A summary table of the paradigms and their main assumptions is presented in table 6.1 below.

Table 6.1: Summary of Types of Paradigms in Research

Issue	Positivism	Post Positivism	Critical Theory et al	Constructivism	Participatory	References
Ontology	naive realism - "real" reality but apprehendable	critical realism - "real" reality but only imperfectly and probabilistically apprehendable	historical realism - virtual reality shaped by social, political, cultural, economic, ethnic and gender values crystallized over time	relativism - local and specific constructed realities	participative reality - subjective-objective reality, co-created by mind and given cosmos	Walsham (1995); Bryman (2008); Creswell (2013)
Epistemology	dualist/objectivist: findings true	modified dualist/objectivist; critical tradition/community; findings probably true	transactional/ subjectivist; value mediated findings	transactional/ subjectivist; created findings	critical subjectivity in participatory transaction with cosmos; extended epistemology of experiential, propositional and practical knowing; cocreated findings	Kaplan and Duchon (1988); Lincoln, Lynham, and Guba (2011)

Methodology	experimental/ manipulative; verification of hypotheses; chiefly quantitative methods	Modified experimental/ manipulative; critical multiplism; falsification of hypotheses; may include qualitative methods	dialogic/dialectical	hermeneutic/dialectical	political participation in collaborative action inquiry; primacy of the practical; use of language grounded in shared experiential context	Charambous (2010); Aliyu (2014); Olesen, Westerberg and Klingberg (2004)
Axiology	Propositional knowing about the world is an end in itself, is intrinsically valuable	Propositional knowing about the world is an end in itself, is intrinsically valuable	propositional, transactional knowing is instrumentally valuable as a means to social emancipation, which is an end in itself, is intrinsically valuable	propositional, transactional knowing is instrumentally valuable as a means to social emancipation, which is an end in itself, is intrinsically valuable	practical knowing how to flourish with a balance of autonomy, cooperation and hierarchy in a culture is an end in itself, is intrinsically valuable	Orlikowski and Baroudi (1991); Bergin, Wells and Owen (2008); Easton (2009)

Source: Author's Construction

6.3 Methodology

The methodology of a research gives a clear representation of the steps, tools and all the possible means at the disposal of the researcher to investigate or study a phenomenon (Holden, 2004). Establishing the difference between research methodology and research methods has become important for some. According to Kothari (2004), research methods tell us of all the methods/techniques that are used to conduct research whereas research methodology is a way to solve the research problem in a stepwise manner. On broader scale, these terminologies as defined above are based on two broad categorization or classification i.e., quantitative and qualitative methodologies (Creswell, 2013). Defining a specific choice in methodological approach to be taken in research is dependent on the philosophical paradigm a researcher subscribes to, which in turn influences the researcher's method to be used in the conduct of their research (Mukherji & Albon, 2014). This study adopted a quantitative approach to reach it objectives. One of the main objectives of quantitative research approach, is that it allows for the use of figures and numbers to quantify different variations within a phenomenon to help objectively establish a conclusive position with least interference of the researcher. By this method, the researcher is able to disprove or approve a set off relationships among variables and tested through scientific measures to establish a cause and effect (Venkatesh, Brown, & Bala, 2013). Quantitative research, hence, follows a structure to systematically derive results, and usually presents results in the form of statistics and inferences (Creswell, 2014). This research follows such pattern as statistical tools such as the SmartPLS was used through structural equation modeling to test defined hypotheses. Statistical tables and figures were used to provide explanation to analyzed data.

6.3.1 Design

Research design has been defined as all the set approaches used in collecting information to establish a finding and may take the form of qualitative or quantitative method (Johnson & Onwuegbuzie, 2004). The methods employed under a specific approach is the research method. The two major approaches of quantitative or qualitative employs either experiments, surveys or case studies (Sarantakos, 1998). A survey is defined as a research strategy that encompasses any measurement procedure that involves asking questions of respondents (Powell & Connaway, 2004). Direct or indirect contact is made with the units of the study (for example, individuals, organisations, communities) by using systematic methods of measurement such as questionnaires and interviews (Yin, 2003). This study employed a survey method based on a positivist paradigm (Neuman, 2011) and is also appropriate for studies that involves big samples size. According to Creswell (2009), "survey provides a quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of the population". Hence, from the results of the sample, the researcher can then make claim or generalize about the population. In justifying the motives for choosing a quantitative approach as against qualitative and mixed approaches aside being fit for the study in context, was to unearth conclusive evidence rather than just provide information (Neuman, 2011). A Structural Equation Modelling (SEM) is a quantitative technique adopted by this study as it helps in exploring both direct and indirect relationships.

Due to a lack of empirical evidence on the subject matter, an exploratory tool in the form of questionnaire was employed. Participation was entirely voluntary, and participants took part after giving verbal consent. Informed consent was done on each study participant by asking each respondent if they will willingly participate in the study before a respondent is enrolled to be part. Although assurance of anonymity and confidentiality was given to respondents, they were made

aware that they could discontinue their participation in the study whenever they deemed it necessary to do so.

6.3.2 Instrument Development

A questionnaire was designed based on the constructs identified from review of literature and modified to suit the context of the study. In all, there were a total of ten (10) main construct based on which questionnaire was developed. Each construct with the number of items and the source literature have been provided in Tables 6.2 and 6.3 below. The questionnaire used was divided into four main parts: Parts A, B, C and D. Part A was made up of respondents' profile and demographic data, Part B consisted of items on Threat Appraisal and Coping Appraisal, Part C comprised of items on respondents Avoidance Behaviour and the final Part D was made up of items for Generations X, Y and Z. Items on the questionnaire were measured on a five-point Likert-Scale, having end points "1 = Strongly Disagree" and "5 = Strongly Agree". A sample of the questionnaire is attached as Appendix B. After developing the questionnaire, it was subjected to academic review where experts reviewed the individual items, the language construction and the words used for each question, based on which corrections and suggestions were made and were incorporated into the questionnaire by the researcher. The questionnaire was also checked for reliability using scientific tools. To check the reliability, the researcher conducted a pilot study with 30 respondents which helped in checking the Composite Reliability and the Cronbach Alpha values for all the items for the constructs. Both values met the recommended 0.7 figures (Nunnally, 1978). Table 6.2 below provides the constructs that were used, their definitions and key references, whilst Table 6.3 provides the questions used in developing the research instrument and their sources in a questionnaire source matrix.

Table 6.2: Constructs, Definitions, and Key References

Constructs	Definitions	Key References
Perceived Threat		
Susceptibility Threat	This refers to mobile payment users' belief on their degree of vulnerability to mobile payment fraud attacks.	Liang and Xue (2009); Pechmann et al. (2003); Rogers (1975); Witte et al. (1996)
Severity Threat	This refers to mobile payment users' belief about the magnitude of potential harm caused by mobile payment attacks	Liang and Xue (2009); Pechmann et al. (2003); Rogers (1975); Witte et al. (1996)
Coping Appraisal		
Self – efficacy	This refers to mobile payment users' belief about the magnitude of potential harm caused by mobile payment attacks	Compeau and Higgins (1995); Lam and Lee (2006); Liang and Xue (2009); Maddux et al. (1986); Maddux and Rogers (1983); Pechmann et al. (2003); Rogers (1975); Witte et al. (1996)
Perceived Effectiveness	This refers to mobile payment users' belief about whether or not recommended	Compeau and Higgins (1995); Lam and Lee (2006); Liang and Xue

	protective measures can effectively protect them against fraud attacks	(2009); Maddux et al. (1986); Rogers and Mewborn (1976); Witte et al. (1996)
Perceived Security Threat	This refers to mobile payment users' degree of worry/fear about fraud threats. It manifests as security concern.	Leventhal et al. (1965); Liang and Xue (2009); Maddux et al. (1986); Rogers and Mewborn (1976)

	Generational Theory	
Generation X	These are people born from the early 1960s to the year 1974. Such respondents will fall between 46 – 60 years	Levickaitė (2010); Howe and Strauss **(**2000**);** Martin and Tulgan **(**2002).
Generation Y	This generational cohort is said to be born between the period 1975–1989. Such respondents will fall between 31 – 45 years.	Levickaitė (2010); Glum (2015); Holmes (2011); Howe and Strauss **(**2000**);** Martin and Tulgan **(**2002).
Generation Z	This group or generation are people born from the mid-1990s to the late 2000s. Such respondents will fall between 30 – Below years.	Levickaitė (2010); Glum, (2015); Holmes (2011); Howe and Strauss **(**2000**);** Martin and Tulgan **(**2002)

Table 6.3: Questionnaire Source Matrix

CONSTRUCT QUESTIONS	SOURCE(S)
Threat Appraisal	
When it comes to the likelihood of Mobile Payment Fraud, I believe that: 1. I am at high risks of getting defrauded 2. The likelihood that I would be a target of mobile payment fraud attacks is very high 3. The extent of my vulnerability to mobile payment fraud attacks is very high 4. My chances of getting defrauded is high 5. It is extremely likely that I will get defrauded When it comes to severity of mobile payment fraud attacks, I believe that 1. The consequences of fraud attacks for me are very serious 2. In general, the severity of fraud attacks for me is very severe 3. I believe that losing money through mobile payment fraud would be a severe problem. 4. Being defrauded would seriously affect me 5. The consequences of me being defrauded would be great	Chen and Zahedi (2016) Dupuis, Crossler and Endicott-Popovsky (2012) Liang and Xue (2009)
Coping Appraisal	
When it comes to my ability in dealing with mobile payment fraud attacks, I believe that 1. My knowledge for taking preventive actions is very adequate 2. My ability to get appropriate advice on how to take protective actions is very high 3. For me, taking protective action is very easy	Chen and Zahedi (2016)

4. I am more than capable to handle any possible fraud attack
5. I know exactly what to do when attacked without help from anyone
6. I am very confident in my ability to deal with any possible fraud attempt

Dupuis, Crossler and Endicott-Popovsky (2012)

When it comes to the effectiveness of protective actions against mobile payment fraud attacks, I believe that

1. The success rate of my protective actions is very high
2. The chance of stopping fraudulent attacks by taking protective actions is very high
3. The likelihood to neutralize fraud threats is very high
4. My confidence in effectiveness of protective actions is very high

Dupuis, Crossler and Endicott-Popovsky (2012)

5. All information on protective measures can effectively stop any fraud attack
6. My knowledge on protective measures will make it easier to deal with fraud attacks

When it comes to my feelings and concerns about mobile payment fraud attacks, I believe that

1. My fear of exposure to fraudulent attacks is very high
2. The extent of my worry about mobile fraudulent attacks is very high
3. The extent of my anxiety about potential loss due to mobile payment fraud attacks is very high
4. It is risky to use mobile payment system for transactions nowadays
5. Using mobile payment makes me anxious because it is not safe anymore

Liang and Xue (2009)

Avoidance Behaviour	
When it comes to avoiding the use of mobile payment services where threats of being defrauded exist, I have 1. Avoided using mobile payment services 2. Reduced my reliance on mobile payment services 3. Reduced frequency of my use of Mobile payment services	Chen and Zahedi (2016)
4. I am always on the lookout of any fraud attempt to avoid being defrauded 5. Been gathering more information on fraud strategies to avoid possible fraud attacks	Liang and Xue (2009)
Intention to Continuously Use	
1. I intend to continue using mobile payment systems rather than discontinue its use. 2. My intentions are to continue using mobile payment system than use any alternative means. 3. I have in mind to continue using mobile payment system	Thiruselvi et al. (2013)
4. In the future, I would not hesitate to use mobile payment system for transactions. 5. In the future, I will consider mobile payment system to be my first choice when sending money 6. In the future, I intend to increase my use of mobile payment systems	Wangpipatwong, Chutimaskul and Papasratorn (2008)

Source: Author's Construction

6.3.3 Study Context

Mobile Money Service is spread across Africa. According to GSMA 2019 report, there are over 90 countries across the globe that operates some form of mobile money with over $1.3 billion daily transactions happening. This daily transaction value is from global mobile money registered users of 1.2 billion. According to the GSMA 2021 state of mobile money report, there are currently 310 live mobile money services operating in the said 96 countries. 171 of these 310 services are operating in Africa with 157 specifically in sub-Saharan Africa. In the year 2020, Africa had over 562 million mobile money subscribers. This study was conducted in Ghana, a country that is among the leading giants of MM service on the continent of Africa. According to Summary of Economic Data published by the Bank of Ghana, the small West African country with an estimated population of a little over 30 million has 14.7 million active mobile money accounts and 235,000 active agents. MTN Mobile Money, operated by Safaricom, has the largest number of subscribers in the country. According to the report, Ghana's mobile money economy is the fastest growing in Africa and is worth almost $40 billion. The study was therefore conducted in Ghana as the country plays a pivotal role in Africa's mobile money economy.

6.3.4 Sampling Technique and Sample Size

MM service is arguably the most popular service in Ghana currently. Registration unto the service requires that a person would present any form of national ID card, whether, Voters ID Card, Driver's License, Passport, and the Ghana Card (ECOWAS Card). However, to obtain any of these IDs, a person must be 18 years and above. By this, it is assumed that all legal mobile money account holders in the country are above 18years of age. However, it is also important to note that there are also users or consumers of the service who may not necessarily be above 18 years. This is so as people below 18years can access the service by visiting an agent. Any consumer that

presents him/herself at an agent to use the service must present any of the above stated IDs before they can access the service. The study therefore employed convenient sampling technique. Convenient sampling is a form of non-probability sampling technique which involves selecting study respondent who are readily available and may qualify to participate in the study based on some established criteria by the researcher, and was considered appropriate because it helps in establishing tentative hypotheses that can be tested strongly (Galloway, 2005). Anybody registered unto the MM service was hence qualified to participate in the study. In addition, Stratified sampling was used: a probabilistic sampling method that involves breaking down population into strata based on certain classification or characteristic (Qian, 2010). This method was also considered appropriate due to partitioning of the respondents into Generational cohorts of X, Y and Z.

Regarding the sample size for the study, statistics from Bank of Ghana indicate that, by the end of the year 2021, there were a total of over 17 million active mobile money accounts (BoG Payment Systems Oversight Report, 2022). Thus, according to the Krejcie and Morgan table, when a study's population is over a million, a sample size of 384 is enough representation (Krejcie & Morgan, 1970). In all, 422 respondents verbally consented to participate in the study after the researcher had explained the purpose of the study and questionnaires were administered to them by researcher. Therefore, this sample size is deemed fit for the study as it falls within the minimum recommended threshold by Krejcie and Morgan (1970).

6.3.5 Data Collection

Data was collected by the use of administered questionnaires. Out of the 422 questionnaires that were administered to the target respondents, a total of 384, which represent approximately 91%, were retrieved after several follow ups and were considered valid and were used for the study.

6.3.6 Measurement

The PLS-SEM method which uses the SmartPLS 3.2.6 was used for obtaining the inferential statistics of the study constructs (Ringle, Wende, & Becker, 2015). The SmartPLS 3.2.6 (PLS-SEM) was chosen based on the fact it is able to handle relatively small sample sizes, and particularly as the data was not normally distributed (Hair et al., 2014). Test for skewness and kurtosis were used in examining whether data used for the study was normally.

For a relatively big sample size of 384 respondents, this approach was considered most appropriate as against the Kolmogorov–Smirnov and Shapiro–Wilks tests which is appropriate for a small sample size (Dallal & Wilkinson, 1986; Royston, 1982). The result showed the data was not normally distributed and are presented in the results and analysis section, further justifying the use of the PLS-SEM approach (West et al., 1995).

6.4 Chapter Summary

This Chapter of the study presented the methodology of the research. In this chapter, the paradigms and types of reasoning in research were discussed. The major paradigms in research, thus, positivism, interpretivism and critical realism, were all discussed as well as major contributors to these paradigms. The chapter also discussed the actual methods that were employed for the study i.e., Study Design, Sampling Techniques and Sample Size, Measurement, Scale Development, etc. The next chapter discusses the results of the study.

CHPATER SEVEN

RESULTS AND ANALYSIS

7.1 Chapter Overview

Discussions from the previous chapter centred on the conceptual framework of the study. Presentation made in this chapter of the study will focus on the results of the research. Issues discussed includes results obtained after running data collected from the field. Descriptive statistics about respondents and all the constructs used for the study are presented. The presentation also covers all the research constructs used for the study, as well as analysis of the structural equation model. The chapter concludes with a summary of the issues discussed in this chapter.

7.2 Descriptive Statistics of Respondents

The descriptive statistics of respondents covers the gender categorization of respondents, their age groups, religious affiliation, level of education, occupational status, marital status, registration unto the mobile money service, how regular the respondent uses the service and the generational cohort a respondent belongs to. The questionnaire used for this survey was measured on a five-point Likert scale from point 1 to point 5, where 1 represented strongly disagree and 5 represented strongly agree.

7.2.1 Gender

As has been stated, there were a total of 384 respondents who participated in the study. By grouping these respondents into two groups, one representing male and the other representing females, there were a total of 188 males which represented forty-nine percent [49%] and 196 females which represented fifty-one percent [51%] of the total respondents. This shows an almost even distribution for the two gender groups which is also particularly good for comparisons of the findings. This is presented in table 7.1 below.

7.2.2 Age Groups

In terms of age distribution, there were a total 45 respondents representing about twelve percent [11.7%] who were below the age of 20 years. For age groups between twenty [20] to twenty-nine [29] years, there were a total of 123 respondents which represented thirty-two percent [32%] and were the largest group of respondents who participated in the study. The next age group was those within the age of thirty [30] to thirty-nine [39], which had a total of 100 respondents and represented twenty-six percent [26%] of the total respondents. This group was followed by respondents between the ages of forty [40] to forty-nine [49], having a total of 48 respondents representing almost thirteen percent [12.5%]. The next group was respondents between fifty [50] to fifty-nine [59] which had a total of 47 respondents representing a little above twelve percent [12.2%], and the final age group being those from sixty years [60] and above, which had a total of 21 respondents representing five and a half percent [5.5%]. This can be seen in table 7.1 below.

7.2.3 Religion

Regarding religion, there were three main categorizations: Christian, Muslims and Others, depicted in table 7.1 below. In all, there were a total of 59 Muslim respondents which represented a little above fifteen percent [15.4%], a total of 300 Christian respondents representing seventy percent [78.1%], and finally respondents who belong to other faith outside these two main groups being 25 and representing six and a half percent [6.5%]. This finding of such large group of Christian respondents was particularly surprising as the data was collected from large spreads of communities which had large presentation of the two main faith groups i.e., Christians and Muslims.

7.2.4 Educational Level

In terms of educational level of respondents, there were six [6] main categorizations: Primary School, Junior Hugh School leavers, Senior High School, Diploma or Degree holders, Masters degree holders and PhD holders. For primary school leavers, there were a total of 13 respondents, which represented a little above three percent [3.4%]. For junior high school leavers, there were a total of 68 respondents, which represented almost eighteen percent [17.7%] of total respondents. Senior High School leavers were 103 in number, representing almost twenty-seven percent [26.8%] of the total respondents. There were a total 162 respondents who had either bachelor's degrees or diploma certificates and represented a little above forty two percent [42.2%]. They were the highest group of respondents in the study, and when combined with SHS leavers, represented almost seventy percent [70%] of the total number of respondents who participated in the study, and gave a correct view of the current Ghanaian society in terms of education. For Masters degree holders, there were a total of 31 respondents which represented eight percent [8.1%] of the total number of respondents and 7 PhD holders which represented almost two percent [1.8%]. This is depicted in table 7.1 below.

7.2.5 Occupational Status

As can be seen from table 7.1 below, there were five [5] main categorizations for occupational status: Students, Self–Employed, Private Sector Worker, Public Sector Worker, and Unemployed. There were 75 student respondents representing nineteen and half percent [19.5%]. For the Self-Employed category, there were a total of 121 respondents, which represented thirty-one and half percent [31.5%], the largest in this category. There was a total of 91 Private Sector Workers which represented almost twenty-four percent [23.7%], 69 Public Sector Workers which represented

eighteen percent [18.0%] and 28 unemployed respondents which represented a little above seven percent [7.3%].

7.2.6 Marital Status

There were five categorizations under this group: Single, Married, Divorced, Widow(er), and Others, as can be seen in table 7.1 below. Respondents who were single constituted the largest group among the categories. There was a total of 201 respondents, which represented a little above fifty-two percent [52.3%]. This was followed by the married group which had 142 respondents which represented thirty-seven percent [37%]. There were total of 22 divorcees which represented almost six percent [5.7%], 10 in the widow(er) group representing a little above two and half percent [2.6%] and 9 for the "Other" group which also represented a little above two percent [2.3%]. This can be seen in table 7.1 below.

7.2.7 Registered on Mobile Payment System

Ascertaining whether respondents were registered unto mobile money service was important as not all users of the mobile money service are actually registered unto the service. As indicated under the type of service available to the users, there is the Over-The-Counter (OTC) which a customer can access from an agent without necessarily being registered unto the service. In this study, such persons are still considered as users of the service. There were two groups under this category: those who are registered unto the service [Yes] and those who are not registered unto the service [No]. There were 370 respondents who have been registered unto the service representing 96.4 percent [96.4%], and 14 respondents representing 3.6 percent [3.6%] who have not been registered unto the service, as can be seen in table 7.1 below. This is not particularly surprising as the service is really widespread in Ghana.

7.2.8 Regularity of Use

Regarding how regular respondents use the service, respondents were asked to score themselves between 1 to 10, where a score between 1–3 was grouped as Low, a score between 4–6 was categorized as Moderate, and a score between 7–10 categorized as High. 24 respondents which represented a little above six percent [6.3%] fell under the Low category. There were 118 respondents representing almost thirty-one percent [30.7%] who fell under the Moderate category, and 242 respondents representing sixty-three percent [63 %] who fell under the High category. This is depicted in table 7.1 below.

7.2.9 Owns any Social Media Account

For respondents who owned a social media account, there were two groups, thus, those who had any form of social media account and those who did not have any social media presence. A total of 315 respondents representing eighty-two percent [82%] had social media account(s), and 69 respondents representing eighteen percent [18%] not having any social media account(s), as can be seen in table 7.1 below.

7.2.10 Generation X, Y, and Z

The three generational groups: Generation X, Y and Z, were represented in table 7.1 as follows. There were 77 Generation X respondents, representing a twenty one percent [21%], 119 Generation Y respondents, representing thirty two point nine percent [32.9%], and 167 Generation Z respondents, representing forty-six percent [46%].

Table 7.1: Descriptive Statistics of Respondents

Variable	Groupings	Frequency	Percent
Gender	Male	188	49.0
	Female	196	51.0
Age	Below 20	45	11.7
	20-29	123	32.0
	30-39	100	26.0
	40-49	48	12.5
	50-59	47	12.2
	60 and Above	21	5.5
Religion	Muslim	59	15.4
	Christian	300	78.1
	Any Other	25	6.5
Educational Level	Primary	13	3.4
	JHS	68	17.7
	SHS	103	26.8
	Diploma/Degree	162	42.2
	Masters/MPhil	31	8.1
	PhD	7	1.8
Occupational Status	Student	75	19.5
	Self-Employed	121	31.5
	Private Sector Worker	91	23.7
	Public Sector Worker	69	18.0

	Unemployed	28	7.3
Marital Status	Single	201	52.3
	Married	142	37.0
	Divorced	22	5.7
	Widow(er)	10	2.6
	Others	9	2.3
Registered on Mobile Payment System	Yes	370	96.4
	No	14	3.6
Do you use mobile payment system for transactions?	Yes	371	96.6
	No	13	3.4
Score on Regularity of Usage	1-3 (Low)	24	6.3
	4-6 (Moderate)	118	30.7
	1-10 (High)	242	63.0
Owns Any Social Media Account	Yes	315	82.0
	No	69	18.0
Generation	X	77	21.2
	Y	119	32.9
	Z	167	46

7.3 Descriptive Statistics of Constructs

In this section of the study, we discuss the descriptive statistics of the seven main constructs that were used for the study, i.e., Susceptibility Threat, Severity Threat, Self-Efficacy, Perceived

Effectiveness, Perceived Security Threat, Avoidance Behaviour and Intention to Continuously Use. Their Means, Standard Deviations, Skewness and Kurtosis of each of the construct are discussed. Findings for each construct are summarized and presented in table 7.8 below. The Mean scores tells the average score for each construct, whiles the Standard Deviation tells the spread of the data. Skewness refers to the rate or manner with which items of a construct are clustered around the mean or average. A perfectly skewed items on a construct will usually depict a bell like shape (Kothari, 2008). It is the measure of asymmetry of the items on a construct. Measuring Skewness is important as it gives an idea of the shape of the bell like curve and can be used to study series formation when, for example, plotted on a graph. Kurtosis, on the other hand, tells the researcher how flat the top of the bell like shape or curve is. This measure tells the humpedness of the curve as well as pointing to the nature of distribution of items in the middle of a series (Kothari, 2008).

7.3.1 Susceptibility Threat Construct

This construct had five items as a measure. By using a five-point Likert scale, susceptibility threat had a mean value of 3.06, and a standard deviation of 1.02. A mean value of 3.06 shows that the threat of being susceptible was moderate among respondents. This construct had a Skewed value of -0.094 and a Kurtosis value of -0.764. This is depicted in table 7.2 below:

Table 7.2: Descriptive Statistics of Susceptibility Construct (N=384)

Code	Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis
SupT1	I believe I am at high risks of getting defrauded through mobile payment fraud	3.02	1.263	-0.107	-1.154
SupT2	The likelihood that I would be a target of mobile payment fraud attacks is very high	3.18	1.225	-0.244	-1.074

SupT3	It is extremely likely that I will be a victim of mobile payment fraud	2.97	1.251	-0.029	-1.148
SupT4	My chances of getting defrauded through mobile payment fraud is very high	3.09	1.203	-0.057	-1.086
SupT5	The extent of my vulnerability to mobile payment fraud attacks is very high	3.03	1.224	-0.017	-1.113
	Overall	**3.06**			

7.3.2 Severity Threat Construct

The construct severity threat also had five items as a measure. Again, by using a five-point Likert scale, this construct had mean value of 3.8, and a standard deviation of 0.8. For a five-point Likert scale, a mean value of 3.8 depicted that severity threat among respondents was high. This construct had a skewed value of -0.65 and a kurtosis value of 0.30. This is depicted in table7.3 below:

Table 7.3: Descriptive Statistics for Severity Construct (N=384)

Code	Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis
SevT1	I believe the consequences of mobile payment fraud for me is very serious	3.69	1.007	-0.83	0.235
SevT2	I believe that losing money through mobile payment fraud would be a severe problem.	3.92	0.95	-0.955	0.662
SevT3	I believe mobile payment fraud on me would seriously affect me	3.85	1.047	-0.954	0.417

SevT4	The consequences of mobile payment fraud on me would be great	3.66	1.077	-0.806	0.073
SevT5	The severity of mobile payment fraud attacks for me would be very high	3.71	1.062	-0.667	-0.344
	Overall	**3.76**			

7.3.3 Self–Efficacy Construct

Next is the self-efficacy construct. This construct had six items that were used as a measure. A five-point Likert scale was used, where the construct had a mean value of 3.39, and a standard deviation of 0.94. For a five-point Likert scale, a mean value of 3.39 showed that Self-Efficacy among respondents was moderate. This construct had a Skewed value of -0.447 and Kurtosis value of -0.380. This is demonstrated in table 7.4 below.

Table 7.4: Descriptive Statistics for Self-Efficacy Construct (N=384)

Code	Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis
SelfE1	My knowledge for taking preventive actions against mobile payment fraud is very adequate	3.48	1.147	-0.54	-0.577
SelfE2	My ability to get appropriate advice on how to take protective actions against mobile payment fraud is very high	3.49	1.126	-0.574	-0.53
SelfE3	I am more than capable to handling any possible mobile payment fraud attack	3.22	1.153	-0.265	-0.878

SelfE4	I know exactly what to do when mobile payment fraud attempt is made on me without help from anyone	3.38	1.188	-0.407	-0.831
SelfE5	I am very confident in my ability to deal with any possible mobile payment fraud attempt	3.38	1.182	-0.462	-0.746
SelfE6	For me, taking protective action is very easy	3.43	1.152	-0.375	-0.743
	Overall	**3.4**			

7.3.4 Perceived Effectiveness Construct

There were five items that were used to measure the construct perceived effectiveness. Again, by using a five-point Likert scale, this construct had a mean value of 3.44, and a standard deviation of 0.838. Using a five-point Likert scale, a mean value of 3.44 showed that perceived effectiveness was moderate among respondents. It had a Skewed value of -0.590 and Kurtosis value of 0.091. This is shown in table 7.5 below:

Table 7.5: Descriptive Statistic for Perceived Effectiveness (N=384)

Code	Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis
PerEff1	The success rate of my protective actions against mobile payment fraud is very high	3.37	1.098	-0.362	-0.703

PerEff2	The chances of stopping fraudulent attacks by taking protective actions is very high	3.33	1.073	-0.46	-0.584
PerEff3	The likelihood to neutralize mobile payment fraud threats is very high	3.39	0.984	-0.494	-0.201
PerEff4	All information on protective measures can effectively stop any mobile payment fraud attack	3.43	1.05	-0.541	-0.353
PerEff5	My knowledge on protective measures will make it easier to deal with mobile payment fraud attacks	3.67	1.019	-0.712	0.092
	Overall	**3.44**			

7.3.5 Perceived Security Threat Construct

The construct perceived security threat also had six items as a measure. Again, by using a five-point Likert scale, this construct had had a mean value of 3.16, and a standard deviation of 0.953 for a five-point Likert scale, a mean value of 3.16 depicted that perceived security threat among respondents was moderate. This construct had a Skewed value of -0.240 and Kurtosis value of -0.656. This is depicted in table 7.6 below:

Table 7.6: Descriptive Statistic of Perceived Security Threat (N=384)

Code	Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis

PerST1	My fear of exposure to mobile payment fraud attacks is very high	3.29	1.108	-0.4	-0.786
PerST2	The extent of my worry about mobile payment attacks is very high	3.28	1.12	-0.28	-0.866
PerST3	Trouble caused by mobile payment fraud threatens me	3.23	1.149	-0.219	-0.96
PerST4	I feel it is very risky to use mobile payment system for transactions nowadays	3.07	1.227	-0.087	-1.066
PerST5	Using mobile payment system for transactions makes me anxious because it is not safe anymore	2.97	1.229	-0.037	-1.076
PerST6	The extent of my anxiety about potential loss due to mobile payment fraud attacks is very high	3.16	1.197	-0.191	-0.977
	Overall	**3.16**			

7.3.6 Avoidance Behaviour Construct

The construct avoidance behaviour also had five items as a measure. Again, by using a five-point Likert scale, this construct had had a mean value of 2.89, and a standard deviation of 0.866. For a five-point Likert scale, a mean value of 2.89 showed that avoidance behaviour among respondents was moderate. This construct had a Skewed value of 0.124 and Kurtosis value of -0.266, as shown in table 7.7 below:

Table 7.7: Descriptive Statistic of Avoidance Behaviour (N=384)

Code	Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis
AVB1	I have avoided using mobile payment services in order to prevent mobile payment fraud attacks	2.36	1.129	0.867	-0.112
AVB2	I have reduced my reliance on mobile payment services in order to prevent mobile payment fraud attacks	2.59	1.23	0.434	-0.964
AVB3	I am always on the lookout of any mobile payment fraud attempt to in order to avoid being defrauded	3.42	1.206	-0.572	-0.732
AVB4	I have been gathering more information on mobile payment fraud strategies in order to avoid possible fraud attacks	3.4	1.136	-0.531	-0.558
AVB5	I have reduced the frequency with which I use mobile payment services	2.67	1.283	0.432	-1.027
	Overall	**2.89**			

7.3.7 Construct for Intention to Continuously Use

Respondents' intention to continuously use a service was also a separate construct measured on six items using a five-point Likert scale. This construct had a mean value of 3.78, and a standard deviation of 0.811. For a five-point Likert scale, a mean value of 3.78 showed that respondent's

intention to continuously use the mobile money service was high. This construct had a Skewed value of -0.777 and Kurtosis value of 0.898, as shown in table 7.8 below:

Table 7.8: Descriptive Statistic of Intention to Continuously Use (N=384)

Code	Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis
IntentCU1	I intend to continue using mobile payment systems rather than discontinue its use.	3.88	1.002	-1.12	1.006
IntentCU2	My intentions are to continue using mobile payment system than use any alternative means	3.69	1.047	-0.897	0.362
IntentCU3	I have in mind to continue using mobile payment system	3.85	0.955	-1.05	1.007
IntentCU4	In the future, I would not hesitate to use mobile payment system for transactions.	3.72	1.077	-0.892	0.205
IntentCU5	In the future, I will consider mobile payment system to be my first choice when sending money	3.77	0.98	-0.682	0.113
IntentCU6	In the future, I intend to increase my use of mobile payment systems	3.79	0.986	-0.743	0.227
	Overall	**3.78**			

Hall and Wang (2005), assert that, there is usually an indication of non-normality when there is high level of skewness or kurtosis among a collected data set as a result of the presence of outliers

in the set of data. It is a rule of thumb that when bell shape fall between -1 to +1, or -2 to +2 or even 3, the data is considered to be normally distributed (Schumacker & Lomax, 2004). Other scholars (Byrne, 2013) have proposed that a cut-off point lesser than 7 should be considered acceptable for kurtosis, and skewed values between -3 to +3 can be deemed as normal distribution. A summary of the above is depicted in a composite normality test table showing the means, standard deviations, skewness and kurtosis of the study's constructs. This is shown in table 7.9 below:

Table 7.9: Descriptive Statistic of Normality Test and Normality Test (Composite)

Variable Indicators	Mean	Std. Dev.	Skewness	Kurtosis
Generation X Y Z	2.18	0.812	-0.340	-1.405
Susceptibility Threat	3.0578	1.02231	-0.094	-0.764
Severity Threat	3.7646	0.79502	-0.653	0.300
Self-Efficacy	3.3967	0.94098	-0.447	-0.380
Perceived Effectiveness	3.4380	0.83832	-0.590	0.091
Perceived Security Threat	3.1649	0.95481	-0.240	-0.656
Avoidance Behaviour	2.8875	0.86610	0.124	-0.266
Intention on Continuous Usage	3.7826	0.81067	-0.777	0.898

7.3.8 Common Method Variance Bias

Checking for the presence of common method bias was important. This is because as recommended by literature, this check is important when a single data gathering instrument was used for collecting research data (Lings & Greenly, 2010). By using Podsakoff et al. (2003) and Andersson & Bateman (1998) recommended approach, the researcher performed the Harman's

(1967) one factor test which requires the performing of exploratory factor analysis where one extracted factor will have a total variance below 50%. On the other hand, a researcher can extract factors that have Eigen values that are greater than one [1] and make sure no single factor is able to explain over 50% of the total variance. This full exploratory factor analysis can also help to explain the common method variance bias. As can be seen from tables 7.10 and 7.11 below, the variance that was explained by the highest single factor variance (as can be seen factor 1) is 37.031% < 50% variance. As can be seen, with a value of 37.031% there is no problem with common method variance bias. The issue of common method variance only becomes a problem when the variance is almost at 70%, and further also that when common method variance falls between 30% and 60%, almost all correlations are likely to have confidence interval of between 95% or above (Fuller et al., 2015). Other measures were taken with the designing of the questionnaire to minimize or prevent acquiescence bias (Lings & Greenly, 2010).

Table 7.10: Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.466	24.909	24.909	9.466	24.909	24.909
2	4.876	12.833	37.742			
3	3.551	9.344	47.086			
4	2.092	5.506	52.592			
5	1.952	5.137	57.729			
6	1.477	3.888	61.617			
7	1.352	3.557	65.174			
8	1.205	3.171	68.345			
9	0.974	2.563	70.908			
10	0.925	2.435	73.343			
11	0.731	1.924	75.268			
12	0.709	1.865	77.133			
13	0.677	1.782	78.914			
14	0.653	1.719	80.634			
15	0.554	1.458	82.092			
16	0.525	1.383	83.474			
17	0.513	1.349	84.823			
18	0.465	1.224	86.048			
19	0.429	1.130	87.178			

20	0.413	1.088	88.266			
21	0.375	0.987	89.253			
22	0.347	0.914	90.167			
23	0.332	0.873	91.040			
24	0.322	0.848	91.888			
25	0.309	0.814	92.702			
26	0.291	0.765	93.467			
27	0.275	0.725	94.192			
28	0.264	0.696	94.887			
29	0.245	0.645	95.532			
30	0.240	0.632	96.164			
31	0.229	0.602	96.766			
32	0.211	0.555	97.321			
33	0.206	0.543	97.864			
34	0.183	0.482	98.347			
35	0.177	0.465	98.812			
36	0.166	0.437	99.249			
37	0.145	0.380	99.630			
38	0.141	0.370	100.000			

Note: Since the percentage value is 24.909% which is less than 50%, common method bias is not an issue

Table 7.11: Total Variance Explained (Composite Variables)

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.592	37.031	37.031	2.592	37.031	37.031
2	1.396	19.949	56.981			
3	1.097	15.666	72.647			
4	0.582	8.312	80.959			
5	0.541	7.729	88.688			
6	0.437	6.242	94.930			
7	0.355	5.070	100.000			

Note: Since the percentage value is 37.031% which is less than 50%, common method bias is not an issue

7.4 Analysing the Measurement Model

Before a structural equation modelling (SEM) analysis can be performed, two key requirements are needed to be examined: the model for measurement (measurement model) and the model for the structure of the equation (structural model). The purpose of running the measurement model is to examine the nature or relationship or the underlying relationship between the latent variables and their measures in the study. The structural model on the other hand examines the relationship within the constructs of the study. The examination of the measurement model requires, first,

performing a pre-test on the instrument or questionnaire that will be used for the data gathering process. This is important to ascertain whether all the items on the questionnaire can correctly measure that which it is supposed to measure and is particularly distinct from other items on the instrument. According to Sarstedt, Ringle and Hair (2017), it is best that the retaining factor loadings of the item is 0.708 or above to make sure the loading is significant.

7.4.1 Item Validity

Generally, based on the preliminary analysis of measurement model, Hulland (1999), asserts that not all the construct indicators are made in the final analysis, since researchers frequently obtain weaker outer loadings (<0.70). Indicators with lower outer loadings between 0.40 and 0.70 should be considered for removal, but sometimes these weaker outer loadings are retained on the basis of their contribution to content validity. However, indicators with very low outer loadings (below 0.40) should be eliminated from the construct (Bagozzi, Yi & Phillips, 1991; Hair et al., 2011).

At the same time, the loading values equal to and greater than 0.40 (Hulland, 1999), and 0.50. 0.60 (Byrne, 2016) is acceptable if it contributes to the average variance extracted (AVE) scores of greater than 0.5. Therefore, certain items are eliminated in order to achieve AVE score greater than 0.5. Based on this, indicators (below 0.50) that do not meet the requirements are deleted.

In all there were 38 items for the constructs on the questionnaire. After examining the initial loadings of the items used for the study, very few items had loading values below the recommended 0.708. Out of six (6) items for each of the constructs, Severity Threat and Avoidance Behaviour had two (2) items falling below the recommended loading value and so were sequentially deleted until the recommended construct measures were obtained (Hair et al., 2014). These offending items at pretesting were **SevT2 & SevT3** (Indicators that measures Severity Threats) and **AVB3 & AVB4** (Indicators that measure Avoidance Behaviour). The items were

deleted sequentially until acceptable construct measures were obtained (Hair et al., 2014). The revised model is presented in the figure 7.1 below. Further, for each of the constructs used for the study, the highest and lowest factor loadings for construct items are provided.

For Susceptibility threat, among the five items, the item with the highest factor loading was: respondents' chances of getting defrauded through mobile payment fraud is very high **(SupT4; 0.893)**; and the one having the lowest factor loading was: respondents believing they are at high risks of getting defrauded through mobile payment fraud **(SupT1; 0.758)** as indicated in table 7.1 below.

The construct Severity Threat also had five items. The item that had the highest factor loading was whether the severity of mobile payment fraud attacks on them would be very high **(SevT5; 0.898)**; and the item having the lowest factor loading was: whether the consequences of mobile payment fraud on them would be great **(SevT4; 0.683)** as indicated in table 7.1 below.

For the Self-Efficacy construct, the item that had the highest factor loading was whether respondents were very confident in my ability to deal with any possible mobile payment fraud attempt **(SelfE5; 0.845)**; and the item with the least factor loading was: whether respondents taking protective action was very easy **(SelfE6; 0.746)**, as is depicted in table 7.1 below.

The highest factor loading for Perceived Effectiveness was whether respondent's chances of stopping fraudulent attacks by taking protective actions was very high **(PerEff2; 0.878)**; and the item with the least factor loading was: whether respondents' likelihood to neutralize mobile payment fraud threats was very high **(PerEff3; 0.735)**. This is depicted in table 7.1 below.

With regards to Perceived Security Threat, among the six items, the item with the highest factor loading was: whether the extent of respondents' anxiety about potential loss due to mobile payment

fraud attacks was very high **(PerST6; 0.870)**; and the one having the lowest factor loading was: whether respondents fear of exposure to mobile payment fraud attacks was very high **(PerST1; 0.744)**. This is indicated in table 7.1 below.

The item with the highest factor loading for Avoidance Behaviour was whether respondents have reduced their reliance on mobile payment services in order to prevent mobile payment fraud attacks **(AVB2; 0.912)**; and the item with the least factor loading was: whether respondents have avoided using mobile payment services in order to prevent mobile payment fraud attacks **(AVB1; 0.851)**, as depicted in table 7.1 below.

And then finally, for the construct Intention on Continuous Usage, among the six items, the item with the highest factor loading was: whether respondents have in mind to continue using mobile payment system **(IntentCU3; 0.832)**; and the one having the lowest factor loading was: whether in the future, respondents would not hesitate to use mobile payment system for transactions **(IntentCU4; 0.768)**. This is also depicted in table 7.1 below.

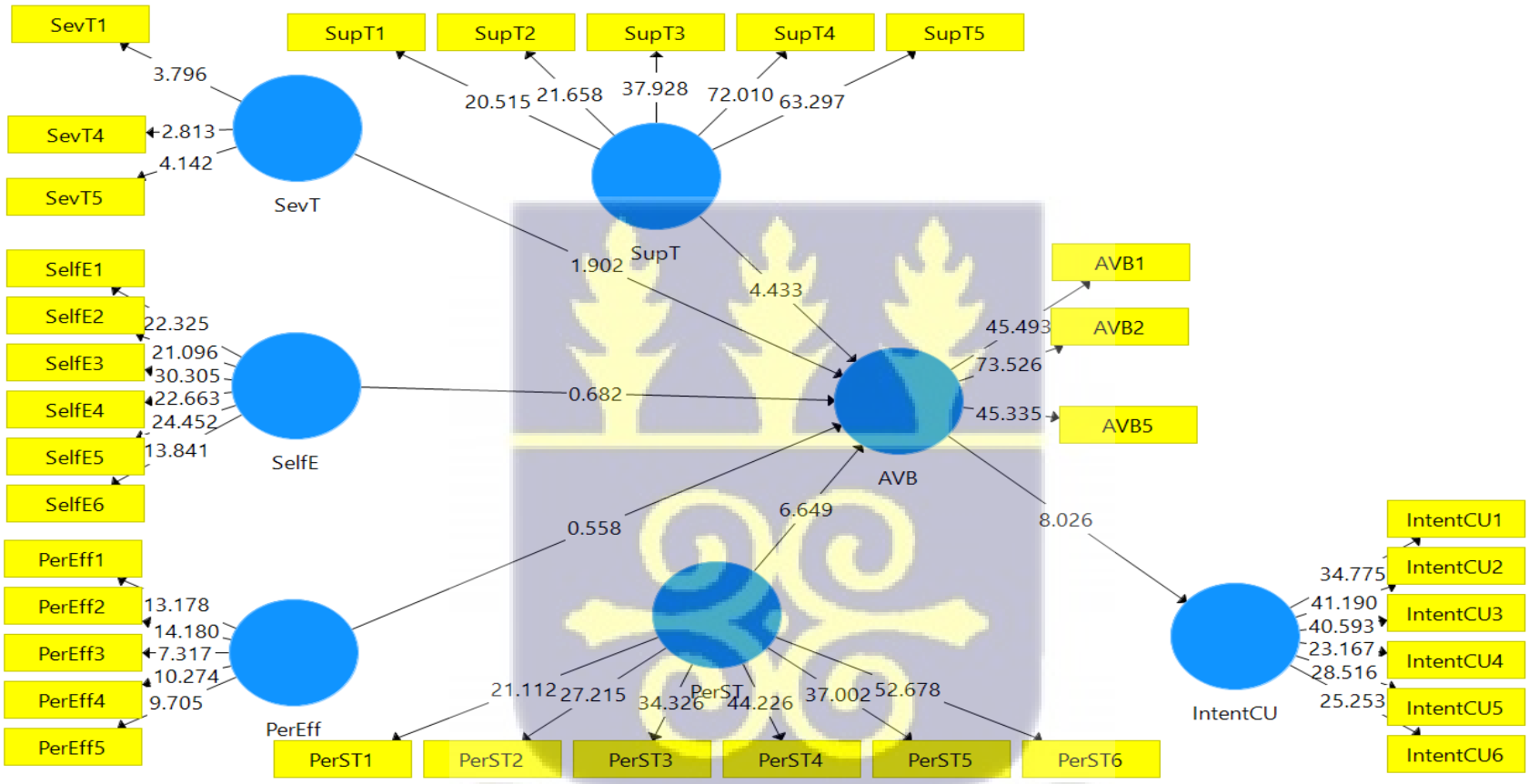


Figure 7.1: PLS-SEM Structural Model

Items deleted during CFA

SevT2 & SevT3 (Indicator to measure Severity Threats)

AVB3 & AVB4 (Indicators to measure Avoidance Behaviour)

Summary: Original number of items = 38 Revised number of items = 34

Table 7.12 below shows the revised form of the various constructs, their related codes and the values for their outer loadings.

Table 7.12: Indicator Loadings

Variable	Code	Outer Loadings
Avoidance Behaviour	AVB1	0.851
	AVB2	0.912
	AVB5	0.857
Intention on Continuous Usage	IntentCU1	0.793
	IntentCU2	0.830
	IntentCU3	0.832
	IntentCU4	0.768
	IntentCU5	0.808
	IntentCU6	0.796
Perceived Effectiveness	PerEff1	0.824
	PerEff2	0.878
	PerEff3	0.735
	PerEff4	0.763
	PerEff5	0.773
Perceived Security Threat	PerST1	0.744
	PerST2	0.777
	PerST3	0.818
	PerST4	0.836
	PerST5	0.830
	PerST6	0.870

Self-Efficacy	SelfE1	0.806
	SelfE2	0.797
	SelfE3	0.829
	SelfE4	0.832
	SelfE5	0.845
	SelfE6	0.746
Severity Threat	SevT1	0.807
	SevT4	0.683
	SevT5	0.898
Susceptibility Threat	SupT1	0.758
	SupT2	0.770
	SupT3	0.840
	SupT4	0.893
	SupT5	0.868

Table 7.13 below indicates a summary of the total number of items that were used as a measure for each construct.

Table7.13: Original and Final Value of Measurement Items

Constructs	Original No. of Items	Final No. of Item
Susceptibility Threat	5	5
Severity Threat	5	3
Self-Efficacy	6	6
Perceived Effectiveness	5	5

Perceived Security Threat	6	6
Avoidance Behaviour	5	3
Intention on Continuous Usage	6	6

7.4.2 Assessing for Convergent Validity

Concerning convergent validity, Sarstedt et al. (2017) and Henseler et al. (2009) assert that the acceptable minimum of Cronbach's alpha should be 0.7, a minimum composite reliability of 0.7, as well as an AVE of at least 50% per construct in order to satisfy an acceptable convergence validity. Other scholars (Efron & Gong, 1983; Tortosa, Moliner, & Sanchez, 2009) have also recommended the use of statistical bootstrap t-values testing method (5000 sub-samples) to ensure that each item loading is statistically significant before concluding on adequate convergence validity. In this study, all the seven constructs had Cronbach's alpha ranging from 0.757 to 0.898, and composite reliability ranging from 0.841 to 0.921, and AVE ranging from 0.634 to 0.763, all meeting the minimum recommended by Sarstedt et al. (2017) and Henseler et al. (2009). Furthermore, each of the item loadings remaining, after removing the items which didn't meet the required standard for the model, was statistically significant using bootstrap t-values (5000 sub-samples) (Efron & Gong, 1983; Tortosa et al., 2009). Therefore, convergent validity had been adequately met. Table 7.14 provides a summary of the convergence validity test. Below are the results for each of the seven constructs.

7.4.3 Assessing for Construct Reliability

For many years, the use of Cronbach's alpha to measure for how reliable a construct is, or its internal consistency, has become the traditionally accepted means. It is however important to note that, the use of such has not come with its own criticisms by many scholars. This is as a result of

one assumption related to the Cronbach's alpha, thus, all loadings of the constructs indicators are the same, and so some current researchers have rather adopted the composite reliability as a better measure (Hair et al., 2011; Sarstedt et al., 2017) basically because the composite reliability ignores that same assumption but rather places more priority on indicators own reliability when estimating a model, as it is the case when using PLS-SEM (Hair et al., 2011). The PLS-SEM as it was used for the statistical analysis study, for example, consciously places more emphasis on the composite reliability, due to its emphasis on the reliability of individual indicators. Reliability values between 0.5 and 0.7 are the acceptable recommended values (Byrne, 2016; Sarstedt et al., 2017). According to Hair et al. (2011), the AVE and composite reliability can be complemented when loading figures are between 0.4 and 0.7 and must be considered for deletion.

Susceptibility Threat was examined using five (5) items. The Cronbach's alpha for these five items was 0.886, with a composite reliability of 0.915 and an average extracted (AVE) estimate of 0.685, as can be seen in table 7.14 below. In addition, each of the item loading was statistically significant using bootstrap t-values (5000 sub-samples). Severity Threat construct was examined using five (5) items. The Cronbach's alpha for these five items was 0.757, with a composite reliability of 0.841and an average extracted (AVE) estimate of 0.641, as can be observed in table 7.14 below. Furthermore, each of the item loading was statistically significant using bootstrap t-values (5000 sub-samples). Concerning Self-Efficacy, there were six (6) items that were used to examine the construct. The Cronbach's alpha for the six items was 0.897, a composite reliability of 0.919 and an average extracted (AVE) estimate of 0.656. This can be seen in table 7.14 below. Each of the item loading was statistically significant using bootstrap t-values (5000 sub-samples). With the construct Perceived Effectiveness, there were five (5) items that were used for examination. The Cronbach's alpha for the six items was 0.862, a composite reliability of 0.896 and an average

extracted (AVE) estimate of 0.634, as indicated in table 7.14 below. Each of the item loading was statistically significant using bootstrap t-values (5000 sub-samples). Perceived Security Threat was examined using six (6) items. The Cronbach's alpha for these six items was 0.898, with a composite reliability of 0.921 and an average extracted (AVE) estimate of 0.662. This is depicted in table 7.14 below. In addition, each of the item loading was statistically significant using bootstrap t-values (5000 sub-samples). The construct Avoidance Behaviour was examined with five (5) items. The Cronbach's alpha for the five items was 0.845, having a composite reliability of 0.906 and an average extracted (AVE) estimate of 0.763, as seen in table 7.14 below. Each of the item loading was statistically significant using bootstrap t-values (5000 sub-samples).

Intention to Continuously Use was examined using six (6) items. The Cronbach's alpha for these six items was 0.891, with a composite reliability of 0.917 and an average extracted (AVE) estimate of 0.648 and can also be seen in table 7.14 below. In addition, each of the item loading was statistically significant using bootstrap t-values (5000 sub-samples).

Table7.14: Assessment of Construct Reliability and Convergent Validity of Variables

Variable	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Avoidance Behaviour	0.845	0.906	0.763
Intention on Continuous Usage	0.891	0.917	0.648
Perceived Effectiveness	0.862	0.896	0.634
Perceived Security Threat	0.898	0.921	0.662
Self-Efficacy	0.897	0.919	0.656
Severity Threat	0.757	0.841	0.641
Susceptibility Threat	0.886	0.915	0.685

7.4.4 Assessing for Discriminant Validity

The measure of discriminant validity tells the researcher how unique each construct is. Traditionally, to be able to measure for discriminant validity, many scholars have recommended the use of the Cross Loading and the Fornell-Lacker criterion (Hair et al., 2014; Henseler et al., 2009), and have become the dominant approaches in assessing for discriminant validity. With regards to the Fornell-Lacker criterion, when the square root of the minimum AVE is found to be greater than the highest inter-construct correlation, then discriminant validity does exist (Fornell & Lacker, 1981). They also recommend that the cross-loading values of the items should be determined to ascertain whether there are no significant cross loadings to adequately conclude the existence of discriminant validity.

7.4.4.1 Discriminant Validity (Fornell–Lacker Criterion)

First, we consider the discriminant validity using the Fornell–Lacker criterion. As has been established earlier, this method requires that a construct shares more variance within its indicator items, as compared to other constructs, and establishes positive outcomes. As can be seen from Table 7.15, discriminant validity using this criterion was established as the squared values of the AVEs of all seven constructs as highlighted diagonally are greater than correlations within the row and the column (Fornell & Lacker, 1981; Barclay, Thompson, & Higgins, 1995). This result suggest that each construct is distinctively different from the other measurement constructs in the model.

Table 7.15: Discriminant Validity (Fornell-Lacker Criterion)

Code	Variable	AVB	IntentCU	PerEff	PerST	SelfE	SevT	SupT
AVB	Avoidance Behaviour	0.874						
IntentCU	Intention on Continuous Usage	-0.419	0.805					
PerEff	Perceived Effectiveness	-0.186	0.300	0.796				
PerST	Perceived Security Threat	0.485	-0.243	-0.230	0.814			
SelfE	Self-Efficacy	-0.228	0.434	0.575	-0.310	0.810		
SevT	Severity Threat	0.111	0.068	-0.055	0.337	-0.150	0.801	
SupT	Susceptibility Threat	0.405	-0.206	-0.205	0.471	-0.277	0.325	0.827

7.4.4.2 Discriminant Validity using the Item Cross Loadings Criterion

The second method is the Items Cross Loadings Criterion after items which were not required were deleted. As can be seen from table 7.16, all the items as per each construct had loadings higher than 0.708 (Chin, 1998), and also these items did not have any significant cross loadings which indicates that all seven constructs demonstrate discriminant validity.

Table 7.16: Loading and Cross Loading of Constructs to Assess Discriminant Validity

Variable	Code	AVB	IntentCU	PerEff	PerST	SelfE	SevT	SupT

	AVB1	0.851	-0.366	-0.157	0.397	-0.217	0.071	0.346
Avoidance Behaviour	AVB2	0.912	-0.374	-0.175	0.450	-0.210	0.112	0.402
	AVB5	0.857	-0.360	-0.155	0.422	-0.168	0.108	0.310
	IntentCU1	-0.359	0.793	0.248	-0.215	0.346	0.029	-0.123
	IntentCU2	-0.345	0.830	0.236	-0.194	0.351	0.081	-0.157
Intention on Continuous	IntentCU3	-0.364	0.832	0.275	-0.206	0.360	0.082	-0.135
Usage	IntentCU4	-0.343	0.768	0.194	-0.201	0.329	0.047	-0.176
	IntentCU5	-0.305	0.808	0.237	-0.160	0.349	0.044	-0.200
	IntentCU6	-0.296	0.796	0.259	-0.192	0.362	0.044	-0.216
	PerEff1	-0.156	0.188	0.824	-0.183	0.453	-0.046	-0.160
	PerEff2	-0.205	0.252	0.878	-0.209	0.481	-0.058	-0.198
Perceived Effectiveness	PerEff3	-0.052	0.199	0.735	-0.149	0.445	-0.053	-0.118
	PerEff4	-0.139	0.261	0.763	-0.196	0.435	-0.018	-0.167
	PerEff5	-0.104	0.312	0.773	-0.157	0.517	-0.046	-0.142
	PerST1	0.366	-0.142	-0.141	0.744	-0.184	0.284	0.407
	PerST2	0.310	-0.076	-0.202	0.777	-0.191	0.328	0.374
Perceived Security	PerST3	0.317	-0.154	-0.219	0.818	-0.237	0.254	0.342
Threat	PerST4	0.409	-0.218	-0.155	0.836	-0.244	0.308	0.368
	PerST5	0.432	-0.249	-0.184	0.830	-0.297	0.210	0.332
	PerST6	0.484	-0.288	-0.227	0.870	-0.324	0.283	0.464
	SelfE1	-0.177	0.365	0.414	-0.281	0.806	-0.140	-0.235
	SelfE2	-0.207	0.331	0.361	-0.247	0.797	-0.152	-0.191
Self-Efficacy	SelfE3	-0.243	0.364	0.499	-0.298	0.829	-0.116	-0.257
	SelfE4	-0.161	0.345	0.522	-0.218	0.832	-0.091	-0.225
	SelfE5	-0.156	0.378	0.521	-0.209	0.845	-0.096	-0.226

	SelfE6	-0.099	0.323	0.539	-0.222	0.746	-0.136	-0.206
	SevT1	0.086	0.064	-0.043	0.253	-0.120	0.807	0.250
Severity Threat	SevT4	0.018	0.123	-0.029	0.274	-0.064	0.683	0.183
	SevT5	0.112	0.042	-0.051	0.311	-0.142	0.898	0.308
	SupT1	0.243	-0.151	-0.164	0.344	-0.181	0.247	0.758
	SupT2	0.245	-0.091	-0.103	0.312	-0.123	0.222	0.770
Susceptibility Threat	SupT3	0.328	-0.178	-0.209	0.389	-0.280	0.262	0.840
	SupT4	0.401	-0.213	-0.173	0.418	-0.242	0.281	0.893
	SupT5	0.402	-0.189	-0.187	0.455	-0.281	0.318	0.868

7.4.4.3 Heterotrait-Monotrait Ratio (HTMT)

In recent times, other studies have revealed that using the Cross Loading and Fornell and Lacker criterion variance alone as a basis for structural equation modelling will not be adequately conclusive on the existence of discriminant validity (Henseler et al., 2015). Performing the heterotrait-monotrait ratio (HTMT) of correlations as an addon is the best. Henseler et al. (2015), contend that the Fornell-Lacker and the HTMT criterion explained 20.82 percent, and 97 to 99 percent of discriminant validity respectively whereas the cross-loading indicators explained zero percent of discriminant validity in their examination. And that provided three main HTMT criteria: An HTMT specificity ratio of 0.9, an HTMT specificity ratio of 0.85 and an HTMT inference score that ranges between -1 and 1 (-1 < HTMT < 1) as a measure of distinctiveness (Henseler et al., 2015). They explained further that what causes the difference between the HTMT criteria is within their specificity. Among the three-criterion provided, the most conservative criterion is the HTMT.85 since it has the least specific rate among the three and can indicate problems of discriminant validity in a research simulation that has HTMT value of 0.90 with HTMT inference

indicating the establishment of discriminant validity (Henseler et al., 2015). This study therefore adopted the Fornell and Lacker Criterion in addition to HTMT 0.85 to assess the discriminant validity.

Heterotrait–Monotrait Ratio (HTMT) was performed in this study to examine the correlations between the factors or constructs using a specificity criterion rate of 0.85 (HTMT0.85). The HTMT results presented in table 7.17 shows that none of the correlations exceeded 0.85, as a result discriminant validity has been established.

Table 7.17: Discriminant Validity (Heterotrait–Monotrait – HTMT)

Code	Variable	AVB	IntentCU	PerEff	PerST	SelfE	SevT	SupT
AVB	Avoidance Behaviour							
IntentCU	Intention on Continuous Usage	0.480						
PerEff	Perceived Effectiveness	0.192	0.345					
PerST	Perceived Security Threat	0.544	0.257	0.254				
SelfE	Self-Efficacy	0.246	0.485	0.674	0.330			
SevT	Severity Threat	0.117	0.115	0.068	0.417	0.159		
SupT	Susceptibility Threat	0.450	0.227	0.222	0.516	0.299	0.364	

7.5 Structural Model Analysis

Having confirmed the psychometric properties of the reflective measures, the next stage is to examine the structural model in order to assess the model's explanatory power and the significance of the hypothesized paths (Ledden et al., 2011; Lings & Greenly, 2010), using the Smart PLS-SEM. This analysis involves assessment of collinearity, significance and relevance of relationship in structural model (path coefficient), assessing the level of R^2 (coefficient of determination), level of f^2 (effect size), and assesses predictive relevance of Q^2 (Hair et al., 2014). After these analyses,

the study proceeded to examine for the moderation effect. The analysis is conducted based on the constructs used for the study.

7.5.1 Check for Multicollinearity

Hair et al. (2014) proposed five steps for assessing structural model before conclusions can be made:

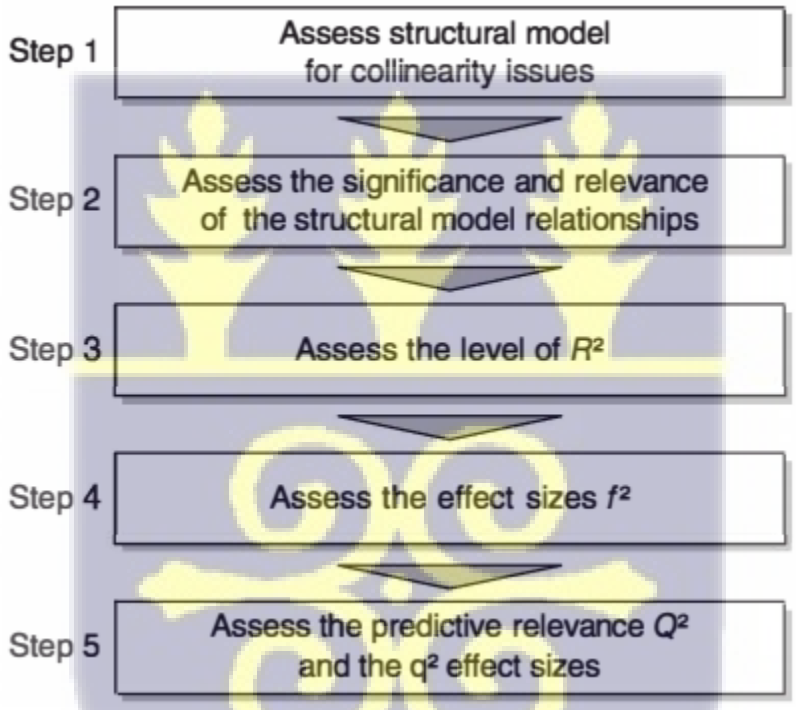


Figure 7.2: Steps in Assessing Structural Model

Source: Hair et al. (2014).

7.5.2 Assessment of Structural Model for Collinearity Issues

The structural model evaluation requires examining the collinearity test to evade a poor result. Construct tolerance and Variance Inflation Factor (VIF) are the indicating values in defining the extent of collinearity issue. Traditionally, a VIF not greater than 3.3 (Diamantopoulos et al., 2006) or 5 (Hair et al., 2011) is regarded ideal for reflective constructs and VIF value not greater than 5 is for formative constructs. Consistent with this point

(Diamantopoulos et al., 2006; Hair et al., 2011), collinearity issue is examined, and the result is presented in Table 6.20, and there is no collinearity issue occurring in the model.

Before assessing the structural model, it is important to ensure that no collinearity issues exist. Collinearity problem is non-existent if the variance inflation factor of the inner model is less than 5 (Sarstedt et al., 2017). The results of collinearity test presented in Table 7.18 showed that all VIF values were less than five (5) showing absence of collinearity problems in the model (Sarstedt et al., 2017)

7.5.2.1 Multicollinearity

Another essential assumption that should be achieved in multivariate analysis is the absence of multicollinearity. This issue must be addressed as it has the potential to diminish any individual independent variables' predictive power by the extent to which it is associated with other independent variables. In order to resolve the multicollinearity issue in this study, both the Inner and Outer Variance Inflation Factor (VIF) values were assessed. The rule of thumb emphasizes that multicollinearity is not a serious problem when the VIF values are below two (>2). A VIF value between greater than one but less than five, the predictors are considered to be moderately correlated (Hair et al., 2011). This however does not pose a challenge except VIF values are beyond five (5<). As can be seen from Table 7.19, an Inner VIF less than two (>2) and Outer VIF values of less than four (>4) shows moderate correlation between predictors shows no multicollinearity issues (Hair et al., 2011). Table 7.18 depicts the results of multicollinearity test of Avoidance Behaviour as the dependent variable with Perceived Effectiveness, Perceived Security Threat, Self-Efficacy, Susceptibility, and Severity, and shows no multicollinearity issues.

Table 7.18: Multicollinearity Check

Variable	Code	Inner VIF	Outer VIF
Avoidance Behaviour	AVB1	1.000	1.890
	AVB2		2.527
	AVB5		2.007
Intention on Continuous Usage	IntentCU1	1.510	2.435
	IntentCU2		2.642
	IntentCU3		2.404
	IntentCU4		1.952
	IntentCU5		3.126
	IntentCU6		3.100
Perceived Effectiveness	PerEff1		1.991
	PerEff2		2.443
	PerEff3		1.961
	PerEff4		1.894
	PerEff5		2.023
Perceived Security Threat	PerST1	1.413	1.920
	PerST2		2.561
	PerST3		2.665
	PerST4		2.758
	PerST5		2.738
	PerST6		2.622
Self-Efficacy	SelfE1	1.597	2.758

	SelfE2		2.609
	SelfE3		2.323
	SelfE4		3.087
	SelfE5		3.021
	SelfE6		2.034
	SevT1		1.361
Severity Threat	SevT4	1.182	1.672
	SevT5		1.724
	SupT1		2.026
	SupT2		2.156
Susceptibility Threat	SupT3	1.372	2.226
	SupT4		3.069
	SupT5		2.717

7.6 Structural Model

This study examines the relationship (if any) existing between the constructs Susceptibility Threat, Severity Threat, Perceived Security Threat, Self-Efficacy, Perceived Effectiveness towards Avoidance Behaviour and then Avoidance Behaviour towards Intention to Continuously Use. Figure 7.3 presents the results of the structural model for this study showing regression weights and factor loadings.

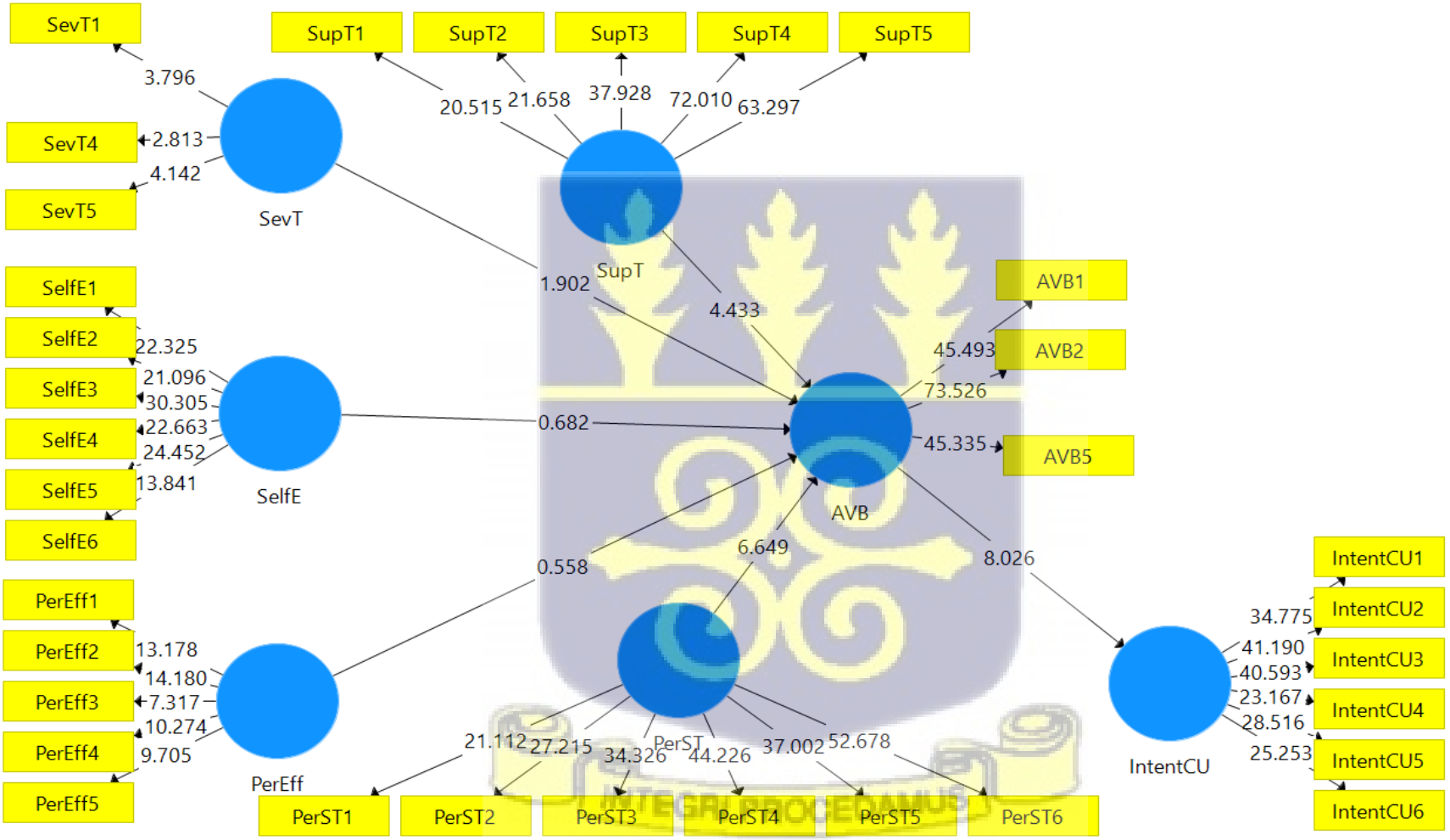


Figure 7.3: PLS-SEM Structural Model

7.6.1 Path Coefficients Assessment and Hypotheses Testing

By determining the path coefficient of the constructs, the study seek to determine how significant the hypothesized relationships between the constructs in the model are. In this study as has been already mentioned, there are six direct relationship hypotheses proposed between the constructs. The study examined both the direct and indirect relationship between the constructs. In the direct relationship, the five main constructs i.e., Susceptibility, Perceived Effectiveness, Severity, Self-Efficacy and Perceived Security Threat, were examined against Avoidance Behaviour. In examining the indirect relationship, the five main constructs mentioned were examined against the construct Intention to Continuously Use. The path coefficients of the structural model were assessed by examining the regression weights of the inner model and significance of hypothesized paths using bootstrap t-values (5000 sub-samples) (Efron & Gong, 1983; Tortosa et al., 2009). This procedure is useful for finding answers to the study hypotheses. Summary of the direct relationship hypotheses are presented below.

H1: Susceptibility Threat will have a direct effect on Avoidance Behaviour

H2: Severity Threat will have a direct effect on Avoidance Behaviour

H3: Self – Efficacy will have a direct effect on Avoidance Behaviour

H4: Perceived Effectiveness will have a direct effect on Avoidance Behaviour

H5: Perceived Security Threat will have a direct effect on Avoidance Behaviour

H9: Avoidance Behaviour will have a direct effect on Intention to Continuously Use the Service

In conjunction, a bootstrapping command is carried out using SmartPLS 3.2 software in order to assess the path coefficient in line with the proposed hypotheses, and the results of path coefficient, t-statistics and p-value are presented in Table 7.19. As can be seen from the table, three of the

hypothesized relationships were supported at a significant p-value ($p<0.05$) at 95% confidence interval i.e., H1, H5 and H9, and one of the hypotheses was supported at a significant p-value ($p<0.1$) at 90% confidence interval i.e., H2 whiles the remaining two were not supported i.e., H3 and H4.

Table 7.19: Assessing Path Coefficient - Direct

Hypotheses	Path	Coefficient	T Statistics	P Values	Results
H1	SupT -> AVB	0.240	4.433	0.000	Significant
H2	SevT -> AVB	-0.105	1.902	0.057*	Significant
H3	SelfE -> AVB	-0.039	0.682	0.495	Not Significant
H4	PerEff -> AVB	-0.031	0.558	0.577	Not Significant
H5	PerST -> AVB	0.388	6.649	0.000	Significant
H9	AVB -> IntentCU	-0.419	8.026	0.000	Significant

*p<0.1

According to Hair et al. (2014), when the t-value or t statistic is less than a recommended threshold of 1.65 ($\alpha = 0.10$), 1.96 ($\alpha = 0.05$), and 2.57 ($\alpha = 0.01$), the effect size is considered not significant, thus, the effect size is not significantly predictive of the relationship. From the above table 7.19, the direct effect of the path coefficient shows that, out of the six hypotheses, two were not significant i.e., H3, and H4. Thus, in the context of the study, Self-Efficacy and Perceived Effectiveness does not predict Avoidance Behaviour. On the other hand, four other hypotheses were also found to be significant i.e., H1, H2, H5, and H9. Thus, in the context of the study, Susceptibility Threat, Severity Threat, and Perceived Security Threat predict respondents Avoidance Behaviour. Also, the construct Avoidance Behaviour significantly predict Intention to Continuously Use.

When path coefficients were assessed for indirect relationships, the paths Perceived Security Threat (PerST), Severity Threat (SevT), and Susceptibility Threat (SupT) were found to significantly predict Intention to Continuously Use (IntentCU), whereas the paths Perceived Effectiveness (PerEff) and Self-Efficacy (SelfE) did not significantly predict Intention to Continuously Use (IntentCU). This is presented in Table 7.20 below.

Table 7.20: Assessing Path Coefficient – Indirect

Path	Coefficient	T Statistics	P Values	Results
PerEff -> IntentCU	0.013	0.546	0.585	Not Significant
PerST -> IntentCU	-0.163	5.552	0.000	Significant
SelfE -> IntentCU	0.016	0.651	0.515	Not Significant
SevT -> IntentCU	0.044	1.819	0.069*	Significant
SupT -> IntentCU	-0.100	3.834	0.000	Significant

*p<0.1

7.6.2 Assessing R-Square Level and Q-Square Predictive Relevance

R-Square, which is the coefficient of determination, is a very important measure used in structural model evaluation. The R-square value tells the amount of variance that exist in the endogenous variable being explained by the exogenous variables used in the model. This measure tells how accurate the model is able to predict a relationship, and such values usually falls between 0 to 1, with one (1) depicting a perfect model. To assess the predictive relevance of the Q-Square, the Stone - Geisser's (Q^2) cross-validated redundancy approach has been widely used. This approach is a blinding folding method in partial least squares (PLS) that sets omission distance criterion of 7 for predictive relevance (Sarstedt et al., 2017; Chin, 2010). By using the Q^2 approach, researchers

are able to tell the predictive relevance of the model they used for the study (Sarstedt et al., 2017; Chin, 2010). If a Q^2 value is greater than zero (0), it shows predictive relevance.

The results of the model's predictive accuracy (R^2) are presented in Table 7.21 which shows only two of the constructs used for the study, thus, Avoidance Behaviour and Intention on Continuous Usage. The constructs, Severity Threat, Perceived Security Threat, Susceptibility Threat, Perceived Effectiveness, and Self Efficacy jointly accounts for 28.8% of the variance in Avoidance Behaviour, whiles Avoidance Behaviour accounts for 17.6% of variance in Intention to Continuously Use. From the table 7.21, it can also be seen that constructs Avoidance Behaviour and Intention to Continuously Use have Q^2 values of 0.213 and 0.110, which are all greater than zero shows predictive relevance.

Table 7.21: Coefficient of Determination, R^2 and Predictive Relevance Q^2

Code	Variables	R Square	Q Square
AVB	Avoidance Behaviour	0.288	0.213
IntentCU	Intention on Continuous Usage	0.176	0.110

7.6.3 Assessing Effect Size f^2

In order to determine the weight or magnitude of the effect sizes (f^2) on the R^2 value of the endogenous constructs, as it is with the traditional multiple regression, when effect size (f^2) value falls in the ranges of 0.02, 0.15 and 0.35, they are considered as depicting small, medium and large effects respectively (Sarstedt et al., 2017; Chin, 2010; Cohen, 1988). An effect size that is considered small means that the exogenous variable has very little or small influence on the endogenous variable, and hence, the exogenous variable may not be a good predictor of the endogenous variables or that it may be a weak predictor. On the other hand, effect sizes that are considered medium to large, depicts a moderate or medium to large or substantial effect of the

exogenous variable on the endogenous variable. Small effect size implies that the influence of the exogenous variable on the endogenous is minimal, as a result the exogenous variable might be a weak predictor of the endogenous variable. Medium and large effect sizes however are explained to mean that, the exogenous variables have moderate to substantial effects on the endogenous (Cohen, 1988).

After examining the effect sizes of the individual constructs, the following effect sizes were obtained. From the six constructs used for the study, two had no effect sizes i.e., Perceived Effectiveness (f^2=0.001), and Self-Efficacy (f^2=0.001); two obtained small effect sizes, which were, Susceptibility Threat (f^2=0.059), and Severity Threat (f^2=0.013) on Avoidance Behaviour. One construct had medium effect size, i.e., Perceived Security Threat (f^2=0.150) on Avoidance Behaviour, and one construct had high effect size i.e., Avoidance Behaviour (f^2=0.213) on Intention to Continuously Use. The models effect size results are presented in the table 7.22 below.

Table 7.22: Assessing Effect Sizes, f^2

Code	Variable	Avoidance Behaviour	Intention on Continuous Usage
SupT	Susceptibility Threat	0.059	
PerEff	Perceived Effectiveness	0.001	
PerST	Perceived Security Threat	0.150	
SelfE	Self-Efficacy	0.001	
SevT	Severity Threat	0.013	
AVB	Avoidance Behaviour		0.213

7.6.4 Assessing for Importance–Performance

The use of Importance-Performance tool is critical for decision making by managers and stakeholders after examining the importance of each variable in determining a possible outcome. This is important, as decision makers will know which variable to focus more resources on. According to Hair et al., (2014), before performing Importance-Performance Analysis (IPMA), it is important that certain requirements are met. First, it is necessary that all indicators must have the same direction; a low value represents a bad outcome and a high value a good outcome. If this requirement is not met, the scale cannot be interpreted in a way that allows the latent variables' higher mean values (i.e., toward 100) to represent a better performance. If this is not the case, the direction needs to be changed by reversing the scale (e.g., on a 1- to 5-point scale, 5 becomes 1 and 1 becomes 5, 2 becomes 4 and 4 becomes 2, and 3 remains unchanged) (Hair et al., 2014, p.210).

Secondly, it is also required that the outer weights (formative measurement model) or outer loadings (reflective measurement model) used have positive expected and estimated values. Without meeting such condition in terms of a measurement model of a certain latent variable, the extracted performance value could possibly fall outside the scale of 0 to 100 and could fall, for example, between -5 to 95 (Hair et al., 2014, p.210). Both requirements were met so examining for Importance–Performance was acceptable. In this study, both direct and indirect Importance-Performance analysis was done.

After performing the direct Importance-Performance analysis, it was observed that the variable Avoidance Behaviour (AVB) has a negative importance value and the lowest performance value as compared to the remaining constructs. Perceived Security Threat (PerST) is the next on the importance index as it has a negative importance although higher than Avoidance Behaviour

(AVB) but also has a little above 50 performance which is also higher as compared to Susceptibility Threat (SupT). Susceptibility Threat (SupT) on the other hand has a negative importance as well although higher than that of Perceived Effectiveness (PerEff) and Avoidance Behaviour (AVB). However, it has a slightly lower performance as compared to Perceived Security Threat. Both Perceived Effectiveness (PerEff) and Self-Efficacy (SelfE) have the same levels of Importance and Performance, which in both cases are higher than that of Susceptibility Threat, Perceived Effectiveness and Avoidance Behaviour. Severity Threat (SevT) has the highest Importance as well as Performance compared to all the other constructs. These are depicted in Table 7.23 and Table 7.24 and Figure 7.4

Table 7.23: Importance–Performance Map Analysis - Direct

		Standardized	*Unstandardized*
Code	**Variable**	**Intention on Continuous Usage**	**Intention on Continuous Usage**
AVB	Avoidance Behaviour	-0.419	-0.321
PerEff	Perceived Effectiveness	-0.031	-0.038
PerST	Perceived Security Threat	0.388	0.428
SelfE	Self-Efficacy	-0.039	-0.044
SevT	Severity Threat	-0.105	-0.127
SupT	Susceptibility Threat	0.240	0.246

Table 7.24: Importance–Performance Map Analysis - Indirect

	Standardized	*Unstandardized*

Code	Variable	Intention on Continuous Usage	Intention on Continuous Usage
PerEff	Perceived Effectiveness	0.013	0.012
PerST	Perceived Security Threat	-0.163	-0.137
SelfE	Self-Efficacy	0.016	0.014
SevT	Severity Threat	0.044	0.041
SupT	Susceptibility Threat	-0.100	-0.079

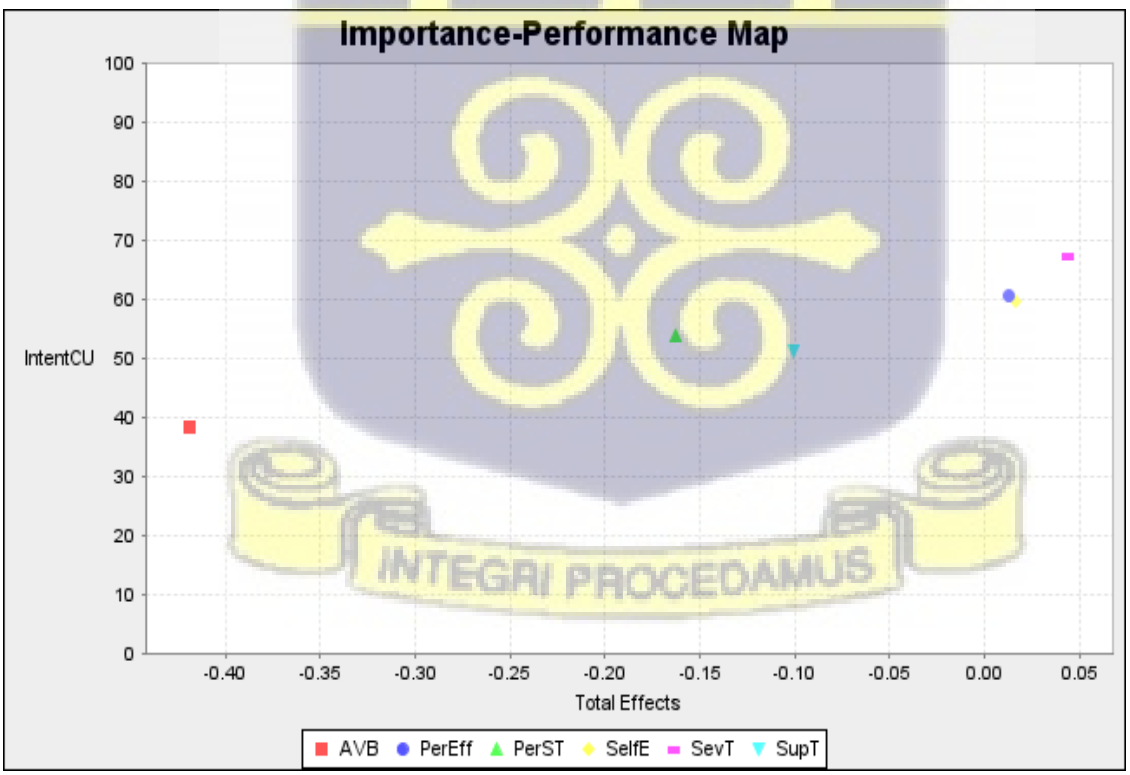


Figure 7.4 Importance-Performance Map

7.7 Assessing the Moderating Effect of Generation X, Y and Z

In this section, the role of the moderating variables is analyzed and presented. The moderator variable used for the study is the generational cohort which had three categorizations, Generation X, Y and Z. We therefore access the moderating role of these groups on the direct relationship between the independent variable or constructs Susceptibility Threat, Severity Threat, Self-Efficacy, Perceived Effectiveness and Perceived Security Threat, on the Avoidance Behaviour of respondents. The corresponding hypotheses are presented as follows:

H6a: Generation X will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour

H6b: Generation X will moderate the direct relationship between Severity Threat and Avoidance Behaviour

H6c: Generation X will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour

H6d: Generation X will moderate the direct relationship between Perceived Effectiveness and Avoidance Behaviour

H6e: Generation X will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior

H7a: Generation Y will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour

H7b: Generation Y will moderate the direct relationship between Severity Threat and Avoidance Behaviour

H7c: Generation Y will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour

H7d: Generation Y will mediate the direct relationship between Perceived Effectiveness and Avoidance Behaviour

H7e: Generation Y will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior

H8a: Generation Z will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour

H8b: Generation Z will moderate the direct relationship between Severity Threat and Avoidance Behaviour

H8c: Generation Z will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour

H8d: Generation Z will moderate the direct relationship between Perceived Effectiveness and Avoidance Behaviour

H8e: Generation Z will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior

The moderation effects of Generation X, Y and Z on the direct relationship between Threat Appraisal (Susceptibility Threat and Severity Threat) and Coping Appraisal (Perceived Security Threat, Perceived Effectiveness, and Self Efficacy), on Avoidance Behaviour was done by using the partial least squares multi group analysis (PLS-MGA) (Sarstedt et al., 2011). Analysing for the moderating effect of the various generational groups was to ascertain whether the generational group a respondent belonged to, played a significant role in determining their threat appraisal and coping appraisal on their avoidance behaviour. Thus, to be able to test for possible variances that

may exist between using similar models to measure for different groups of respondents to examine whether statistically, there would be significant differences between the individual group models (Owusu, 2017; Hair et al., 2014).

Hair et al., (2014, p.276), explains that PLS-MGA is a combination of different techniques or methods developed to help in comparing PLS-SEM estimation for different groups, usually two or above. Tentatively, it refers to "a set of different techniques that have been developed for comparing PLS-SEM estimates across two or more groups of data". It is a general requirement for researchers to perform the normal algorithm for PLS in order to reveal the path coefficients of the model then proceed to perform the PLS-MGA, a procedure that requires performing bootstrapping procedure with the selected groups to obtain the group-specific path coefficients, standard errors and sample sizes (Hair et al., 2014). From the descriptive statistics of the study's respondents, Generation X, Y and Z is a categorical variable with three data groupings (46–60 years for Generation X, 31–45 years for Generation Y, and 30 years–Below for Generation Z). According to Hair et al., (2014), categorical variables work as a group where the data collected for the study is divided into subsamples during MGA which helps researchers to ascertain the significant differences between the groups through comparison. This method also requires that the categorical variable for the moderator has more than 10 records for each of the groups in order to make it possible to run the algorithm. From the descriptive information for the various generational groups, Generation X has 98 records, Generation Y has 119 records, and Generation Z has 167 records, therefore all groups meeting the minimum requirement of at least 10 records, and so PLS-MGA can be performed comparing the three groups.

The Path coefficients and the p-values for the three groups after PLS-MGA had been performed is presented for both direct and indirect effects are presented in Tables 7.26 and 7.27 respectively

below. For the MGA direct relationship, it can be observed that none of the groups tested had p-values that falls within the required significant limit or value of $p<0.05$. This shows that the moderator variable of Generation did not substantially affect the relationship between the Threat Appraisal (Susceptibility Threat and Severity Threat) and Coping Appraisal (Perceived Security Threat, Self-Efficacy and Perceived Effectiveness) on Avoidance Behaviour, as is depicted in Table 7.25 below.

Table 7.25: Multi-Group Analysis (MGA) - Direct

Relationship	Path Coefficients-diff (Generation X and Y)	P-Value	Path Coefficients-diff (Generation X and Z)	P-Value	Path Coefficients-diff (Generation Y and Z)	P-Value
AVB -> IntentCU	-0.072	**0.592**	-0.149	**0.226**	-0.077	**0.527**
PerEff -> AVB	0.077	**0.669**	0.212	**0.230**	0.135	**0.302**
PerST -> AVB	-0.220	**0.143**	-0.133	**0.384**	0.087	**0.436**
SelfE -> AVB	-0.049	**0.749**	-0.033	**0.801**	0.017	**0.871**
SevT -> AVB	-0.048	**0.820**	0.017	**0.891**	0.065	**0.709**

SupT -> AVB	0.130	**0.374**	0.124	**0.383**	-0.006	**0.953**

For MGA indirect relationship, it can be observed again that none of the groups tested also had p-values that fell within the required significant value of $p<0.05$. This also means that, in an indirect approach, the moderator variable divided into subsamples of generation x, y and z, did not have any substantial effect on the relationship between the Threat Appraisal (Susceptibility Threat and Severity Threat) and Coping Appraisal (Perceived Security Threat, Self-Efficacy and Perceived Effectiveness) on Avoidance Behaviour, as is depicted in Table 7.26 below.

Table 7.26: Multi-Group Analysis (MGA) -Indirect

Relationship	**Path Coefficients-diff (Generation X and Y)**	**P-Value**	**Path Coefficients-diff (Generation X and Z)**	**P-Value**	**Path Coefficients-diff (Generation Y and Z)**	**P-Value**
PerEff -> IntentCU	-0.039	**0.658**	-0.088	**0.294**	-0.049	**0.402**
PerST -> IntentCU	0.078	**0.346**	0.010	**0.891**	-0.068	**0.331**
SelfE -> IntentCU	0.027	**0.765**	0.023	**0.788**	-0.004	**0.901**
SevT -> IntentCU	0.024	**0.805**	0.000	**0.951**	-0.024	**0.715**

SupT -> IntentCU	-0.082	**0.340**	-0.096	**0.216**	-0.014	**0.813**

Thus, in effect, hypotheses H6a, H6b, H6c, H6d, H6e, H7a, H7b, H7c, H7d, H7e, H8a, H8b, H8c, H8d, and H8e were all not supported. The results of all the hypotheses are presented in the table 7.27 below.

Table 7.27 Overall Results of Hypotheses

Statement of Hypothesis	Decision
H1: Susceptibility Threat will have a direct effect on Avoidance Behaviour	Supported
H2: Severity Threat will have a direct effect on Avoidance Behaviour	Supported
H3: Self – Efficacy will have a direct effect on Avoidance Behaviour	Not Supported
H4: Perceived Effectiveness will have a direct effect on Avoidance Behaviour	Not Supported
H5: Perceived Security Threat will have a direct effect on Avoidance Behaviour	Supported
H6a: Generation X will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour	Not Supported
H6b: Generation X will moderate the direct relationship between Severity Threat and Avoidance Behaviour	Not Supported
H6c: Generation X will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour	Not Supported
H6d: Generation X will moderate the direct relationship between Perceived Effectiveness and Avoidance Behaviour	Not Supported
H6e: Generation X will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior	Not Supported

H7a: Generation Y will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour	Not Supported
H7b: Generation Y will moderate the direct relationship between Severity Threat and Avoidance Behaviour	
H7c: Generation Y will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour	Not Supported
H7d: Generation Y will mediate the direct relationship between Perceived Effectiveness and Avoidance Behaviour	Not Supported
H7e: Generation Y will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior	Not Supported
H8a: Generation Z will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour	Not Supported
H8b: Generation Z will moderate the direct relationship between Severity Threat and Avoidance Behaviour	Not Supported
H8c: Generation Z will moderate the direct relationship between Self – Efficacy and Avoidance Behaviour	Not Supported
H8d: Generation Z will moderate the direct relationship between Perceived Effectiveness and Avoidance Behaviour	Not Supported
H8e: Generation Z will moderate the direct relationship between Perceived Security Threat and Avoidance Behavior	Not Supported
H9: Avoidance Behaviour will have a direct effect on Intention to Continuously Use the Service	Supported

7.7 Chapter summary

This chapter of the study served a presentation on the results and analysis of the study. Presentation included results on respondents' demographic data, partial least squares structural equation modelling analysis of the various constructs used and their results. The chapter also tested the

hypotheses and explains which of them were supported and those rejected. The presentation also covers the moderating role of the various general groups through a partial least squares multi group analysis. The chapter concludes by presenting a table depicting all the hypotheses stated and their correspondent decisions.

CHPATER EIGHT

DISCUSSION OF FINDINGS

8.1 Chapter Overview

This chapter presents the discussion of the study findings. This discussion is centred on the results established after data analysis, and in relation to other studies conducted on the subject matter. The study draws the similarities and differences from other studies and demonstrates the important contributions this study has made to academia, policy makers and practitioners. The chapter concludes by providing the general conclusions of the study, the limitations of the study and recommendations for future research.

8.2 Discussion

The hypotheses of the study were formulated based on the objectives that were set out to be achieved. To begin the discussion on direct effects, it is important to establish that a number of studies have been conducted to ascertain how threatening situations can lead to motivation to avoid the said threatening situation. When an individual discovers a threat, they are naturally motivated to avoid the threat, and this has been established in both information systems and health psychology. For example, among the bedrock of assumptions underlying the Technology Threat Avoidance Theory (TTAT) is that, when individual IT users come across or are threatened by a malicious IT, they surely will be motivated to protect themselves from the threat (Liang & Xue, 2009). This position of the TTAT had long been established by the hedonic principle at the turn of the eighteenth (18th) and the nineteenth (19th) centuries, which stated that "people are basically attracted to pleasure and avoid pain" (Freud, 1915; Higgins, 1997), as well as studies in health psychology research which posits that health problems usually help to perpetuate perceived threats increasing the likelihood of victim partaking in protective health behaviour (Janz & Becker, 1984;

Oliver & Berger, 1979; Rosenstock, 1974). Further, it is important to emphasize that, research has proven that avoidance motivation actually leads to avoidance behaviour (Carpenter et al., 2019). Also, a number of studies (Liang & Xue, 2009; Carpenter et al., 2019) have established that Perceived Susceptibility (Susceptibility Threat), Perceived Severity (Severity Threat), Perceived Effectiveness, and Self–Efficacy, are among the factors that affect avoidance motivation which in turn leads to avoidance behaviour. These served as the motivation for the formulation of hypothesis that the threat of mobile money fraud can lead to avoidance behaviour of users.

1. **Research Question 1. What are the rates of subscription and patronage of the MM service given cognisance to the current fraud situation in Ghana?**

This question was answered based on the demographic characteristics of sampled respondents who participated in the study.

The basic assumption of the TTAT is that when technology users hold a negative perception about a technology, they are most likely going to stop using the technology or in a situation where the technology is almost indispensable, they will develop a coping strategy to mitigate the negative consequences that they would have suffered (Liang & Xue, 2009; Liang & Xue, 2010). In either of such situation, the patronage and use of such a technology will be affected and even potentially diminish. The level of diminish could be ascertained basically by examining the rate of subscription or patronage of the technology, whether the technology is being used, and the frequency with which it is being used (La Chance et al., 2003).

Even before this assessment was done, this study examined respondents on two critical factors that could be important factors in technology adoption and use: First, is the level of education of respondents, and second, whether respondents own any social media account. From the demographic data in table 7.1 above, all respondents have had some level of education, thus 100

percent education level, with 3.4 percent receiving only primary education. The remaining 96.6 percent had received from Junior High School education to PhD levels. This was particularly important as a number of studies have established that technology adoption and use is influenced by a person's level of education (Uematsu & Mishra, 2010; Riddell & Song, 2011). Riddell and Song (2011) for example, after assessing the role of education in technology use and adoption among Canadian workers, found that the probability of a worker using a using computer increased as their level of education increases, and that employees who had higher education had longer working experience in computer use. Hence, with a 96.6 percent of respondents being literate, the use of the MM service was certainly not a problem as they are capable of manoeuvring the platform.

The study further assessed respondents on whether they had enrolled or registered unto the mobile money payment system, 96.4 percent reported YES and the remaining 3.6 percent stating NO; a clear depiction of the wide acceptance of the service. The study further enquired whether respondents actually use the service, with 96.6 percent claiming YES and the remaining 3.4 percent stating NO. The study further assessed respondents on how regular they use the mobile money service by rating their regularity of use on a scale of 1 to 10, where a rating of 1-3 was ranked as LOW, 4 - 6 ranked as MODERATE and 7–10 ranked as HIGH. 6.3 percent of respondents reported LOW frequency, 30.7 percent reported AVERAGE, and the remaining 60 percent reporting HIGH. This shows over 93.7 percent of respondents rated themselves between 4–10 regarding their regularity of use. This depicts a very high level of use of the mobile money service and also serving a proof that the wildly reported issue of fraud is not greatly affecting the rate of subscription

This finding may partially support the TTAT's assumption that when users of a technology cannot avoid the threat related to the technology, they adopt a coping mechanism to it use (Liang & Xue,

2009; Liang & Xue, 2010). However, questions could still be asked on whether users adopting a coping mechanism towards the threat associated with a technology could still lead to such high levels of patronage and regularity of use. Leavell (2019), for example, has established that convenience of use or personal convenience is a critical factor when assessing the adoption of a technology in specific context. Carpenter et al. (2019) also argued that, one of the critical components that determines the use of a technology even in the face of threat is the level of the user's risk appetite. People with higher risk appetite will go for a technology regardless of the risk. Given that this is true, the high level of patronage empirically established by this study makes it conspicuous to assume that all such users have high risk appetite. Other scholars (Stobierski, 2019) have also posited that, regardless of the given situation, when an individual establishes that the potential benefit associated with a decision of using a technology outweighs the cost, they will most likely choose to go ahead and use the technology (Stobierski, 2019). This study therefore argues that, a cost-benefit analysis precedes a user's decision to adopt a coping mechanism against the threat associated with a technology.

Research Question 2. What is the effect of user's threat perception on avoidance behaviour towards the MM service?

To be able to answer the second research question, perception of threat and coping abilities were measured or appraised. After review of literature, threat and coping perceptions were made up of five main constructs: Susceptibility Threat, Severity Threat, Self–Efficacy, Perceived Effectiveness and Perceived Security Threat, based on which hypotheses 1, 2, 3, 4 and 5 were formulated.

Hypothesis **H1** aimed at measuring how respondents perceived themselves to be susceptible to the threat of mobile money fraud and how this susceptibility threat has affected their avoidance

behaviour towards the service. By this hypothesis, the study asserted that an individual's appraisal of how susceptible they are to mobile money fraud will have a direct effect on their desire or willingness to avoid using the mobile money service. After empirically testing this hypothesis, it was established that the direct relationship between respondent's susceptibility threat and avoidance behaviour was positive based on path coefficient **β= 0.240; *p*= 0.000** and was also statistically significant. This finding shows or means that a respondent's perception of how susceptible they are to the threat of mobile money fraud will cause them to avoid using the service. The positive relationship means the more respondents feel susceptible to fraud attacks, the more likely they are to avoid using the service.

Hypothesis **H2** also sought to measure respondent's perception of severity of the threat and how this will affect their avoidance behaviour. By this hypothesis, the study sought to establish that when respondents perceive that the consequences of mobile money fraud on them would be severe, they will avoid using the mobile money service. This postulation was made after review of literature done on the subject of severity of a threatening situation and was empirically tested to establish a direct relationship between threat of severity and avoidance behaviour. The study found that the direct relationship between severity threat and avoidance behaviour was negative based on a path coefficient of **β= -0.105; *p*= 0.057***, was also found to be statistically significant. A negative path coefficient means that there is an inverse relationship between severity threat and avoidance behaviour, and so the more severe the potential threat would be, the less likely that respondents will avoid using the service in the context of this study. This finding was found to be consistent with TTAT theory and a number of studies. Liang and Xue (2009), in the formation of TTAT opined that, there was a positive interaction effect between susceptibility and severity which leads to perceived threat. This postulation was confirmed as perceived threat was found to

significantly determine avoidance motivation (Liang & Xue, 2009). In the year 2010, Liang and Xue (2009) conducted a study that sought to understand security behaviours in personal computer usage from the perspective of the threat avoidance theory. By using a survey approach, a survey instrument was administered online to 166 business students at one of the major universities in the U.S., with 152 students giving their responses. The study found that perceived susceptibility and severity, significantly determined perceive threat (Liang & Xue, 2010). In a study conducted by Carpenter et al. (2019) on refining the TTAT, both Susceptibility threat and Severity threat were found to lead to perceived threat, and perceived threat was found to significantly affect avoidance motivation which leads to avoidance behaviour. By using the TTAT to assess the individuals' internet security perception and behaviours: a polycontextual contrast analysis between China and the US, Chen and Zahedi, also established that susceptibility and severity threat significantly defined perceived threat, and perceived threat significantly determining internet users' perception of threat and avoidance behaviour (Chen & Zahedi, 2016)

In Hypothesis **H3**, the study postulated that a respondent's level of Self–Efficacy will have a direct effect on the Avoidance Behaviour. By this postulation, the study sought to emphasize that a respondent's perception of themselves and their ability to deal with the threat of mobile money fraud will influence their decision of whether to avoid the service or use the service at any given moment. After testing this hypothesis, it was established that there was a negative direct relationship between Self-Efficacy and Avoidance Behaviour, based on the path coefficient of **β= -0.039; *p*= 0.495,** in the context of the study. This negative path coefficient means there was an inverse relationship between Self–Efficacy and Avoidance Behaviour, although this finding was not statistically significant. Which means that the value of the relationship was not big enough to establish and emphatically conclude that the higher the level of Self–Efficacy, the lower the

possibility of Avoidance Behaviour. Nonetheless, this finding means that as respondent becomes more aware and is confident of their ability to deal with the threat of mobile money fraud, they are less likely to avoid using the service, although this relationship was not strong enough to establish an emphatic position. The findings of this study have been supported by other studies in Information Systems (Chen & Zahedi, 2016; Carpenter et al., 2019). Chen and Zahedi (2016), in their study which involved 489 respondents, compared internet security perception and behaviour between Chinese and Americans. The study found that Self–Efficacy had a negative inverse relationship with avoidance motivation for both Chinese and American internet users although the effect sizes were not significant. This finding is also supported by the work of Carpenter et al., (2019). In their study "Refining the Technology Threat Avoidance Theory", Self–Efficacy did not significantly predict avoidance motivation, although they found a positive direct effect relationship. This study used an online survey method, where respondents were the first 650 respondents who completed a questionnaire were offered US$0.50 as an incentive. In all, 644 responses were used after data was cleaned (Carpenter et al., 2019).

Hypothesis **H4** was aimed at measuring the direct effect relationship between Perceived Effectiveness and Avoidance Behaviour. This hypothesis asserted that respondent's perception of how effective available protective measures were against the threat of mobile money fraud will impact their real time decision to either avoid or use the service. After empirically examining this hypothesis, the study found that there was a direct negative relationship between Perceive Effectiveness and Avoidance Behaviour, based on a path coefficient of **β= -0.031; *p*= 0.577**. This means that, a high level of Perceived Effectiveness of protective measures will lead to a low rate of Avoidance Behaviour among users. In other words, when users consider protective measures to be effective in dealing with the threat of possible mobile money fraud, they are less likely to avoid

using the service. On the other hand, when users consider or perceives protective measures to be ineffective, they will avoid using the service. This negative path coefficient was however, found not to be statistically significant, which means that although there is an inverse relationship between Perceived Effectiveness and Avoidance Behaviour, this relationship was not strong enough to make an emphatic direct causative relationship. This finding of the study has found contrary evidence to other studies conducted on the same construct. In the work of Carpentter et al. (2019), safeguard effectiveness, also referred to as perceived effectiveness was found to be significantly associated with avoidance motivation, after surveying a sample of 647 respondents. Liang and Xue (2010) also established in their study that there was a significant positive effect between safeguard effectiveness or perceived effectiveness and avoidance motivation, after assessing examining the individuals' security behaviours when using personal computers. In the original theoretical position of the TTAT, Liang and Xue (2009) offered two main explanations for such findings, thus, in situations where the relationship is positive and when it is negative. For a negative relationship, proponents of TTAT argue that there are situations where perceived effectiveness has a negative relationship with avoidance behaviour. Perceived Safeguard Effectiveness is a demonstration of the level of control an IT user has over possible threat. When a user has strong control over possible threats, it connotes that their safeguard measure has been effective helping to keep the threat under control. According to coping theorist, a person is more likely to perform problem–focused (tackle the problem head-on) when they consider themselves capable and in control of the situation (Beaudry & Pinsonneault, 2005). However, Liang and Xue (2009) opine that, this high-level confidence of an individual suggesting he/she has everything under control leads to complacency. Likewise, a computer user who knows that the safeguarding measure is effective in dealing with possible threat, "will not be so eager to deal with the threat",

regardless that they are fully aware that such a threat is present. Consequently, as the effectiveness of the safeguard increases, users are less motivated to deal with the threat.

Hypothesis **H5** asserted that Perceived Security Threat will have a direct effect on Avoidance Behaviour. This hypothesis sought to measure respondent's perception of security threat and how this perception would affect their decision to avoid using the service. Thus, a user's general perception of threats to their security when they use the mobile money service would have consequential effect on their decision to use or avoid the service. This hypothesis was statistically measured of which it was determined that, indeed Perceived Security Threat has a direct positive relationship with Avoidance Behaviour based on a path coefficient of **β= 0.388; *p*= 0.000.** This means that when mobile money users perceive that the issue of fraud threatens their security on the service or they perceive their financial security in using the service to be under threat, they will avoid using the service. In addition, this positive path coefficient was found to be statistically significant which means that perception of security threat can sufficiently predict avoidance behaviour towards the mobile money service.

In all, the study established that perception of threat indeed affects avoidance behaviour, a fact that supports the TTAT, and has been corroborated by other studies. This finding is supported by the works of Carpenter et al. (2019) as well as Chen and Zahedi (2016). Other studies in neuroscience and psychology (Fernandes et al., 2013) have affirmed the that how an individual perceive threat, determines their behaviour, and that emotional processing of events affects areas in the brain that helps us make decisions and take actions (Oliviera et al., 2012)

Research Question 3. What is the effect of users' avoidance behaviour on their continuous use of the MM service?

To be able to answer this research question, the study assessed respondents Intention to Continuously Use the Service. By this question, the study sought to answer whether users may decide to continue or discontinue their use of the service in the future, as this was a correct parameter in examining the future sustainability and viability of the service in the face of persistent fraud attacks on users. Based on this construct, hypothesis 9 was formulated.

Hypothesis **H9** asserted that Avoidance Behaviour will have a direct effect on Intention to Continuously User the service. After testing this hypothesis, it was established that Avoidance Behaviour will have a direct negative effect on Intention to Continuously Use the Service, based on the path coefficient of **β= -0.419; *p*= 0.000.** This means that the more mobile money users avoid using the service today, the less likely that they would consider coming back and continue using the service in the future. The negative effect was also found to be statistically significant, which also means that Avoidance Behaviour can be used to sufficiently predict mobile money user's intention to continue or discontinue using the service. In summary, when users lose trust in the security of the service and constantly feels threatened by mobile money fraud attacks, they will discontinue using the service. Several studies that have examined the continuous usage construct, have measured the construct on different parameters and with different antecedents, with none of the research reviewed by this study finding avoidance behaviour as an antecedent (Gu et al., 2019; Fang et al., 2019; Wangpipatwong, Chutimaskul, & Papasratorn, 2008). Perhaps, such studies have envisaged that at the point of avoidance, there is not turning back for the user of the technology. This assumption served as part of the motivation for this study. Continuous use or usage have been measured on different technologies, such as continuous use of smart homes, mobile banking technology, e-government website, smartphone application for energy efficiency, among others, albeit with different outcomes. Kubfer et al. (2016), examined whether decision criteria of

technology users change from the point of adoption to the point of continuous usage. Their study assessed the use of smart meters which had an application that gave users information on the consumption rate and efficiency among 549 respondents in the Netherlands. Among other things, their study found only "moderate support" when examined on continuous usage intention and encouraged further studies on the construct just as other studies (Bhattacherjee, 2001; Bhattacherjee & Lin, 2015).

Research Question 4: What is the moderating effect of users' generation in relation to their threat perception and avoidance behaviour towards the MM service?

The study sought to answer the question of how users' threat and coping perception on avoidance behaviour would be affected by the generational cohort they belong to. The term generation used in this study referred to respondents who were born within a specific period defined by years. The generations were grouped under three main cohorts: Generation X, Generation Y and Generation Z. Each generational group was examined against each of the perception constructs as identified: Susceptibility threat, Severity Threat, Self-Efficacy, Perceived Effectiveness and Perceived Security Threat. Hypotheses **H6a, H6b, H6c, H6d, H6e; H7a, H7b, H7c, H7d, H7e;** and **H8a, H8b, H8c, H8d, H8e,** were postulated to ensure such examination. Multi group Analysis (MGA) was done for all hypotheses under each construct.

For the construct Susceptibility Threat, three hypotheses were postulated, H6a, H7a and H8a, which all postulated that Generation X, Y, and Z, will moderate the direct relationship between Susceptibility Threat and Avoidance Behaviour. With path coefficients of (**β= 0.130** between X and Y, **β= 0.124** between X and Z, and **β= -0.006** between Y and Z) and p–values of (**p=0.374**

between X and Y, **p=0.383** between X and Z, and **p= 0.953** between Y and Z). Based on the above path coefficients, there was a direct positive relationship between Generation X and Y, and Generation X and Z, and a direct negative relationship between Generation Y and Z, when between group analysis on Susceptibility Threat and Avoidance Behaviour were performed. The positive relationship between Generation X and Y, and Generation X and Z, shows that these generations behave in similar fashion in terms of Susceptibility Threat and Avoidance Behaviour. The negative relationship between Generation Y and Z, means that these two generation groups will exhibit opposite behaviour when it comes to Susceptibility Threat and Avoidance Behaviour. However, based on the estimated p-values among all the between group analysis, these direct effects, whether positive or negative, were not significant as it did not meet the significant requirement of $p<0.05$, which means that the relationship was not strong enough to establish an emphatic position when it comes to Susceptibility Threat and Avoidance Behaviour.

For the construct Severity Threat, three hypotheses were also postulated, thus, H6b, H7b, and H8b, which stated that Generation X, Y and Z, will moderate the direct relationship between Severity Threat and Avoidance Behaviour. Having path coefficients of (**β= -0.048** between X and Y, **β= 0.017** between X and Z, and **β= 0.065** between Y and Z) and p–values of (**p=0.820** between X and Y, **p=0.891** between X and Z, and **p= 0.709** between Y and Z). Based on the above path coefficients, there was a direct negative relationship between Generation X and Y, a direct positive relationship between Generation X and Z, as well as a direct positive relationship between Generation Y and Z, when between group analysis was performed on Severity Threat and Avoidance Behaviour. The negative relationship between Generation X and Y shows that the behaviour of these two generations is opposite to each other when it comes to Severity Threat and Avoidance Behaviour. On the other hand, the positive relationship between Generation X and Z,

and Generations Y and Z, shows that in both instances, these generations behave in similarly in terms of Severity Threat and Avoidance Behaviour. Also, based on the estimated p-values among all the between group analysis, these direct effects, whether positive or negative, were not significant as it did not meet the significant requirement of $p<0.05$, which means that none of the groups were significantly different from the other when it comes to their perception of severity threat on their avoidance behaviour.

For constructs Self–Efficacy, three hypotheses were formulated, thus, H6c, H7c, and H8c, which asserted that Generation X, Y, and Z will moderate the direct relationship between Self Efficacy and Avoidance Behaviour. Having path coefficients of (**β= -0.049** between X and Y, **β= -0.033** between X and Z, and **β= 0.017** between Y and Z) and p–values of (**p=0.749** between X and Y, **p=0.801** between X and Z, and **p= 0.871** between Y and Z). Given the above path coefficients, there was a direct negative relationship between Generation X and Y, a direct negative relationship between Generation X and Z, as well as a direct positive relationship between Generation Y and Z, when between group analysis was performed on Self–Efficacy and Avoidance Behaviour. The negative relationships between Generation X and Y, and Generation X and Z, shows that in the given scenario, these generations behave in an opposite manner to each other in terms of Self–Efficacy against Avoidance Behaviour. On the other hand, the positive relationship between Generations Y and Z, the behaviour of these two generations is similar in terms of Self–Efficacy and Avoidance Behaviour. With this construct, based on the estimated p-values among all the between group analysis, these direct effects, whether positive or negative, were not significant as it did not meet the significant requirement of $p<0.05$, which means that the relationship between the various generation groups were not strong enough to establish an emphatic position when it comes to Self–Efficacy and Avoidance Behaviour.

For the construct Perceived Effectiveness, three hypotheses were formulated, which were, H6d, H7d, and H8d, which postulated that Generation X, Y, and Z will moderate the direct relationship between Perceived Effectiveness and Avoidance Behaviour. These hypotheses had between group path coefficients and p-values of (**β= 0.077** between X and Y, **β= 0.212** between X and Z, and **β= 0.135** between Y and Z) and p–values of (**p=0.669** between X and Y, **p=0.230** between X and Z, and **p= 0.302** between Y and Z). Given the above path coefficients, there was a direct positive relationship between Generation X and Y, a direct positive relationship between Generation X and Z, and a direct positive relationship between Generation Y and Z, after performing between group analysis on Perceived Effectiveness and Avoidance Behaviour. The positive relationship between Generation X and Y, Generation X and Z, and Generation Y and Z, shows that all generational groups behave almost the same in terms of Perceived Effectiveness and Avoidance Behaviour. With this construct and based on the estimated p-values among all the between group analysis, all the direct positive relationships between the generation groups were not significant as it did not meet the significant requirement of $p<0.05$. This means that the relationship between the various generation groups were not strong enough to establish an emphatic position when it comes to Perceived Effectiveness and Avoidance Behaviour.

And finally, for the construct Perceived Security Threat, three hypotheses were formulated, which were H6e, H7e, and H8e, all of which postulated that Generation X, Y, and Z will moderate the direct relationship between Perceived Security Threat and Avoidance Behaviour. With path coefficients (**β= -0.220** between X and Y, **β= -0.133** between X and Z, and **β= 0.087** between Y and Z) and p–values of (**p= 0.143** between X and Y, **p= 0.384** between X and Z, and **p= 0.436** between Y and Z). Based on the estimated path coefficients, there was a direct negative relationship between Generation X and Y, a direct negative relationship between Generation X

and Z, and a direct positive relationship between Generation Y and Z, after performing between group analysis on Perceived Security Threat and Avoidance Behaviour. The negative relationships between Generation X and Y, and Generation X and Z, shows that in the given scenario, these generations behave in an opposite manner to each other in terms of Perceived Security Threat against Avoidance Behaviour. On the other hand, the positive relationship between Generations Y and Z, the behaviour of these two generations is similar in terms of Perceived Security Threat and Avoidance Behaviour. Based on the estimated p-values for this construct, all the direct positive or negative relationships between the generation groups were not significant as it did not meet the significant requirement of $p<0.05$. This means that the relationship between the various generation groups were not strong enough to establish an emphatic position when it comes to Perceived Security Threat and Avoidance Behaviour.

In all, this study did not find a significant effect of the MM users' generation on the relationship between their threat perception and its consequential avoidance behaviour. It is important to establish that studies on the effect of generations as moderator to threat perception and avoidance behaviour is lacking after review of literature. However, a number of studies have been conducted on the various generations and their general behaviour in relation to technology adoption (Althaus, 2016; Owusu et al., 2017; Debb, Schaffer & Colson, 2020). Debb et al. (2020), conducted a study to examine information security behaviours between Generation Y and Z adults. From their perspective, although young adults in today's world are considered to be more technologically savvy compared to older population, there is lack of literature when it comes to their security awareness. The main objective of the study was therefore to compare these two generation groups when it comes to their practice of online cybersecurity practices. The study found that respondents in the Generation Z bracket, which is the younger population "demonstrated less endorsement of

widely known cybersecurity best practices" (Debb et al., 2020). In another study, Althaus (2016), also sought to analyze possible difference between the internet security perceptions of millennials (Generation Y'ers) and non–millennials (Generation X'ers) and how these perceptions affect their online shopping behaviour. The study found, after analyzing responses from 363 German respondents through an online survey that, the perception of risk among millennials was significantly different when compared to Generation X'ers, and also established that a reduction in the risk perception of the two generations resulted in higher levels of online shopping after identifying strong correlations between reducing risk perception and shopping behaviour (Althaus, 2016). Other studies have also found that when it comes to e commerce adoption, perceived risk; financial risk, privacy risk, safety, among others, were important factors for consideration. In their study, Panjaitan et al. (2019), examined the experiences of generation X'ers when adopting a technology. Their study combined the Technology Acceptance Model (TAM) and Perceived Risk, and through online survey assessed 89 respondents. Respondents, however, expressed optimism to continue shopping when they are assured of reduced risk or safety (Panjaitan et al., 2019). Although studies have security, risk or threats as influencing factors when adopting or using a technology among the various generation groups, no study was found to have accessed these generations as moderators when establishing a direct relationship between two variables. This study is therefore novel as it opens new avenue in Information Systems research.

8.3 Chapter Summary

This chapter of the study presented a discussion of the study's findings. The discussion centred on the current state of mobile money in Ghana, which was discussed using the demographic data from the results. Also, the effect of user's threat perception on their avoidance behaviour, the effect of user's avoidance behaviour on their continuous use of the service, and the moderating effect of

user's generation on the relationship between their threat perception and avoidance behaviour were all discussed in relation to other research works.

CHAPTER NINE

CONCLUSION, RECOMMENDATION AND SUGGESTIONS FOR FUTURE RESEARCH

9.1 Chapter Overview

This chapter of the presents the conclusion, the various recommendations which informed suggestions for future studies. Presentation in this chapter includes a summary of the research problem, the objectives that the study sought to achieve and the research questions. The chapter also presents the final framework of the study based on findings after data was analysed and hypotheses tested.

9.2 Summary of Research Problem, Objectives and Questions

As has been established, studies on mobile payment technology popularly known as mobile money (MM) is definitely not few. Since its inception, the mobile money phenomenon has not been short on research (Narteh et al., 2017) although a lot of these studies are based on the conceptualization MM, its growth and associated benefits. The service, under two decades of its inception has suddenly become a major backbone to economies on the African continent. However, it is important to emphasize that recent issues of fraud attacks have put the service in danger. Review of literature has suggested that, the issue of mobile money fraud is indeed a big problem, and the continent loses millions of dollars annually to both local (country specific) and international (across Africa and the world) fraudsters and cybercriminals (Busuulwa, 2016; Laryea, 2016; CGAP, 2017; Akomea–Frmpong, 2019). Research have established that, the financial sector thrives particularly on trust and confidence. As a result, a consistent rise in mobile money fraud attacks will affect subscriber confidence as the service will be deemed risky. This study therefore sought to examine how the risk perception of mobile money users can potentially affect decision

to use or quit using the service, and the possibility of decision continuing into the future. The study therefore had four key objectives:

The study therefore sought to achieve the following objectives:

1. To perform an empirical examination of subscription and patronage rates of the MM service given cognisance to the current fraud situation in Ghana.
2. To examine the effect of mobile money users' threat perception on their avoidance behaviour towards the service.
3. To examine the effect of users' avoidance behaviour on their on their continuous use of the MM service.
4. To ascertain the moderating effect of users' generation in relation to their threat perception on their avoidance behaviour towards the MM service.

Based on the objectives of the study, following questions served as a guide:

1. What are the rates of subscription and patronage of the MM service given cognisance to the current fraud situation in Ghana?
2. What is the effect of mobile money users' threat perception on their avoidance behaviour towards the service?
3. What is the effect of users' avoidance behaviour on their continuous use of the MM service?
4. What is the moderating effect of users' generation in relation to their threat perception on avoidance behaviour towards the MM service?

9.3 Final Research Framework

The primary purpose of this study was to investigate how users of mobile payment system, commonly referred to as mobile money, are able to avoid the threat of mobile money fraud that has bedevilled the service, and how this avoidance behaviour affects their intention to continuously use the service. By this purpose, this study sought to appraise respondents' threat and coping perceptions, and how these two affects their avoidance behaviour and then goes further to examine how respondent's avoidance behaviour affects their intention to continuously use the service. The Technology Threat Avoidance Theory (TTAT) was used as the main governing theory, and the appraisal of threat and coping perceptions on avoidance behaviour was moderated by the Generational theory. After its inception about a decade ago, the TTAT continues to be tested by researchers as can be seen in a number of studies (Chen & Zahedi, 2016; Liang & Xue, 2010; Carpenter et al., 2019). Studies that have examined TTAT moderated by Generation X, Y and Z, are almost non-existent after review of literature. This served as the main motivation for the study and informed the development of the framework of the research as presented in chapter five of this study. Statistical analysis was performed for the constructs and the moderator variables as presented in the previous chapter. The final research framework is presented in figure 8.1 below:

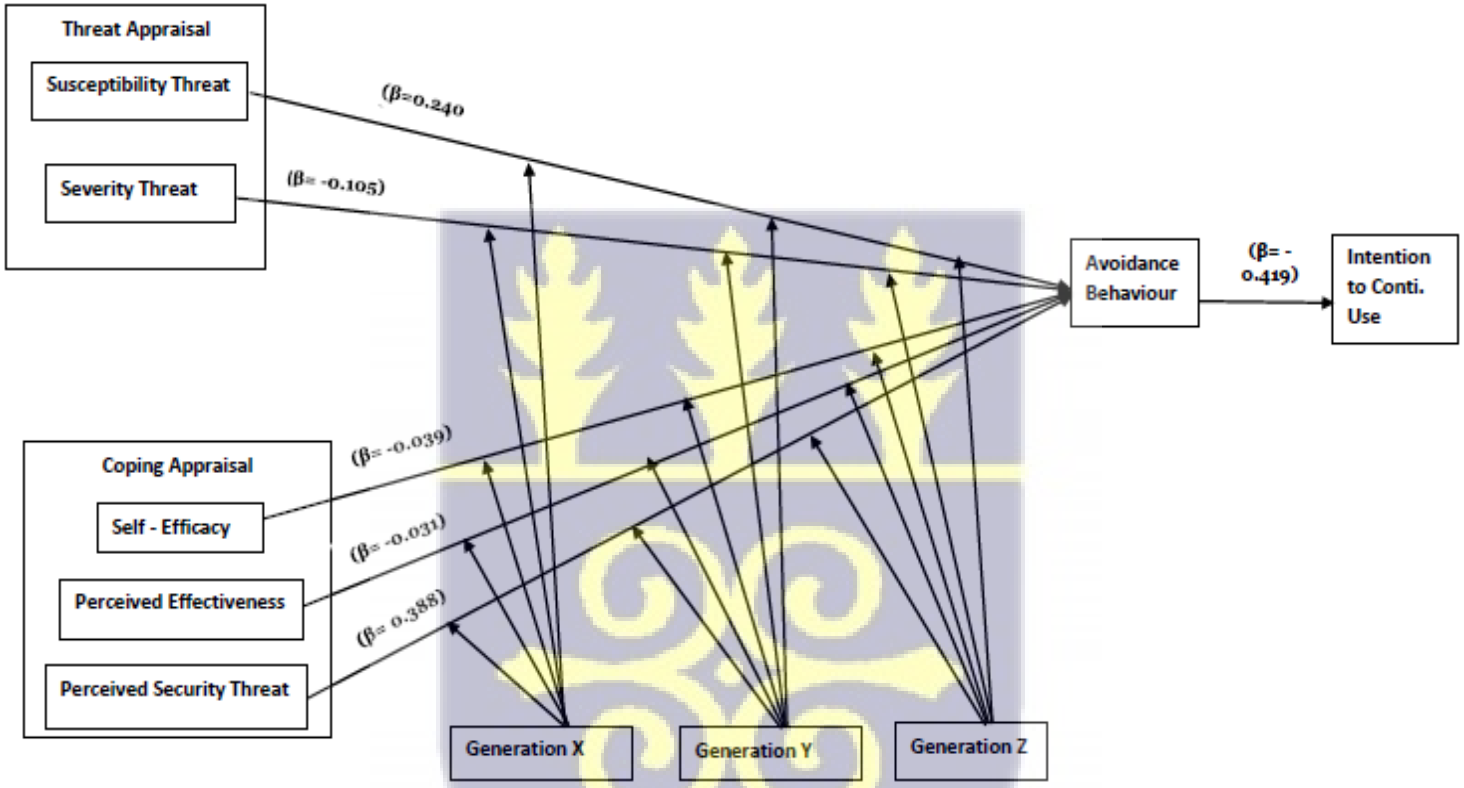


Figure 8.1: Final Research Framework
Source: Author's Construction

Table 9.1 Mapping Matrix of Research Objectives, Theoretical Basis, Findings, and Contributions

Research Gaps	Research Objectives	Empirically Established Findings	Supporting Literature	Contributions
Gaps in literature particularly on the subject of mobile money fraud, as almost all	1. To perform an empirical examination of subscription and patronage rates of the MM service given cognisance to the current fraud situation in Ghana.	96.4% of subscription of the MM service in the face of widely reported issues of fraud, assessed by the percentage of registration. 96.6 % regarding actual use of MM service, ascertained by the respondent's response to actual use of the MM service. 93.7% (moderate to high) regularity of use of the service irrespective of increasing fraud reports, assessed by	Lachance et al. (2003), Leavell (2019), Liang and Xue (2009), Stobierski (2019), Carpernter et al. (2019), Oliviera (2012)	Raises critical question to the TTAT, whether coping strategy alone is enough to still ensure high subscription, use, high regularity of use for a technology that poses significant threat of fraud to it users. Possible reasons might be when the said technology is almost a need to daily life

studies on the subject of mobile money relates to it adoption, ease and convenience of use and worldwide acclaim and growth (Akomea-Frimpong, 2019; GSMA, 2018; GSMA, 2019)		respondents rating of how regular they use the MM service.		
		Respondents' perception of Susceptibility significantly affects their decision to avoid using the service.		High Degree of user susceptibility poses serious danger to user confidence and trust in the service and raises significant risk to the MM service.
	2. To examine the effect of users' threat perception on avoidance behaviour	As Severity threat goes up, Avoidance Behaviour comes down. This was however not significant.	Carpenter et al. (2019), Chen and Zahedi (2016), Fernandes et al. (2013), Oliviera et al. (2012)	Ensuring high level of user Self-Efficacy through constant public education bodes well for the services as it will help reduce or limit possible avoidance behaviour.

Examining the TTAT in relation to mobile money adoption in the face of widely reported fraud incidents (Liang & Xue, 2009; Liang & Xue, 2010; Carpenter et al., 2019)	towards the MM service.	The higher respondents Self Efficacy, the lower the lower avoidance behaviour. High level Perceived Effectiveness of protective measures will lead to a low rate of Avoidance Behaviour. Perceived security threat significantly affected Avoidance Behaviour		Ensuring that information given users on how to deal with possible fraud attacks are correct and effective, will be key to reduce avoidance rate. A general sense of insecurity poses an existential threat to the service. Investment into security infrastructure to significantly reduce fraud attacks remains increasingly paramount.
		The study found that the more mobile money users avoid using the		It is critical for mobile network operators and policy makers to ensure users of the service do not increasingly seek to avoid using the service,

Gaps in theory regarding the translation from avoidance behaviour to either continuance or discontinuance of use of technology (Laing & Xue, 2009; Carpenter et al., 2019)	3. To examine the effect of users' avoidance behaviour on continuous use of the MM service.	service today, the less likely that they would consider continue using the service in the future. The negative effect was also found to be statistically significant, which also means that Avoidance Behaviour can be used to sufficiently predict mobile money user's intention to continue or discontinue using the service.	Gu et al. (2019), Fang et al. (2019), Kubfer et al. (2016)	as there will be no turning back if the service is completely avoided. Evidence abounds regarding technologies that used to dominate the world but have never resurrected after users switched to other technologies for various reasons. Significant investment is needed in security infrastructure to boast user confidence.
	4. To ascertain the moderating effect of users'	Overall, the generational groups didn't have any significant moderating effect. Assessing them on individual construct however, helped to put some perspective to the discussion.		Future studies can still focus on and further examine possible potential generational effects.

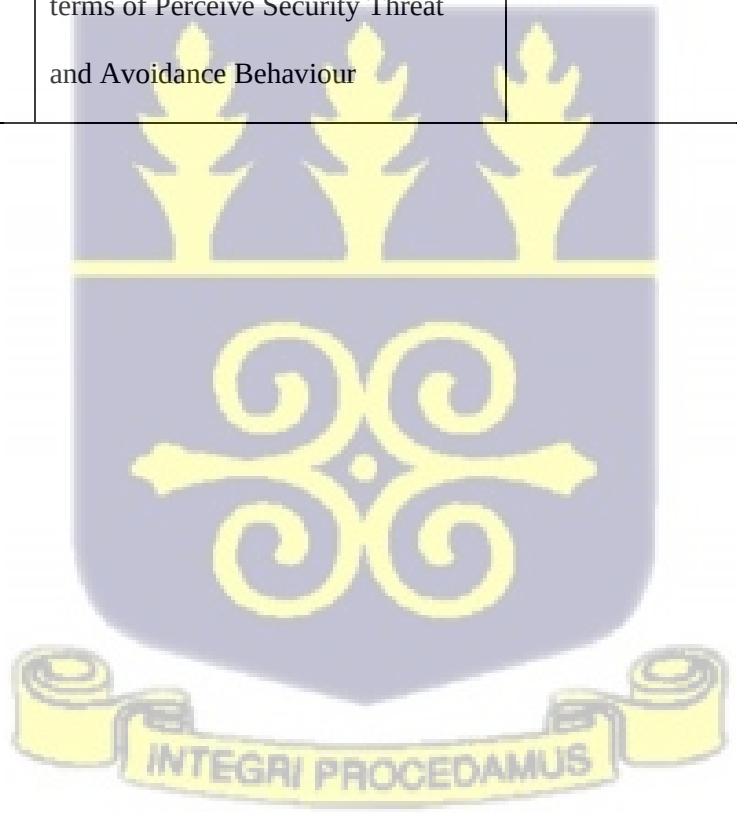
	generation in relation to their threat perception on their avoidance behaviour towards the MM service.	**For Susceptibility Threat** The positive relationship between Generation X and Y, and Generation X and Z, shows that these generations will portray similar behaviour in terms of Susceptibility Threat and Avoidance Behaviour. The negative relationship between Generation Y and Z, means that these two generation groups behave in opposite manner when it comes to Susceptibility Threat and Avoidance Behaviour **For Severity Threat**	Althaus (2019), Owusu et al. (2017) Panjaitan et al. (2019) Debb, Schaffer and Colson (2020)	By comparing the various generation groups, people within the age groups 46-60 and 31-45 are likely to make similar decisions on issue of susceptibility, as well as people within the age groups 46-60 and 30-Below making similar decisions on issue of susceptibility. People within the age groups 31-45 and 30-Below are likely to behave differently on susceptibility.
Theoretical gap in technology avoidance behaviours among technology users using generational groups as moderating variables (Liang & Xue, 2009; Carpenter et al., 2019: Levickaitė, 2010)				On the issue of Severity Threat, the negative relationship shows that whiles people within the age group 46-60years may choose to stick with the MM service, those within the age group 31-

		The negative relationship between Generation X and Y shows that the behaviour of these two generations is opposite to each other when it comes to Severity Threat and Avoidance Behaviour The positive relationship between Generation X and Z, and Generations Y and Z, shows that in both instances, these generations behave in similarly in terms of Severity Threat and Avoidance Behaviour **For Self-Efficacy** The negative relationships between Generation X and Y, and Generation		45 may choose to avoid the MM service, or vice versa. On the other hand, people within the age group 46-60 and 30-Below, as well as 31-45 years and 30-Below, are all likely to either stick with the MM service or avoid the using service. Regarding Self-Efficacy, if people within the age 46-60 years decide to avoid the MM service, those within the age group 31-45 years are likely not to avoid the service, and vice versa. This

		X and Z, shows that in the given scenario, these generations behave in an opposite manner to each other in terms of Self–Efficacy against Avoidance Behaviour On the other hand, the positive relationship between Generations Y and Z, the behaviour of these two generations is similar in terms of Self–Efficacy and Avoidance Behaviour **For Perceived Effectiveness** The positive relationship between Generation X and Y, Generation X and Z, and Generation Y and Z,		verdict or explanation is also same for those between 46-60 years and 30-Below. Inversely, those with the age 31-45 years and 30-Below years are likely to make the same decision i.e., all avoid, or all do not avoid. Regarding Perceived Effectiveness, a between group comparison of all generational groups shows all groups are likely to have the same perception regarding effective solutions. They are

		shows that all generational groups behave almost the same in terms of Perceived Effectiveness and Avoidance Behaviour		all likely to believe that solutions are effective, or they don't believe. When users perceive provided solutions are not effective, this notion will be the same no matter how each generation is compared to the other.
		For Perceived Security Threat The negative relationships between Generation X and Y, and Generation X and Z, shows that in the given scenario, these generations behave in an opposite manner to each other in terms of Perceived Security Threat against Avoidance Behaviour		Regarding Perceived Security threat, people within the age 46-60 years and 31-45 years are likely to have divergent or opposing perception on security threat. This postulation is also the same for people within the age 46-0 years against ages 30-Below. Conversely, people within the age 31-45years and 30-Below will likely have the same security threat perception.

		The positive relationship between Generations Y and Z, the behaviour of these two generations is similar in terms of Perceive Security Threat and Avoidance Behaviour		



9.4 Contributions of the Study

First, this study contributes to the body of knowledge in information systems by providing literature for information systems research.

9.4.1 Contribution to Theory and Body of Knowledge

From the theoretical perspective, this study also makes important contributions to particularly the TTAT, which served as the backbone theory for this study. The TTAT has been used in several studies that have sought to examine the behaviour of technology users in relation to potential threats associated with the technology. This theory took it roots from the Technology Acceptance Model (TAM), with some major contributions from the Protection Motivation Theory.

To begin with, this study makes a great theoretical contribution as it deliberately examined the role of the various generations in influencing the linkage between threat and coping perception on avoidance behaviour. After the TTAT was propounded by Liang and Xue (2009) almost all studies that have been conducted using the TTAT have mostly sought to test the theory or consider other potential factors that could play contributing roles in determining avoidance motivation or behaviour. However, establishing an important role of various generational groups on the relationship between perception of threat and avoidance motivation, has not been attempted after reviewing literature. This study is novel as gives an important insight to the potential role of either or all of Generations X, Y and Z, that a technology user might belong to, on the relationship between their perception of threat and its consequential effect on avoidance motivation or behaviour. This is particularly important as technology, just as with other social phenomenon, are not static and have transformed over the years. Each generational group experiences different technological advancement, coupled with the occurrence of other equally impacting social events, it is safe to assume that each generation will react differently to new technologies as they come

more so as they are accompanied with threats. Although, the study did not find significant moderator effect for generational hypothesis which could be attributed to several factors, important relationships were established between the generational groups. This provides an important step for future studies in testing the TTAT along such parameters.

Next, this study contributes to the TTAT by moving the theory from the proposition of technology threats affecting avoidance motivation to actually measuring the expression of the behaviour. Although other studies have established a significant direct positive relationship between Avoidance Motivation and Avoidance Behaviour, literature on this association remains significantly few. Liang and Xue(2009) the original proponents of the TTAT asserted that the presence of threats in relation to a technology places the technology user in two main constraint: a situation where they may avoid using the technology totally after assessing the threat and realizing that they could avoid the threat, referred to in the theory as problem–focused coping strategy, or, a possible situation of coping with the threat after assessing and realizing they are unavoidable an hence have to manage the them whilst still using the technology, referred to in the theory as emotion–focused coping strategy. In the context of the problem focused coping strategy, the presence of the threat give rise to avoidance motivation on the part of the technology user, which may eventually lead to avoidance behaviour. The use of the word "may", connotes a possibility and not a cast-in-stone position as other studies have raised the question of whether motivation always leads to the actual manifestation of the behaviour. This study adds to the literature, specifically by establishing a direct relationship between avoidance motivation and avoidance behaviour, and as a result, also partly addresses the above question raised.

In addition, this study goes further to examine how the manifestation of avoidance behaviour, influence technology users' decision to continuously use a technology. As has been stated, TTAT

is well known from the point of threat identification to avoidance motivation and possibly behaviour. However, the question of continuous usage was never attempted by the theory. Perhaps, for the reason that, that wasn't the focus of the theory, it is also legitimate to ask whether a display of a behaviour today necessarily predict continuous display of the same behaviour. In the context of technology usage, does the manifestation of the avoidance motivation through the behaviour necessarily establishes a continuous pattern? This study sought to examine this association by assessing the avoidance behaviour of respondent as an antecedent or enough evidence to future continuous usage. The findings of this study established that, indeed, avoidance behaviour now is enough prerequisite, antecedent or testament that a future avoidance or continuous usage is possible. This goes further to strengthen the TTAT as a good predictor of future behaviour in the context of this study.

9.4.2 Contribution to Policy

This study makes enormous contribution for both policy directions and work of practitioners. For policy makers, the advent of mobile money in the Ghanaian financial space has come with benefit and satisfaction as it has enormously bridged the gap in financial inclusion. The government of Ghana, before the advent of mobile money, had tried a number of policy initiatives to solve the problem of financial inclusion but with little success. A such, the success enjoyed by the mobile money service as it has penetrated both the formal and informal sector of the economy have ensured the access to financial services by the general population, coupled with the opportunities that it presents to government in terms of revenue generation through taxes, among others. It is therefore not surprising that government must have keen interest in the issues surrounding mobile money fraud. This study has established that the issue of mobile money fraud, if not properly tackled, could pose and existential threat to the service. Although there is a great level of

responsibility on service providers, the assistance of government is such fight would come highly handy. Continuous rise in mobile money fraud cases will derail the trust of users or subscribers which may eventually affect the growth, sustainability and profitability of the service.

Mobile money service has also created a great deal of opportunity for employment, a problem that governments all over the world have been struggling with. As at March 2020, the Bank of Ghana reported that there were over 230, 000 mobile money agents alone spread across the country, a huge support in governments effort to combat unemployment. Coupled with the long list of other employment opportunities that the service provides along the mobile money value chain, all effort in ensuring it sustainability should be a priority agenda for the government. The government has done well by instituting the World's first ever Digital Finance Policy in the year 2020, a policy that has helped in the removal of fees for low value transactions, has increased the minimum daily limit for transactions by mobile money subscribers, allowed for interoperability of transactions from one service provider to the other with less fees as well. The policy has a four-year short to medium term agenda which includes:

- Improving governance of the DFS ecosystem
- Supporting Fintech
- Creating an enabling regulatory framework
- Actively building the capacity of authorities to supervise the space.
- Supporting the development of market infrastructure for DFS
- Driving the expansion of digital payment use cases.

All these are important steps that will do the service and subscribers a lot of good. Although the policy tackles building capacity to curtail such issues as mobile money fraud, perhaps, a more

comprehensive policy such as that of financial crime act or regulations in Ghana, may do the service a lot better.

It is also important that such research inform policy direction in the area of new avenues for financial crime activities. The advent of mobile money has opened up new ways through which money laundering and other financial crimes such as has engulfed the service, could be perpetrated. Ghana has in place a well informed and internationally acclaimed money laundering and financial crimes laws. Although this law was made to cover all forms of financial crimes, it has mostly been targeted at commercial banks as they have been the main avenue through which such crimes occur. However, as mobile money service has spread globally, receiving remittances have now become a lot easier, as foreign remittances to locals does not go through the banking sector anymore with more and more subscribers receiving such remittances unto their wallets. A more sophisticated policy direction and implementation strategy is needed for the Fintech sector in order to enhance user confidence and trust in the service.

9.4 .3 Contribution to Practice

This study also makes enormous contribution to the providers of mobile money service. Perhaps, they stand to benefit the most from the findings of this study as the service has now become the mainstream of revenue generation for the telecoms involved.

The issue of mobile money fraud has been a great concern to service providers as it has for users. From impersonation of staff of service of service providers to all manner of fraud attempts, it may be safe to assume that perhaps, even staff of telecommunication companies may have fallen victim to mobile money fraud. It is instructive to emphasize that all respondents are aware and are concerned with the issue of fraud. The fact that respondents are aware of fraud attacks may be positive for the service and telecoms could ride on this awareness to educate subscribers. Educating

subscribers on the various forms of fraud attacks and remedies available to them will help provide raise subscriber confidence.

It is also important that telecoms focus their education message on both the literate and illiterates. It is instructive to note that a lot of the education drive against mobile money fraud such as adverts, are done mostly in English language. This might serve well for the elite as they will stay well informed. This was particularly evident in this study as majority (over 80 percent) of respondents had obtained Senior High education or above and so felt less at risk of fraud attacks as they considered themselves well abreast with information on what to do. This may not be the case for the uneducated who may find it difficult deciphering who a genuine or fake staff of a telecom network may be. Structuring educational messages on mobile money fraud will serve a great deal for customers who may not be educated.

The telecom sector thrives on technology which definitely doesn't come cheap. To seek to implement a mobile financial service such as that of mobile money service even adds more cost to these telecoms. The great technological strides that have been made globally, has put these telecoms constantly at risk of cyberattacks from cybercriminals. Security is therefore a major requirement for such service providers, worse of all after mobile money service has been included in their activities. Service providers have to constantly invest in modern security equipment and software as cybercriminals become more sophisticated. This is also important in ensuring that customers always feel safe and do not have any feeling of insecurity about funds on their wallets. the inclusion of mobile money service among their operations has made these service providers more attractive and appetizing to cybercriminal attacks.

9.5 Limitations of the Study

As with many research, this study is also limited in certain parameters due to the limitations it faced. It is however also important to establish that these limitations do not make the findings of this study null or void. They are only factors that when sufficiently controlled, would make the study even better.

First, this study faced a limitation of being cross sectional rather than longitudinal. A cross sectional study basically refers to an observational study whose data was collected and analyzed within a specific point in time across a sample population whereas a longitudinal study collects and analyze different sets of data from the same study population over an extended period of time. The issue of mobile money fraud, although growing rapidly, is also fairly new to the operators and stakeholders of the service. In Ghana for instance where the study was conducted, the mobile money service itself began in the year 2007 and so it's only a decade and a half old. Since it started, the services have constantly varied and improved, as it has included a lot more services than just sending electronic cash. The service has grown and has become very popular in the Ghanaian financial space. The issue of fraud also began a few years down the line and with the widespread popularity of the service, the resolve of users to keep using the service is still being tested as stakeholders put in frantic efforts to drastically minimize or eradicate the fraud issues by plugging all possible loopholes in the provision of the service. Therefore, examining avoidance behavior among users by analyzing a single data set may not be sufficient to prove distrust among users who have become accustomed to the service and have come to appreciate it convenience, flexibility and accessibility.

In addition, the sample of 384 respondents, although large enough for statistical analysis, may prove insufficient to establish an avoidance or non-avoidance behavior on the part of mobile

money users. This may partly account for the reason behind the fact that, statistically, most of the hypothesis were not significant although effects were established. For a service that has over 14.7 million active accounts according to data published by the Bank of Ghana as of March, 2020, a sample of 384 may not be enough to establish a generalizable conclusion.

There is also the limitation from the selected constructs that were used for the study. In order to examine avoidance behavior among subscribers or users of mobile money as a result of fraud, the study used only five constructs as measure. Given that the use of these construct could give insight to possible behavioral intentions, it is also instructive to emphasize that the avoidance behavior of the study's respondents will not be adequately accounted for by these five constructs. There are potentially numerous factors that can affect a person's intention to avoid a technology such as belief systems, as some cultural and religious beliefs may not subscribe to over digitization. Others such as the degree of a formalized economy and the nature of occupation that the people are engaged in, could all be potential factors that future research could investigate.

Also, as it was evident from the sample demographics, a large percentage of the respondents had completed either Senior High School or even higher. This is very important as it demonstrates the level of literacy among respondents. As has been established from literature, the most prevalent form of mobile money fraud is customer fraud; where a customer receives a text or a call from an unknown person claiming to be a representative of the service provider calling to inform the users of winning a lottery, or some other person calling to deceive a subscriber in any form. Based on their level of education, respondents may be well informed on the issue of fraud and well abreast and smart enough to decipher what is a fraud attempt. This potentially could account for the non-significant effect established between the variables, a situation that could potentially be a limitation

for the study. Perhaps, another study with less literature or illiterate subscribers could establish interesting revelations.

Finally, the study was also limited in terms of resources to execute the study raising contextual limitations to the findings. This study was conducted in Accra, the capital of Ghana, with all samples who responded to the questionnaire being in Accra. There are however, sixteen regions in Ghana, with mobile money having strong presence. Although there is no statistical breakdown of regional cases of mobile money fraud, it would be safe to assume that prevalence of fraud attempts may differ, and even perhaps considerably based on regions. However, due to resource constraint the study could not gather data from across the country. In addition, experience of fraud and the nature of fraud may differ from one user to the other, as a result,

9.6 Suggestions for Future Studies

Despite the limitations, this study also presents a lot of positives out of which the following recommendations are suggested. Besides the use of the TTAT primarily as the source of the constructs used for the study, future researchers can also consider the inclusion of other factors cultural disposition of respondents and its contribution to avoidance behaviour, the risk aversion of respondents and perhaps the specific role of education when it comes to technology use and avoidance behaviour. The cultural values of an individual play an integral role in establishing the behavioural patterns of an individual or a group, for example whether a society is collectivist or individualist, has its own ramifications on a person in terms of what they consider to be risky enough to take necessary steps. Further, individuals differ in terms of their risk assimilation levels. Whiles some may be risk averse, others might be risk takers, and both situations have its own way of influencing behavioural patterns. There is also the potential role of the level of education and its role in determining how a technology user will respond to threatening situations.

Establishing a significant effect for the moderator variable Generation X, Y and Z, could be experimented using a larger sample size. As has been established, a number of studies have posited the differences in the adoption behaviour of different generation groups. What this study sought to do was to begin to lay the foundations for studies regarding moderator effect of generational groups using the TTAT as the main underlying theory. Researchers can further this study by enlarging the sample size to give more data in order to identify potential effects.

Also, future research can include charts and other statistical outputs, as well as the use of digitzed analytical tools that would appeal more to non-IS scholars.

Finally, this study recommends a wider or broader context specifically in terms of geographical coverage. Mobile money service and it associated fraud issues are spread across a host of countries on the African continent. Examining it effect on subscriber perception of security and patronage of the service would likely provide more interesting revelations for policy directions and stakeholder decisions.

9.7 Conclusion

In conclusion, this study serves as a revelation to all stakeholders along the mobile money value chain. As to whether effects established were significant or not, the issue of mobile money fraud is causing trepidation among users of the service, affecting user trust and confidence. It is important that maximum effort is put in by all stakeholders as one party cannot tackle it. Government needs to ensure maximum support to service providers, as they also strive to put in the needed technological and human resource investment to ensure a sustained fight. Users of the service must ensure constant alertness and stay informed of current issues about the service to help reduce risk of exposure to these fraud attacks.

REFERENCES

Abdullahi, R., & Mansor, N. (2015). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent For Future Research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *1* (4), 38-45.

Abdurrahaman, D. T., Owusu, A., Soladoye, B. A., & Kalimuthu, R. K. (2018). Celebrity Brand Endorsement - A Study on its Impact on Generation Y-ers in Nigeria. *Asian Journal of Cseintific Research*, *11* (3), 415-427.

Adebisi, J. F., & Gbegi, D. O. (2013). Effect of Tax Avoidance and Tax Evasion on Personal Income Tax Administration in Nigeria. *Journal of Humanities and Social Sciences*, *1* (3), 1-20.

Adedoyin, A., Kapetanakis, S., Samakovitis, G., & Petridis, M. (November 2017). Predicting Fraud in Mobile Money Transfer Using Case-Based Reasoning. *International Conference on Innovative Techniques and Applications of Artificial Intelligence*, *1* (1), 1-8.

Afeti, E. Y., & Owusu, A. (2022). Impact of Mobile Payments on Micro-Business Activities: A Developing Country Experience. In R. Boateng, S. L. Boateng, T. Anning-Dorson, & B. L. Olumide (Eds.), *Digital Innovations, Business and Society in Africa. Advances in Theory and Practice of Emerging Markets* (pp. 75-95). Springer, Cham.

AFI. (2015, January). *AFI Annual Report: Making Financial Services More Accesible to the World's Unbanked. Kuala Lumpur, Malaysia*: Retrieved from Alliance for Financial Inclusion.

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). Research Report: The Evolving Relationship Between General and Specific Computer Self-Efficacy - An Empirical Assessment. *Journal of Information Systems Research*, *11* (4), 418-430.

Aheebwa, J. (2022, June 28). *How Ugandans lose millions in mobile money fraud*. Retrieved from MONITOR: https://www.monitor.co.ug/uganda/business/prosper/how-ugandans-los-millions-in-mobile-money-fraud

Ahmad, H. A., Green, C., & Jiang, F. (2020). Mobile Money, Financial Inclusion and Development: A Review With Reference to African Experience. *Journal of Economic Surveys, Willey Blackwell, 34* (4), 753-792.

Aklorbortu, P. (2019, September 9). *Fact Check: MTN shuting down mobile money service is false*. Retrieved from YEN: https://yen.com.gh/132869-fact-check-mtn-shutting-mobile-money-service-false.html

Akomea-Frimpong, I., Andoh, C., & Akomea-Frimpong, A. (2019). Control of Fraud on Mobile Money Services in Ghana: An Exploratory Study. *Journal of Money Laundering Control, 22* (2), 300-317.

Albashrawi, M., & Motiwalla, L. (2017). Privacy and Personalization in Continued Usage Intention of Mobile Banking: An Integrative Perspective. *Information Systems Frontiers*, 1-13, https://doi.org/10.1007/s10796-017-9814-7.

Albrecht, C., Turnbull, C., Zhang, Y., & Skousem, C. J. (2010). The Relationship between South Korean Chaebols and Fraud. *Managerial Auditing Journal, 33* (3), 1-25.

Aldiabat, K. M., & Le Navenec, C.-L. (2013). Data Saturation: The Mysterious Step in Grounded Theory Methodology. *Qualitative Report, 23* (1), 245-261.

Aliyu, A., Bello, M., Kasim, R., & Martin, D. (2014). Positivist and Non-Positivist Paradigm in Social Science Research: Conflicting Paradigms or Perfect Partners? *Journal of Management and Sustainability, 4* (3), 32-50.

Althaus, D. (2016). Differences of Millennials and Non-Millennials Privacy and Security Perceptions and Their Influence on Online Shopping Behaviour. *7th IBA Bachelor Thesis Conference. Enschede, Netherlands: University of Twente, 27* (3),1-12.

Andersson, L. M., & Bateman, T. S. (1998). Cynicism at the Workplace: Some Causes and Effects. *Journal of Organizational Behaviour, 18* (5), 449-469.

Andianaivo, M., & Kpodar, K. (2012). Mobile Phones, Financial Inclusion and Growth. *Review of Economics and Institutions*, *3* (2), 1-6.

Andrea, B., Gabriella, H. C., & Timea, J. (2016). Y and Z Generations at Workplaces. *Journal of Competitiveness*, *8* (3), 90-106.

Annan, S. E. (2017, October 7). *Avoiding Fraud Due to Mobile Money*. Retrieved from GhanaWeb: https://mobile.ghanaweb.com/GhanaHomePage/business/Avoiding-farud-due-to-mobile-money-588682

Antovski, L., & Gusev, M. (2003). M-Commerce Services. *Institute of Informatics, Faculty of Natural Sciences and Mathematics. Ss. Cyril and Methodus University*, *12* (2), 15-23.

Anurag, S., Tyadi, R., & Raddi, S. (2009). Mobile Payment 2.0: The Next - Generation Model. *HSBC's Guide to Cash, Supply Chain and Treasury Management in Asia Pacific*, *8* (2), 178-183.

Arachchilage, A. G., & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. *Journal of Computers in Human Behaviour*, 38, 304-312.

Aron, J., & Muelbauer, J. (2019, May 7). *The Economics fo Mobile Money: Harnessing the Transformative Power of Technology to Benefit the Global Poor*. Retrieved from Voxeu Web site: https://voxeu.org/article/economics-mobile-money

Aron, J., Meulbauer, J., & Sebudde, R. (2015, February 3). *Inflation Forecasting Models for Uganda: Is Mobile Money Relevant?* Retrieved from Centre for Economic Policy Research: https://www.sbs.ox.ac.uk/sites/defaults/files/research-projects/mobile-money/inflation-forecasting

Asongu, S., & Asongu, N. (2018). The Comparative Exploration of Mobile Money Services in Inclusive Development. *International Journal of Social Economics*, *45* (1), 124-139.

Avornyo, P., Fang, J., Odai, R. O., Vondee, J. B., & Nartey, M. N. (2019). Factors Affecting Continous Usage Intention of Mobile Banking in Tema and Kumasi. *International Journal of Business and Social Science* , 114-126.

Ayo, C. K., Ekong, U. O., Tolulope, F. I., & Adebiyi, A. A. (2007). M-Commerce Implementation in Nigeria: Trends and Issues. *Journal of Internet Banking and Commerce, 7* (2), 1-17.

Baba, K. (2010, September 16). *Can Mobile Money Be Profitable? We Asked Mobile Money Managers*. Retrieved from CGAP: https://www.cgap.org/blog/can-mobile-money-be-profitable-we-asked-mobile-money-managers

Baganzi, R., & Lau, A. K. (2017). Examining Trust and Risk in Mobile Money Acceptance in Uganda. *Journal of Sustainability, 9* (1), 1-22.

Bagchi, K. K., & Udo, G. (2003). An Analusis of the Growth pf Computer and Inetrnet Security Breaches. *Communications of the Association for Information Systems, 12* (46), 684-697.

Bagozzi, R. P., Yi, Y., & Philips, L. W. (1991). Assessing Cinstruct Validity in Organizational Research. *Administrative Science Quarterly, 36* (1), 421-458.

Bandura, A. (1982). Self-Efficacy Mechanism in Human Agency. *Journal of American Psychologist, 37* (2), 122-147.

Bank of Ghana. (2016, December). *Payment Systems Oversight. Accra, Ghana*. Retrieved from Bank of Ghana Website.

Bank of Ghana. (2017, December). *Impact of Mobile Money on The Paymenet System in Ghana: An Econometric Analysis. Accra, Ghana*. Retrieved from Bank of Ghana Website.

Barclay, D. W., Thompson, R., & Higgins, C. (1995). The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Use as an Illustration. *Journal of Technology Studies: Special Issue on Research Methodology, 2* (1), 284-324.

Batista, C., & Vicente, C. P. (2018). Is Mobile Money Changing Rural Africa? Evidence from a field experiment. *NovaAfrica Working Paper Series*, wp1805, 1-61.

BBC Africa. (2018, July 20). *Phone Scam: How Kenyans are Losing Money*. Retrieved from BBC Africa: https://www.bbc.com/news/world-africa-44899854

Beaudry, A., & Pinsonneault, A. (2005). Understanding User Responses to Information Technology: A Coping Model of User Adaption. *Management Information Systems (MIS) Quarterly, 29* (3), 493-524.

Bejtkovsky, J. (2016). The Employees of Baby Boomers Generation, Generation X, Generation Y and Generation Z in Selected Czech Corporations as Conceivers of Development and Competitiveness in their Corporation. *Journal of Competitiveness, 8* (4), 105-123.

Bencsik, A., Horváth-Csikós, G., & Tímea, J. (2016). Y and Z Generations at Workplaces. *Journal of Competitiveness, 8* (3), 90-106.

Bergin, M., Wells, J. S., & Owen, S. (2008). Critical Realism: A Philosophical Framework for the Study of Gender and Mental Health. *Journal of Nursing Philosophy, 9* (3), 169-179.

Bersudskaya, V., Khan, M., & Kuijpers, D. (2016, August). *Agent Network Accelrator Survey: Uganda Country Report 2015. Kampala*. Retrieved from HELIX Institute of Digital Finance Website.

Bhattacherjee, A. (2001). Understanding Information Systems Continuance: An Expectation-Confirmation Model. *MIS Quarterly, 25* (3), 351-370.

Bhattacherjee, A., & Lin, C.-P. (2015). A Unified Model of IT Continuance: Three Complementary Perspectives and Crossover Effects. *European Journal of Information Systems, 24* (4), 113-132.

Bidet, J., & Kouvelakis, S. (2007). *Critical Companion to Contemporary Marxism.* Leiden, The Netherlands: BRILL Publishers.

Bittner, M.-I., Donnelly, M., Zanten, A. R., Andersen, J. S., Guidet, B., & Cabello, J. J. (2013). How is Intensive Care Reimbursed? A Review of Eight European Countries. *Annals of Intensive Care, 22* (3), 97-109.

BMGF. (2013, June). *2013 Bill & Melinda Gates Foundation Annual Report. London, England*. Retrieved from Bill & Melinda Gates Foundation Website.

Boateng, R. (2016). *Research Made Easy.* Charleston, USA: CretaeSpace Independent Publishing Platform.

Bank of Ghana. (2020, December). *Payment Systems Oversight Annual Report 2020. Accra, Ghana*. Retrieved from Bank of Ghana Website.

Bold, C., Porteous, D., & Rotman, S. (2012, February). *Social Cash Transfers and Financial Inclusion: Evidence from Four Countries. Washington DC, USA*. Retrieved from CGAP Website.

Bongomin, G. O., & Ntayi, J. M. (2020). Mobile Money Adoption and Usage and Financial Inlcusion: Mediating Effect of Digital Consumer Protection. *Emerald Publishing Limited, 22* (3), 1-21.

Botchey, F. E., Qin, Z., & Hughes-Lartey, K. (2020). Mobile Money Fraud Prediction - A Cross-Case Analysis on the Efficiency of Support Vector Machines, Gradient Boosted Decision Trees, Naive Bayes Algorithms. *Multidisciplinary Digital Publishing Institute - Information, 11* (8), 1-20.

Braun, V., Clarke, V., & Weate, P. (2016). Using Thematic Analysis in Sport and Exercise Research. In B. Smith, A. C. Sparkes (Eds.), *Routledge Handbook of Qualitative Research in Sport and Exercise* (pp. 213-227). Oxfordshire, England: Routeledge Work Press.

Brewster, D. (2014). *India's Ocean: The Story of India's Bid for Regional Leadership*. London, England: Routledge.

Bryman, A. (2008). *Social Research methods*. New York: Oxford University Press.

Buku, M. W., & Mazer, R. (2017, April). Fraud in Mobile Financial Services: Consumers, Providers, and the System. Washington DC, USA. Retrieved from CGAP Website.

Bulmer, M. (1979). Concepts in the Analysis of Qualitative Data. *The Sociological Review, 27* (4), 651-677.

BUSINESSTECH. (2021, January 23). *Beware these 2 Types of Mobile Money Fraud in South Africa*. Retrieved from BUSINESSTECH Web site: https://businesstech.co.za/news/software/462478/beware-2-types-of-mobile-fraud-in-south-africa/

Busuulwa, B. (2016, June 7). *Mobile Money Fraud, Crime Rate Increase in Uganda*. Retrieved from The East African: theeastafrican.co.ke/business/Mobile-money-fraud-and-crime-rate-increase-in-Uganda-/2560-3415786-quaydf/index.html

Byrne, B. M. (2013). *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming*. New York, USA: Routledge.

Byrne, B. M. (2016). *Structural Equation Modelling with AMOS: Basic Concepts, Applications, and Proggramming*. New York, USA: Routeledge.

Carpenter, D., Young, D. K., Barret, P., & McLeod, A. J. (2019). Refining Technology Threat Avoidance Theory. *Communications of the Association for Information Systems*, *44*, 380-407. https://doi.org/10.17705/1CAIS.04422.

Carver, C. (2006). Approach, Avoidance, and the Self-Regulation of Affect and Action. *Journal of Motivation and Emotion*, *30* (2), 105-110.

Cassara, J. (2019, June 2). *Mobile Payments, Smurfs and Emerging Threats*. Retrieved from Special Air Service (SAS): https://www.sas.com/en_us/insights/articles/risk-fraud/mobile-payments-smurfs-emerging-threats.html

CGAP. (2017, April). *CGAP Funder Survey 2017:Trends in International Funding for Financial Inclusion. Washington DC, USA*. Retrieved from Certified Government Auditing Professional (CGAP) Website.

Charalambous, A. I. (2010). Interpreting patients as a means of clinical practice: Introducing nursing hermeneutics. *International Journal of Nursing Studies*, *47* (10), 1283-1291.

Chen, Y., & Zahedi, M. F. (2016). Individual's Internet Security Perception and Behaviours: Polycontextual Contrast BetweenThe United States and China. *Management Information Systems (MIS) Quarterly*, *40* (1), 205-222.

Chin, W. W. (1998). The Partial Least Squares Approach for Structural Equation Modeling. In G. A. Marcoulides, *Modern Methods for Business Research* (pp. 295-336). New Jersey, US: Lawrence Erlbaum Associate Publishers.

Chin, W. W. (2010). How to Write Up and Report PLS Analysis. In V. V. Esposito, W. W. Chin, J. Henseler, & H. Wang, *Handbook of Partial Least Squares: Concepts, Methods and Applications* (pp. 655-690). New York, USA: Springer Publishers.

Churchil, G., & Lacobucci, D. (2010). *Marketing Research: Methodological Foundations.* Ohio, USA: Thomson/South-Western Publishers.

Churchill, G. A., & Iacobucci, D. (2009). *Marketing Research Methodological Foundations* . Nashville, TN, USA: Earlie Lite Books, Inc.

Clubb, A. C., & Hinkle, J. (2015). Protection Motivation Theory as a Theoretical Framework for Understanding the Use of Protective Measures. *Journal of Criminal Justice Studies, 28* (3), 1-20.

Cobla, G. M., & Osei-Assibey, E. (2018). Mobile Money Adoption and Spending Behaviour: The Case of Students in Ghana. *International Journal of Social Economics, 45* (2), 29-42.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioural Sciences.* Hillsdale New Jersey, USA: Lawrence Erlbaum Associates Publishers.

COMVIVA. (2019, January). *Annual Report for the Year . Gurgaon, Haryana*. Retrieved from Comviva Technologies Limited Website.

Cooper, B., & Esser, A. (2019). *Exploring Barriers to Remittances to sub Saharan Africa: Remittances in Nigeria.* Bellville, South Africa. Retrieved from Centre for Financial Regulation and Inclusion Website.

Coupland, D. (1991). *Generation X: Tales for an Accelerated Culture*. New York, USA: St. Martin's Press.

Coupland, J. (1989). Book Reviews. *Journal of Language and Social Psychology, 8* (1), 1-16.

Cressey, D. R. (1950). The Criminal Violation of Financial Trust. *American Sociological Review, 15* (6), 738-743.

Cressey, D. R. (1986). Why Managers Commit Fraud. *Australian and New Zealand Journal of Criminology, 19* (1), 1-27.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approach.*.California, USA: Sage Publications.

Cresswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed methods Aproaches*. California, USA. Sage Publications.

Cresswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* Thousand Oaks, Carlifonia: Sage Publications.

Dallal, G. E., & Wilkinson, L. (1986). An Analytic Approximation to the Distribution of Lilliefors Test Statistic for Normality. *The American Statistician, 40* (4), 294-296.

Danermark, B. D., Ekstrom, M., Jakobsen, L., & Karlsson, J. (2019). *Explaining Society: Critical Realism in Social Sciences.* London, England. Routledge.

Dasai, S. P., & Lele, V. (2017). Correlating Internet, Social Networks and Workplace – a Case of Generation Students. *Journal of Commerce & Management Thought,* Vol.8, 802-815.

David-West, O., Umukoro, I. O., & Mritala, O. (2017). Adoption and Use of Mobile Money Services in Nigeria. *Journal of Electronic Commerce, 10* (4), 2723-2726.

Debb, S., Schaffer, D., & Colson, D. (2020). A Reserve Digital Divide: Comparing Information Securirty Behaviours of Generation Y and Generation Z Adults. *International Journal of Cybersecurity Intelligence and Cybercrime , 3* (1), 42-55.

Deloitte. (2015, June). *Mobile Money Payment Industry Marketing Distribution*. Retrieved from Deloitte: https://www.deloitte.com/content/dam/Deloitte/lu/Documents/financial-servcies/Banking/lu-mobile-money-payment-industry-marketing-distribution

Demirguc-Kunt, A., Leora, K., Dorothe, S., Saniya, A., & Jake, H. (2017, October). *Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution.* Geneva, Switzerland. Retrieved from The World Bank Group Website.

Dill, K. (2015, March). *Things Employers Should Know About The Gen Z Workforce*. Retrieved from Forbes Magazin: http://www.forbes/com/sites/kathryndill/2015/11/06/7-things-employers-should-know-about-the-gen-z-workforce/

Diniz, E. H., Albuquerque, J. P., & Cernev, A. K. (2014). Mobile Payment: A Scoping Study of the Literature and Issues for Future Research. *Sage Journals*, *35* (1) 1-20. https://doi.org/10.1177/0266666914557338.

Donovan, K. P. (2012). Mobile Money for Financial Inclusion. *Journal of Information and Communication for Development, 5* (1), 61-72.

Dorminey, J. W., Fleming, A. S., Kranacher, M.-J., & Riley, R. A. (2010). Beyond the Fraud Triangle. *The CPA Jurnal; New York, 80* (7), 17-23.

Easton, G. (2009). Critical Realism in Case Study Research. *Industrial Marketing Management, Elsevier, 39* (1), 118-128.

Efon, B., & Gong, G. (1983). A leisurely look at the bootstrap, the jack-knife and the cross validation. *American Statistician, 37* (1), 36-48.

Ehrbeck, T., Pickens, M., & Tarazi, M. (2012, February). *Financial Incluive Ecosystems: The Roles of Government Today*. Washington DC, USA. Retrieved from Certified Government Auditing Professional (CGAP) Wedbsite.

Ein-Dor, T. (2014). Facing Danger: How do people behave in times of need? The case of adult attachment styles. *Frontiers of Psychology*, 1-18.

Elmore, T. (2014, July 1). *How Generation Z Differs from Generation Y*. Retrieved from Growing Leaders: http://growingleaders.com/blog/generation-z-differs-generation-y/

Ennew, C., & Sekhon, H. (2003). The Role of Trust in the Financial Services Sector: A Marketing Perspective. *Working Paper, 5* (1), 1-25.

Estrin, S., Pelletier, A., & Khavul, S. (2019, March 25). *Regulating Mobile Money: What's at stake*. Retrieved from London School of Economics, LSE: https://blogs.Ise.ac.uk/businessreview/2019/03/25/regulating-mobile-money-whats-at-stake/

Fang, H., Disteche, C. M., & Berletch, J. B. (2019). X Inactivation and Escape: Epigenetic and Structural Features. *Frontiers in Cell and Developmental Biology, 17* (1), 1-12.

Fanta, A. B., Mutsonziwa, K., Goosen, R., Emmanuel, N., & Kettles, N. (2016). The Role of Mobile Money in Financial Inclusion in SADC Region: Evidence uisng Finscope Survey. *Policy Research Paper, 10* (1), 9-17.

Fintech AFrica. (2017, June 7). *13 Years of MTN Mobile Money*. Retrieved from Financial Technology Africa: www.financialtechnologyafrica.com/2017/08/15/13-years-of-mtnmobile-money/

Fornell, C. D., & Lacker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18* (2), 39-50.

Freud, S. (1915). *The Unconscious.* Standard Edition. London, England: Hogarth

Fuller, C., Simmering, M. J., Atinc, G., & Atinc, Y. (2015). Common Methods Variance Detection in Business Research. *Journal of Business Research, 69* (8), 3193-3197.

Gaber, C., Gharout, S., Achemial, M., & Pasquet, M. (2012). Security Challenges of Mobile Money Transfer Services. *SARSSI Conference on Network and Information Systems Security, 24* (4), 1-4.

Galloway, A. (2005). *Encyclopedia of Social Measurement.* Texas, USA: Elsevier Incoporated.

Gee, J., & Button, M. (2019). *The Financial Cost of Fraud 2019: The Latest Data from Around the World.* London, England: Crowe LLP.

Ghana Business News. (2022, June 6). *Ghana Business News*. Retrieved from MTN Ghana pays Ghc 3.1 billion in taxes to government: https://www.ghanabusinessnews.com/2022/06/06/mtn-ghana-pays-ghc3-1b-in-taxes-to-government

GhiPSS. (2020, May 2). *Mobile Money Interoperability Growth*. Retrieved from Ghana Interbank Payment & Settlement Systems Limited : https://ghipss.net/index.php/component/categorymobile-money-interoperability

Gilbert, P. (2021, May 28). *Kenya, SA worst hit by mobile payment fraud*. Retrieved from Connecting Africa: https://www.connectingafrica.com/author.asp?section_id=761&doc_id=769857

Gill, J., & Johnson, P. (1997). *Research Methods for Managers.* London, England: Sage Publications.

Glum, J. (2015, January 13). *Marketing to Generation Z: Millenials Move Aside as Brands Shift Focus to Under-18 Customers*. Retrieved from International Business Times: https://www.ibtimes.com/marketing-generation-z-millenials-move-aside-brands-shift-focus-under-18-customers

Gosavi, A. (2017). Can Mobile Money Help Firms Mitigate the Problem of Acces to Finance in Eastern sub-Saharan Africa? *Journal of African Business*, *19* (3), 1-18.

GSMA. (2012, June). *Mobile Money for the Unbanked Annual Report 2012*. London, England: Retrieved from Global System for Mobile Communications (GSMA) Website.

GSMA. (2013, November). *The Mobile Economy 2013*. London, England: Retrieved from Global System for Mobile Communications (GSMA) Website.

GSMA. (2014, November). *Mobile for Development Digital Inclusion Report 2014*. London, England: Retrieved from Global Systems for Mobile Communications (GSMA) Website.

GSMA. (2015, December). *The State of Industry Report: Mobile Money*. London, England: Retrieved from GSMA Website.

GSMA. (2015, December). *The State of Industry Report: Mobile Money*. London, United Kingdom: Retrieved from GSMA Website.

GSMA. (2016, October). *State of Mobile Money in West Africa*. London, United Kingdom:Retreived from GSMA Website.

GSMA. (2017, November). *2017 State of the Industry Report on Mobile Money*. London, England: Retrieved from Global Systems for Mobile Communications (GSMA) Website.

GSMA. (2018, December). *Mobile for Development 2018 State of the Industry Report on Mobile Money*. London, England: Retrieved from Global Systems for Mobile Communication (GSMA) Website.

GSMA. (2019, December). *The State of Mobile Internet Connectivity 2019*. London, England: Retrieved from Global Systems of Mobile Communications (GSMA) Website.

GSMA. (2020, December). *The Mobile Money Sub-Saharan Africa* . London, England: Retrieved from Global Systems for Mobile Communication (GSMA) Website.

GSMA. (2021, November). *State of the Industry Report on Mobile Money*. London, England: Retrieved from Global System for Mobile Communications (GSMA) Website.

GSMA Connected Women. (2020, March). *MTN MoMo Pay Merchant Payments: Expanding Women's Mobile Money Use in Ghana*. London, England: Retrived from GSMA Website.

Gu, S., Wang, F., Patel, N. P., Bourgeois, J. A., & Huang, J. H. (2019). A Model for Basic Emotions Using Observations of Behavior in Drosophila. *Frontiers in Psychology*, *27* (1), 1-15.

Guba, E. G., & Lincoln, Y. S. (1994). *Competing Paradigms in Qualitative Research: Handbook of Qualitative Research.* California, USA: Sage Publications.

Gujral, P. S. (2020, July 6). *Vodafone Cash Waives Charges on Transfers up to GHC100 to other networks Indefinitely*. Retrieved from State Interests and Governance Authority: https://siga.gov.gh/siga/vodafone-cash-waives-charges-on-transfer-100-to-other-ntworks

Gurbuz, A. (2017). Mobile Money and Savings in Rural Kenya. *Department of Economics, Georgetown University Working Paper Series*, *17* (5), 1-27.

Gyaisey, A. P., & Owusu, A. (2022). Multi-Contextual Analysis of Internet Security Perception and Behavior: Perspectives of Anglophone and Francophone Internet Users. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *12* (1), 1-20.

Hair, J., Ringle, C., & Sarstedt, M. (2011). PLS SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19* (4), 139-151.

Hair, J., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. (2014). Partial Least Squares Structural Equation Modeling (PLS-SEM): An Emerging Tool for Business Research. *European Business Review*, *26* (2), 106-121.

Hall, D. B., & Wang, L. (2005). Two-component mixtures of generalized linear mixed effects modles for cluster correlated data. *Journal of Statistical Modelling*, *14* (3), 21-37.

Hamblett, C., & Deverson, J. (1964). *GENERATION "X"*. New York, USA. Gold Medal Books.

Heidigger, M. (1962). *Being and Time.* New Jersye, USA: Blackwell Publishing.

Henseler, J., & Christian, R. M. (2015). A New Criterion for Assessing Discriminant Vaildity in Variance-Based Structural Equation Modeling. *Journal of the Academy of Marketing Science*, *43* (1), 115-135.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). *The Use of Partial Least Squares Path Modeling in International Marketing: Advances in International Marketing.* Bingley, United Kingdom. Emerald JAI Press.

Herman, M. (1967). Economic Progress and Social Welfare. *Families in Society: Economic Progress and Social Welfare*, California, USA: Sage Publications

Holmes, R. (2011, May 24). *Boomers and Millenials Reshaping the Workplace*. Retrieved from The Courier: https://www.lincolncourier.com/x227107806/Rick-Holmes-Boomers-and-Millenials-reshaping-the-workplace

Howe, N., & Strauss, W. (2009). *Millenials Rising: The Next Great Generation*. New York, USA: Knopf Doubleday Publishing Group.

Hulland, J. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. *Strategic Management Journal, 20* (2), 195-204.

IMARC. (2022). *Ghana Mobile Money Market: Industry Trends, Share, Size, Growth, Opportunity and Forecast 2022-2027.* Pradesh, India: IMARC Group.

IMF. (2015). *2015 IMF Annual Report Tackling Challenges Together.* International Monetary Fund .

INTERPOL. (2020). *Mobile Money and Organized Crime in Africa.* The Global Initiative Against Transnational Organized Crime, Institute for Security Studies and INTERPOL.

INTERPOL. (2020). *Mobile Money and Organized Crime in Africa.* The Global Institute Against Transnational Organized Crime, Institute for Security Studies and INTERPOL.

Ishak, Q. N., & Owusu, A. (2022). Assessing the Mobile Money Value Creation in the Agriculture Value Chain: Evidence from a Developing Economy. In R. Boateng, S. L. Boateng, & T. Aning-Dorson (Eds), *Delivering Distinctive Value in Emerging Economies.* Routledge Productivity Press.

Jack, W., & Suri, T. (2011). Mobile Money: The Economics of M-PESA an update. *NBER Working Paper Series National Bureau of Economic Research, 7* (5), 1-10.

Jack, W., & Suri, T. (2016). The Long-Term Effects of Access to Mobile Money in Kenya. *Innovation for Poverty Action*, *11* (3), 1-25.

Janz, N. K., & Becker, M. H. (1984). The Health Belief Model. *Health Education & Behaviour*, *6* (1), 1-17.

Janz, N. K., & Becker, M. H. (1984). The Health Belief Model: A Decade Later. *Health Education Quarterly*, *11* (1), 1-47.

Jenkins, B. (2008). *Developing Mobile Money Ecosystem.* Washington DC, USA: International Finance Corporation and Harvard Kennedy School.

Jonker, M. (2003). Estimation of Life Expectancy in Middle Ages. *Journal of the Royal Statistical Society*, *166* (1), 105-117.

Jusuf, M. B., Utami, N. P., Hidayanto, A. N., & Shihab, M. R. (2017). Analysis of Intrinsic Factors of Mobile Banking Application Users' Continuous Intention An Evaluation Using an Extended Expectation Confirmation Model. *2017 Second International Conference on Informatics and Computing (CIC)*, 1-14, doi:10.1109/IAC.2017.8280589.

Kafeero, S. (2020, October 10). *Uganda's Banks have been Plunged into Chaos by a Mobile Money Fraud Hack*. Retrieved from Quartz Media Africa: https://qz.com/africa/1915884/uganda-banks-mtn-airtel-hacked-by-mobile-money-fraudsters/

Kafeero, S. (2020, October 10). *Uganda's Banks have been Plunged into Chaos by Mobile Money Fraud Hacks*. Retrieved from Quartz Media Africa: https://qz.com/africa/1915884/uganda-banks-mtn-airtel-hacked-by-mobile-money-fraudsters/

Kalakota, R., & Robinson, M. (2001). *E-Business 2.0: Roadmap for Success.* Boston, USA: Addison-Wesley Publishers.

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS Quarterly*, *12* (4), 571-586.

Kennedy, K., & Konjang, J. K. (2016). Mobile Money - A Potential Threat to Banks? *International Journal of Computer Applications*, *147* (4), 30-36.

Kim, C., Mirusmonov, M., & Lee, I. (2010). An Empirical Examination of Factors Influencing the Intention to Use Mobile Payment. *Computers in Human Behaviour*, 26, 310-322. doi:10.1016/j.chb.2009.10.013.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. *Journal of Decision Support Systems, 14* (4), 544-564.

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques.* New Delhi, India: New Age International Publishers.

Krishna, A. (2012). An Integrative Review of Sensory Marketing: Engaging the Senses to Affect Perception, Judgement and Behavior. *Journal of Consumer Psychology, 22* (3), 1-15.

Krishnan, S. K., Bopaiah, S., Bajaj, D., & R, P. (2013). Organization, Generation, and Communications - Infosys Experience. *NHRD Journal, 17* (2), 85-93.

Kuhn, T. S. (1970). *The Structure of Scientific Revolutions.* Chicago, USA: The University of Chicago Press.

Kupfer, A., Ableitner, L., Schob, S., & Tiefenbeck, V. (2016). Technology Adoption vs Continous Usage Intention: Do Decision Criteria Change when Using a Technology. *Twenty-second Americas Conference on Information Systems* (pp. 1-12). San Diego: Association of Information Systems.

La Chance, M. J., Beaudoin, P., & Robitaile, J. (2003). Adolescent's Brand Sensitivity in Apparel: Influence of Three Socialization Agents. *International Journal of Consumer Studies, 27* (1), 47-57.

Lahiri, A., Jha, S. S., Chakraborty, A., & Dobe, M. (2021). Role of Threat and Coping Appraisal in Protection Motivation for Adoption of Preventive Behaviour During COVID-19 Pandemic. *Frontiers in Public Health, 9*, 1-17.

Lake, A. J. (2013). *Risk Management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators.* Switzerland: Swiss Confederation State Secretariat for Economic Affairs & International Finance Corporation (World Bank Group).

Laryea, D. (2016, July 14). *Mobile Money Fraudsters very Cunning - Telcos Chamber Warns*. Retrieved from Ghana News Online: http://ghananewsonline.com.gh/mobile-money-fraudsters-very-cunning-telcos-chamber-warns/

Laryea, D. (2016, July 14). *Mobile Money Fraudsters very Cunning-Telcos Chamber Warns*. Retrieved from Ghana News Online: https://ghananewsonline.com.gh/mobile-money-fraudsters-very-cunning-telcos-chamber-warns/

LaTour, M. S., & Rotfled, H. J. (1997). There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. *Journal of Adertising*, *26* (3), 45-59.

Leavell, P. (2019). TAM and PLace: The Role of Convenience in Technology Acceptance. *AtMA 2019 Proceedings* (pp. 1-10). Karnakata, India: International Conference on Advanced Trends in Mechanical and Aerospace Engineering.

Ledden, L., Kalafatis, S., & Mathioudakis, A. (2011). The Idiosyncratic Behavior of Service Quality, Value, Satisfaction, and Intention to Recommend in Higher Education: An Empirical Examination. *Journal of Marketing Management*, *27* (11), 1232-1260.

Levickaitė, R. (2010). Generations X, Y, Z: How Social Networks from the Concept of the World Without Borders (The Case of Lithuania. *LIMES*, *3* (2), 170-183.

Lewis, J., & Ritchie, J. (2003). *Qualitative Research Practice - A Guide for Social Science Students and Researchers*. Thousand Oaks, England: Sage Publications.

Liao, C., Palvia, P., & Chen, J.-L. (2009). Information Technology Adoption Behaviour Life Cycle: Toward a Technology Continuance Theory (TCT). *International Journal of Inoformation Management*, 309-314.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *Management Information Systems Quarterly (MISQ)*, *33* (1), 71-90.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Asoociation for Information Systems*, *11* (7), 15-27.

Lincoln, Y. S., Lynhman, S. A., & Guba, E. G. (2011). PART II: Paradigms and Perspectives in Contention. In N. K. Denzin, & Y. S. Lincoln (Eds), *The SAGE Handbook of Qualitative Research* (pp. 97-128). California, USA: SAGE Publications.

Lings, I., & Greenly, G. E. (2010). Internal Market orientation and Market-Oreinted Behaviours. *Journal of Service Management*, *21* (3), 321-343.

Lister, L. M. (2007). A Practical Approach to Fraud Risk: Comprehensive Risk Assessments can Enable Auditors to Focus Antifraud Efforts on Areas where Their Organization is Most Vulnerable. *The Internal Auditor*, *16* (3), 1-30.

Macwan, U. (2017, April 24). *Mobile Technology, Its Importance, Present and Future Trends*. Retrieved from Finextra: https://www.finextra.com/blogposting/14000/mobile-technology-its-importance-present-and-future-trends

Malaquias, R. F., & Hwang, Y. J. (2016). An Empirical Study on Trust in Mobile Banking: A Developing Country Perspective. *Journal of Computer and Human Behaviour*, *22* (1), 453–461.

Malhotra, N., & Birks, D. (2007). *Marketing Research: An Applied Approach.* New Jersey, USA: Prentice Hall.

Marikyan, D., Papagiannidis, S., Rana, O. F., & Ranjan, R. (2021). Examining the Implications of the Samrt Homes for Work. *Tri-University Annual Conference: Towards a Post-pandemic Sustainable World-Cardiff Business School.* Cardiff, United Kingdom: Tri-University Annual Conference.

Martin, C. A., & Tulgan, B. (975-983). Managing the Generation Mix - From Collision to Collaboration. *Proceedings of the Water Environment Federation*, *21* (2), 103-133.

Maslow, A. H. (1943). A Theory of Human Motivation. *Managetment Pschycology*, *50* (3), 370-396.

Matheson, R. (2016, December 8). *Study: Mobile-money services lifts Kenyans out of Poverty*. Retrieved from Massachusetts Institute of Technology News: https://news.mit.edu/2016/mobile-money-kenyans-out-poverty-1208

Maurer, B. (2012). Mobile Money: Communication, Consumption and Change in the Payments Space. *Journal of Development Studies*, *48* (5), 589-604.

Maurer, B. (2015). *How Would You Like to Pay? How Technology is Changing the Future of Money*. Durham, United Kingdom: Duke University Press.

Mazer, R., & Garg, N. (2015). *Recourse in Digital Financial Services: Opportunities for Innovation.* Geneva, Switzerland: Retrieved from The World Bank Website.

McDonnel, R. (2020, May 1). *The 104 billion euro question: How should merchants take advantage of mobile-commerce growth in Europe*. Retrieved from J.P.Morgan: https://www.jpmorgan.com/europe/merchant-services/insight/mobile-payments-optimisation

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Journal of Information Systems Research*, *32* (1), 334–359.

Mead, G. H. (1962). *Mind, Self and Society*. Chicago, USA: The University of Chicago Press.

Merritt, C. (2010). Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments. *Retail Payments Risk Forum White Paper, Federal Reserve Bank of Atlanta*, 1-28.

Merritt, C. (2011). Mobile Money Transfer Services: The Next Phase in the Evolution of Person-to-Person Payments. *Journal of Payments Strategy and Systems*, *5* (2), 143-160.

Mingers, J., Mutch, A., & Willcocks, L. (2013). Critical Realism in Information Systems Research. *MIS Quarterly*, *37* (3), 795-802.

Mitrega-Niestroj, K., Puszer, B., & Szewczyk, L. (2018). Mobile Money Services Development: The Case of Africa. *University of Economics in Katowice: Contmporary Modern Finance Papers*, *9*, 79-95.

Morawczynski, O. (2015). *Six Takeawys from Rwanda's Financial Inclusion Insights Survey*. Washigton DC, USA: Retrieved from CGAP Website.

MTN Ghana. (2022, August 10). *How To Protect Yourself Against MoMo Fraud*. Retrieved from MTN GHANA: https://mtnghana.com.gh/mobile/money/fraud-how-to-protect-yourself

Mugambe, P. (2017). UTAUT Model in Explaining the Adoption of Mobile Money Usage by MSMEs' Customers in Uganda. *Journal of Advances in Economics and Business*, *18* (3), 129-136.

Mugisha, J., & Ainembabazi, J. H. (2014). The Role of Farming Experience on the Adoption of Agricultural Technologies: Evidence from Smallholder Framers in Uganda. *Journal of Development Studies*, *50* (5), 17-49.

Mukherji, P., & Albon, D. (2014). *Research Methods in Early Childhood: An Introductory Guide*. California, USA: SAGE Publications.

Murdock, H. (2008). The Three Dimensions of Fraud: Auditors Should Understand the Nees, Opportunities, and Justifications that Lead Individuals to Commit Fraudulent Acts. *The Internal Auditor*, *21* (1), 1-14.

Mustapha, S. (2017, October 17). *MTN sanctions 3,000 agents for mobile money fraud*. Retrieved from Graphic.com: https://www.graphic.com.gh/news/general-news/mtn-sanctions-3-000-agents-for-mobile-money-fraud.html

Muthoni, G. (2020, October 13). *How to Reverse MTN Mobile Money Transfer*. Retrieved from YEN: https://yen.com.gh/111977-how-reverse-mtn-mobile-money-transer.html

Narteh, B., Mahmoud, M. A., & Amoh, S. (2017). Customer Behavioural Intentions Towards Mobile Money Services Adoption in Ghana. *The Service Industries Journal*, *37*, (7), 426-447.

Neuman, W. (2011). *Basics of Social Research: Qualitative and Quantitative Approaches (2nd Ed.)*. New Jersey: Pearson Education. In Nevin, A. S., & Omosomi, O. (2019). *Stregth from Abroad: The Economic Power of Nigeria's Diaspora*. Lagos, Nigeria: Price Waterhouse Coopers.

Ng, A., & Lovibond, P. F. (2020). Self-Efficacy Moderates the Relationship Between Avoidance Intentions and Anxiety. *Pub Med*, *35* (3), 1-17.

Ng, A., & Lovibond, P. F. (2017). Intentions Matter: Avoidance Intentions Regulate Anxiety via Outcome Expectancy. *Journal of Behavioural Research, 32* (2), 49-64.

Ng, J. Y., Ntoumanis, N., Thogersen-Ntoumani, C., Leci, E. L., Ryan, R. M., Duda, J. L., & Williams, G. C. (2012). Self Determination Theory Applied to Health Contexts: A Meta-Analysis. *Perspectives on Psychological Science, 27* (4). 325-342.

Nicco-Annan, J. (2020, May 28). *Everything you need to know about mobile money in Ghana*. Retrieved from WorldRemit: https://www.worldremit,com/en/blog/money-transfer/mobile-money-remittances

Nunnaly, J. C. (1978). *Psychometric Theory*. New York: McGraw-Hill, 2nd Ed.

Nyaga, J., & Ogollah, K. O. (2015). Challenges Facing Penetration of New Mobile Money Transfer Services in Nairobi. *Journal of Economics and Finance*, DOI:10.6084/M9.FIGSHARE.1424917.V1.

Nyambe, G. (2022, February 24). *Scams on the Rise as Mobile Money Booms*. Retrieved from MAKANDAY: Centre for Investigative Journalism: https://www.makanday.com/posts/scams-on-the-rise-as-mobile-money-booms

Olesen, P., Westerberg, H., & Kingberg, T. (2004). Increased Prefrontal and Parietal Activity After Training aof Working Memory. *Nature Neuroscience, 7* (1), 75-79.

Oliver, R. L., & Berger, P. K. (1979). A Path Analysis of Preventive Health Care Decision Models. *Journal of Consumer Research, 17* (1), 113-122.

Omyango, R., Ongus, R., Awour, F., & Nyamboga. (2014). Impact of Adoption and Use of Mobile Phone Rchnology on the Performance of Micro and Samll Enterprises in Kisii. *World Journal of Comoputer Application and Technology, 2* (2), 22-39.

Onyango, R., Ongus, R., Awuor, F., & Nyamboga, C. (2014). Impact of Adoption and Use of Mobile Phone Technology on the Performance of Micro and Small Enterprises in Kisii Municipality Kenya. *World Journal of Computer Application and Technology, 2* (2), 34-42.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2* (1), 1-28.

Otieno, C. O., Liyala, S., Odongo, B. C., & Abeka, S. (2016). Challenges Facing the Use and Adoption of Mobile Phone Money Services. *World Journal of Computer Applications and Technology*, *4* (1), 8-14.

Owusu, A. (2017). Business Intelligence Systems and Bank Performance in Ghana: The Balanced Scorecard Approach. *Cogent Business Management*, *4*(1), 1-22.

Owusu, A., Bakare, A. S., & Abdurrahaman, D. T. (2017). The behavior response of the nigerain youths toward mobile advertising: An examination of the influence of values, attitudes and culture. *Cogent Business & Management*, *4*(1), 1-18.

Owusu, A. (2019). Examining the Moderating Effects of Time-Since-Adoption on the Nexus Between Business Intelligence Systems and Organisational Performance: The Ghanaian Banks Perspectives. *International Journal of Technology Diffusion*, *10* (3), 46-63.

Panjaitan, M., & Winarto, J. N. (2019). Examining generation X experiences on using e-commerce: integrating the technology acceptance model and perceived risks. *Journal of Physics Conference Series*, *19* (4), 1-5.

Parekh, N., & Hare, A. (2020). *The Rise of Mobile Money in Sub-Saharan Africa: Has this digital technology lived up to its promises?* Massachusetts, USA: J-PAL Africa.

Pavlov, I. P. (1927). *Conditioned Reflexes: An Investigation of the Physiological Activity of the Cerebral Cortex.* Oxford, England: Oxford University Press.

Peterson, B. K., & Buckhoff, T. A. (2004). Anti-Fraud Education in Academia. *Advances in Accounting Education, Teaching and Curriculum Innovations*, *15* (2), 45-67.

Philips, D. C., & Burbules, N. C. (2000). Postpositivism and Educational Research. In D. C. Philips, & N. C. Burbules, *Philosophy, Theory, and Educational Research Series* (p. 112). Lahham, MD: Rowman & Littlefield Pubishers.

Phiri, P. (2019, March 6). *IN Zambia, Scams on the Rise as Mobile Money Bonus: Has the digital technology lived upt to its promises*. Retrieved from Global Press Journal: https://globalpressjournal.com/africa/zambia-scams-rise-mobile-money-booms/

Phiri, P. (2019, March 6). *In Zambia, Scams on the Rise as Mobile Money Booms*. Retrieved from Global Press Journal: https://globalpressjournal.com/africa/zambia-scams-rise-mobile-money-booms/

Podsakoff, P., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common Method Biases in Behavioural Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology, 88* (5), 879-903.

Powell, R., & Connaway, L. (2004). *Basic research methods for librarians.* London: Libraries Unlimited. Powers, S. (2022, April 14). *Mobile Money: Using Your Cell Phone to Transfer Funds*. Retrieved from Investopedia: https://www.investopedia.com/financial-edge/0910/mobile-money-using-your-cell-phone-to-transfer-funds.aspx#toc-how-does-it-work

Propser, K. (2021, June 6). *How To Protect Your Mobile Money Account from Fraudsters*. Retrieved from EMMARNITECHS.COM: https://emmarnitechs.com/how-to-protect-your-mobile-money-wallet-from-fraudsters

Provencal, R. O. (2017, August 2). *Mobile Money Fraud on the Rise in Ghana: Victims share their stories*. Retrieved from Rainbow Radio Online: http://rainbowradioonline.com/index.php/general-news/item/9324-mobile-money-fraud-onthe-rise-in-ghana-victims-shares-their-stories

Provencal, R. O. (2017, August 2). *Mobile Money Fraud on the Rise in Ghana: Victims share their Stories*. Retrieved from Rainbow Radio Online: https://rainbowradioonline.com/index.php/general news/item/9324-mobile-money-fraud-on-the-rise-in-ghana-victims-shares-their-stories

Purnell, Y. (2022, March 20). *MoneyTransfers.com*. Retrieved from Mobile Money: What Is It & What Are The Benefits?: https://moneytransfers.com/sending-money/mobile-money/

Qian, J. (2010). *International Encyclopedia of Education.* Texas, USA: Elsevier Incoporated .

Quinn, V., Meenaghan, T., & Brannick, T. (1992). Fear Appeals: Segmentation is the Way to go. *International Journal of Advertising: The Review of Marketing Communications*, *11* (4), 355-366.

Rae, K., & Subramaniam, N. (2008). Quality of Internal Control Procedures: Antecedents and Moderating Effect on Organizational Justice and Employee Fraud. *Journal of Managerial Auditing*, *23* (2), 1-43.

Ramos, D., Solana, J., Buckley, R. P., & Greenacre, J. (2016). Protecting Mobile Money Customer Funds in Civil Law Jurisdictions. *The International and Comparative Law Quarterly*, *65* (3), 705-739.

Rao, S., & Vasudevan, S. (2021, June 7). *Mobile Money is Rewritting the Fraud Landscape in Africa*. Retrieved from Subex: https://www.subex.com/blog/mobile-money-is-rewriting-the-fraud-landscape-in-africa

Rezaee, Z., Crumbly, L., & Elmore, R. (2004). Forensic Accounting Education: A Survey of Academics and Practitioners. *Advances in Accounting Education, Teaching and Curriculum Innovations*, *6*, 193-232.

Riddell, C., & Song, X. (2011). The Role of Education in Technology Use and Adoption: Evidence from Canadian Workplace and Employee Survey. *CLSSRN Working Papers*, *11* (3), 1-20.

Ringle, C. M., Wende, S., & Becker, J. M. (2015). *SmartPLS 3*. SmartPLS GmbH, Benningstedt: http://www.smartpls.com.

Roberts, P. (2016, March 17). *Mobile Money Sees 118% Growth*. Retrieved from The BFT Online.com: http://thebftonline.com/business/ economy/21586/mobile-money-sees-118-growth.html

Roberts, P. (2016, March 17). *Mobile Money Sees 118% Growth*. Retrieved from The BFT Online: https://thebftonline.com/business/economy/21586/mobile/money/sees/118/growth/html

Rogers, E. M. (1983). Diffusion of Innovation. *University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research* .

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change 1. *The Journal of Psychology*, *91* (1), 79-106.

Rosenstock, I. M. (1974). The Health Belief Model and Preventive Health Behaviour. *Journal of Health Education and Behaviour, 2(1), 15-36.*

Royston, J. P. (1982). An Extension of Shapiro and Wilk's W Test for Normality to Large Samples. *Journal of the Royal Statistical Society*, *31* (2), 115-124.

Ryan, G. (2018). Introduction to Positivism, Interpretivism and Critical Theory. *Nurse Researcher, 25* (4), 14-20.

Safaricom. (2007, March 31). *M-Pesa - Mobile Money Transfer Service in Kenya*. Retrieved from M-Pesa Safaricom: www.safaricom.co.ke/mpesa_timeline/

Safaricom. (2007, March 31). *M-Pesa - Mobile Money Trasnfer Service in Kenya*. Retrieved from M-Pesa Safaricom: www.safaricom.co.ke/mpesa_timeline/

Sanchez-Prieto, J. C., Olmos-Miguelanez, S., & Garcıa-Penalvo, F. J. (2016). Informal tools in formal contexts: Development of a Model to Assess the Acceptance of Mobile Technologies Among Teachers. *Computers in Human Behavior*, 55, 519–528. doi:10.1016/j.chb.2015.07.002.

Sarantakos, S. (1998). *Social Research.* South Melbourne: Macmillan. Sarstedt, M., Ringle, C. M., & Hair, J. (2017). Partial Least Squares Structural Equation Modeling. In C. Homburg, M. Klarmann, & A. Vomberg, *Handbook of Market Research*. Springer.

Sarstedt, M., Ringle, C. M., & Hair, J. (2017). Partial Least Squares Structural Equation Modeling. In C. Homburg, M. Klamann, & A. Vomberg, *Handbook of Market Research* (pp. 1-34). AG: Springer International Publishing AG.

Sayer, A. (1992). *Method in Social Science: A Realist Approach.* London, England: Routledge.

Schafer, S. B. (2012). Optimizing Cognitive Coherence, Learning, and Psychological Healing with Drama-Based Games. *International Journal of Privacy and Health Information Management, 12* (4), 1-21.

Schäffer, B. (2015). *The Youngest Titans.* Hungary: Boook Publishing.

Schumacker, R. E., & Lomax, R. G. (2004). *A Beginner's Guide to Structural Equation Modeling, 2nd Ed.* New Jersey, USA: Lawrence Erlbaum Associates Publishers.

Schutz, A. (1962). *The Problem of Social Reality: Collected Papers 1.* The Hague: Marthus Nijhoff.

Scott, J., & Marshall, G. (2005). *A Dictionary of Sociology.* Oxford, UK: Oxford University Press.

Shaw, N. (2014). The mediating influence of trust in the adoption of the mobile wallet. . *Journal of Retailing and Consumer Services*, 21, 449-459. doi:10.1016/j.jretconser.2014.03.008.

Shen, S. (2014, June 18). *Forecast: Mobile Payment Worldwide 2013 Update*. Retrieved from Gartner Tech Rep: http://www.gartner.com/doc/2484915

Simiyu, C. N., & Oloko, M. (2015). Mobile Money Transfer and the Growth of Small and Medium Enterprises in Kenya: A Case of Kisumu City. *Journal of Economics, Commerce and Management, 3* (5), 1056-1065.

Skinner, B. F. (1953). *Science and Human Behaviour.* New York, USA: Simon and Schuster Publishers.

Stobierski, T. (2019, September 5). *How to do a cost-benefit analysis & why it is important*. Retrieved from Harvard Business School Online: https://online.hbs.edu/blog/post/cost-benefits-analysis-importnace

Straub, E. T. (2009). Understanding Technology Adoption: Theory and Future Directions for Informal Learning. *Review of Educational Research*, 625-649.

Strauss, R. G. (1991). Writing, Reviewing and Presenting an Abstract. *Journal of Clinical Apheresis*, *6* (4), 244-246.

Subex. (2017, May 4). *Service Providers Combat Mobile Money Frauds*. Retrieved from Subex: www.subex.com/subexhelps-service-providers-combat-mobile-money-frauds

Subex. (2017, May 4). *Service Providers Combat Mobile Money Frauds*. Retrieved from Subex: www.subex.com/subexhelps-service-providers-combat-mobile-money-frauds

Suri, T., & Jack, W. (2016). The Long-run Poverty and Gender Impacts of Mobile Money. *Science, 354* (6317), 1288-1292.

Sutherland, E. H. (1939). *Principles of Criminology.* Chicago, USA: J.B. Lippincott Company.

Tagoe, N. A. (2016). Who Regulates the Mobile Money Operations by Telcos? The Need for Robust Legislative and Regulatory Framework in Ghana. *Journal of Business and Financial Affairs*, DOI: 10.4172/2167-0234.1000208.

Tamakloe, G. K. (2019, February 9). *Challenges Faced by Mobile Financial Services in Ghana*. Retrieved from BASE Group: https://medium.com/@base-group

Tanner, J. F., Hunt, J. B., & Eppright, D. R. (1991). The Protection Motivation Model: A Normative Model of Fear Appeals. *Journal Marketing*, 6 (2), 1-15.

Tari, A. (2010). *Generation Y.* Budapest, Hungary: Jaffa Kaido Publication.

Tari, A. (2011). *The Generation Z.* Budapest: Jaffa Publishing.

Thanasak, R. (2013). The Fraud Factors. *International Journal of Management and Administrative Sciences (IJMAS), 2* (2), 01-0.

The World Bank. (2019, October 17). *Achieving Broadband Access for All in Africa Comes With a $100 Billion Price Tag*. Retrieved from THE WORLD BANK: https://www.worldbank.org/en/news/press-release/2019/10/17/achieving-broadband-access-for-all-in-africa-comes-with-a-100-billion-price-tag

Tijjani, R. K., Soladoye, B. A., Acheampong, O., & Abdurrahaman, D. (2018). Celebrity-Brand Endoresement: A Study on its Impacts on Generation Y-ers in Nigeria. *Asian Journal of Scientific Research, 11* (3), 415-427.

Tortosa, V., Moliner, M. A., & Sanchez, J. (2009). Internal Market Orientation and its Influence on Organisational Performance. *European Journal of Marketing, 43* (11), 1435-1456.

TRA India. (2013). *Telecommunication Regulatory Authority 2013 Annual Report.* New Delhi, India: Telecommunication Regulatory Authority, India.

Transparency International. (2018). *Corruption Perception Index.* Berlin, Germany: Transparency International.

Tyler, K., & Stanley, E. (2007). The Role of Trust in Financial Services Business Relationships. *Journal of Services Marketing, 13* (5), 1-15.

Uematsu, H., & Mishra, A. k. (2010). Can Education be a Barrier to Technology Adoption? *Agricultural & Applied Economics Association Conference*, *18* (7), 25-37.

UNCTAD. (2002). *E-Commerce and Development Report 2002.* New York and Geneva: United Nations Conference on Trade and Development (UNCTAD).

Van Hove, L., & Dubus, A. (2019). M-PESA and Financial Inlcusion in Kenya: Of Paying or Comes Saving? *MDPI Journal of Sustainability*, 23 (2), 1-26.

Velluet, Q. (2020, April 8). *Africa: Over 500 million mobile-money users expected in 2020*. Retrieved from The African Report: https://www.theafricareport.com/25846/25846/africa-over-500-million-mobile-money-users-expected-in-2020/

Vlcek, W. (2011). Development Policy Review. *Development Policy Review*, *29* (4), 415-431.

Vona, L. (2012). *Fraud Risk Assessment: Building the Fraud Audit Program.* New Jersey, USA: J. Willey & Sons.

Vona, L. W. (2021, February 22). *Fraud Risk Assessment: Folly or Prudence?* Retrieved from Fraud Auditing, Detection, and Prevention Blog: www.leonardvona.com/blog/fraud-risk-assessment-folly-or-prudence#

Voorhies, R. (2016, December 9). *The Eviddence is in: Mobile Money can help close the gender gap*. Retrieved from World Economic Forum: https://www.weforum.org/agenda/2016/12/the-evidence-is-in-mobile-money-can-help-close-the-gender-gap/

Vrechopoulos, A., O'Keefe, R. M., Doukidis, G. I., & Siomkos, G. J. (2004). Virtual Store Layout: An Experimental Comparison in the Context of Grocery Retail. *Journal of Retailing, 80* (1), 13-22.

Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Informations Systems*, *4*, 74-81.

Walsham, G. (2006). Doing Interpretive Research. *European Journal of Information Systems*, *15*, 320-330.

Wangpipatwong, S., Chutimaskul, W., & Papasratorn, B. (2008). Understanding Citizen's Continuance Intention to Use e-Government Website: a Composite View of Technology Acceptance Model and Computer Self-Efficacy. *The Electronic Journal of e-Government*, 6. 55-64.

Weber, M. (1947). *The Theory of Social and Economic Organizations.* New York, USA: Free Press Publishers.

Weinstein, N. D. (1993). Testing Four Competing Theories of Health Protective Behaviour. *Journal of Health Psychology*, *12* (4), 324-333.

Wells, J. T. (2011). *Corporate Fraud Handbook: Prevention and Detection.* New Jersey: John Wiley & Sons, Incorporated., *10* (5), 1-400.

West, S. G., Finch, J. F., & Curran, P. J. (1995). *Structural Equation Modeling: Conepts, Issues, and Applications.* Newbery Park, CA: Sage Publications.

Wieser, C., Bruhn, M., Kinzinger, J., Ruckteschler, C., & Heitmann, S. (2019). *The Impact of Mobile Money on Poor Rural Households: Experimental Evidence.* Switzerland: World Bank Group IFC-Mastercard Foundation Partnership for Financial Inclusion.

Wilson, V. (2013). Research Methods: Mixed Methods Research. *Evidence Based Library & Information Practice*, *8* (2), 55-72.

Wimmer, S., Lackner, H. K., Papousek, I., & Paechter. (2018). Goal Orientations and Activation of Approach Versus Avoidance Motivation While Awaiting an Achievement Situation in the Laboratory. *Frontiers in Psychology*, *22* (6), 1-25.

Wohl, R. (1979). *The Generation of 1914.* Cambridge, MA: Harvard University Press.

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *Journal of Certified Public Accountants*, *14* (7), 1-5.

Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *International Conference on Information Systems (ICIS) Proceedings* (p. 31). International Conference on Information Systems (ICIS).

Workman, M. D., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Journal of Computers in Human Behaviour, 24* (6), 2799-2816.

World Bank. (2012). *Information and Communication for Development 2012: Maximizing Mobile.* Washington DC, USA: Retrieved from The World Bank Website.

Wu, J.-H., & Wang, S.-C. (2005). What Drives Mobile Commerce?: An Empirical Evaluation of the Revised Technology Acceptance Model. *Journal of Information and Management, 42* (5), 719-729.

Yasar, K. (2022, August 5). *m-commerce (mobile commerce)*. Retrieved from Techtarget: https://www.techtarget.com/searchmobilecomputing/definition/m-commerce?amp=1

Yeboah, E., Boateng, R., Owusu, A., Afful-Dadzie, E., & Ofori-Amanfo, J. (2020). Assessing the Role of Trust in Merchant Adoption of Mobile Payments in Ghana. In M. Hattingh, M. Matthee, H. Smuts, I. Pappas, Y. Dwivedi, & M. Mantymaki, *Responsible Design, Implementation and Use of Information and Communication Technology* (pp. 204-215). Springer, Cham.

Yin, R. (2003). *Case study research: design and methods.* Thousand Oaks, Cadif: Sage.

Yuan, S., Liu, Y., Yao, R., & Liu, J. (2014). An Investigation of Users' Continuance Intention Towards Mobile Banking in China. *International Journal of Quality and Service Sciences,* 10(3), 279-295. https://doi.org/10.1108/IJQSS-07-2017-0067.

Yu, J., Wang, J., Fang, X., & Huang, F. (2022). Investigation and Analysis of Infection among Impatients in a Tertiary Hospital in Shanghai. *Open Access: Computational and Mathematical Methods in Medicine, 22* (5), 1-10.

Zemke, R., Raines, C., & Filiczak, B. (1999). Generations at Work: Managing the Clash of Veterans, Baby Boomers, Xers, and Nexters in your workplace. *American Management Association.* New York, USA. Sage Publications

Zeng, R., Yuan, Z., & Keller, J. (2003). Model-Based Analysis of Anaerobic Acetate Uptake by a Mixed Culture of Polyphosphate-Accumulating and Glycogen-Accumulating Organisms. *Journal of Biotechnology and Bioengineering, 83* (3), 293-302.

Zhdanoya, M., Repp, J., Rieke, R., Gaber, C., & Hemery, B. (2014). No Smurfs: Revealing Fraud Claims in Mobile Money Transfers. *International Conference on Availability, Reliability and Security (ARES)* (p. 10). Switzerland: ARES Work Press.

Zhou, T., & Liu, Y. (2014). Examining Continuance Usage of Mobile Banking from the Perspective of ECT and Flow. *International Journal of Services, Technology and Management*, 20(4-6), 199-214.

Zikmund, W. G. (2003). *Business Research Methods.* Ohio: Thomson/South-Western Press.

APPENDICES

Appendix A: Publications Published Through the Conceptualisation and Review Phase of the PhD

Publication Type	Full Bibliographic Information
Journal Paper	1. Gyaisey, A. P., & Owusu, A. (2022). Multi-Contextual Analysis of Internet Security Perception and Behavior: Perspectives of Anglophone and Francophone Internet Users. International Journal of Cyber Warfare and Terrorism (IJCWT), 12 (1), 1-20.
Conference Paper	1. Gyasiey, A. P., Boateng, R., Owusu, A., & Afful-Dadzie, A. (2019). Individuals Internet Security Perceptions and Behaviors: Polycontextual Contrast Between Ghana and Nigeria. Twenty-fifth Americas Conference on Information Systems (pp. 1-9). Cancun: AMCIS .

Appendix B: Research Questionnaire

My name is Alfred Paa Gyaisey, a final year PhD candidate in Information Systems at the Business School of the University of Ghana. I am collecting this data to help in my PhD thesis writing. The topic for this study is: **Examining the Effect of Mobile Payment Technology Fraud on Customer Intention on Continuous Usage of the service moderated by Generation X, Y and Z in Ghana.** This study seeks to examine the issue of fraud among users of mobile payment technology commonly referred to as "mobile money". Kindly note that respondent's anonymity and confidentiality of any information is assured, except data collected will be solely used for the purpose for which it was collected. Thank You.

You can contact me via phone: +233243025985 or via email: apaa_gyaisey@st.edu.gh For further information and clarification, you can contact my supervisor, Dr. Acheampong Owusu via email: AOwusu@ug.edu.gh

PART A (Demographic Data)

This part of the questionnaire gathers respondent demographic data. Please tick the box that best applies to you.

1	Gender	Male [ ]	Female [ ]	
2	Age Range	Below 20 [ ] 20 – 29 [ ] 30 – 39 [ ] 40 – 49 [ ] 50 – 59 [ ] 60 and above [ ]		
3	Religion	Muslim [ ]	Christian [ ]	Any Other [ ]

4	Level of Education	Primary [ ] JHS [ ] SHS [ ] Degree/Diploma [ ] Masters/MPhil [ ] PhD [ ]
5	Occupational Status	Student [ ] Self - Employed [ ] Private Sector Worker [ ] Public Sector Worker [ ] Unemployed [ ]
6	Marital Status	Single [ ] Married [ ] Divorced [ ] Widow(er) [ ] Other [ ]
7	Are you registered unto any mobile payment platform? Yes [ ] No [ ]	
8	Do you use any mobile payment system for transactions? Yes [ ] No [ ]	
9	On a scale of 1 – 10, where 1 = Not At All and 10= Extremely Regular, how would you score your usage of mobile payment system ……	
10	Do you own any social media account? Yes [ ] No [ ]	

Part B: Measuring Threat Appraisal and Coping Appraisal

Please indicate your level of agreement or disagreement with each of the following statements.

For each statement below, please circle the number that best describes your view.

Level of agreement or disagreement used for Part B, C and D	**1 = Strongly Disagree** **2 = Disagree** **3 = Neutral** **4 = Agree** **5 = Strongly Agree**

Susceptibility Threat (This refers to mobile payment users' belief on their degree of vulnerability to mobile payment fraud attacks)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1. I believe I am at high risks of getting defrauded through mobile payment fraud	1	2	3	4	5
2. The likelihood that I would be a target of mobile payment fraud attacks is very high	1	2	3	4	5
3. It is extremely likely that I will be a victim of mobile payment fraud	1	2	3	4	5
4. My chances of getting defrauded through mobile payment fraud is very high	1	2	3	4	5
5. The extent of my vulnerability to mobile payment fraud attacks is very high	1	2	3	4	5

Severity Threat (This refers to mobile payment users' belief about the magnitude of potential harm caused by mobile payment attacks)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
6. I believe the consequences of mobile payment fraud for me is very serious	1	2	3	4	5
7. I believe that losing money through mobile payment fraud would be a severe problem.	1	2	3	4	5
8. I believe mobile payment fraud on me would seriously affect me	1	2	3	4	5

9. The consequences of mobile payment fraud on me would be great	1	2	3	4	5
10. The severity of mobile payment fraud attacks for me would be very high	1	2	3	4	5
Self-Efficacy (This refers to mobile payment users' belief in their ability to take protective measures to avoid mobile payment fraud threats)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
11. My knowledge for taking preventive actions against mobile payment fraud is very adequate	1	2	3	4	5
12. My ability to get appropriate advice on how to take protective actions against mobile payment fraud is very high	1	2	3	4	5
13. I am more than capable to handling any possible mobile payment fraud attack	1	2	3	4	5
14. I know exactly what to do when mobile payment fraud attempt is made on me without help from anyone	1	2	3	4	5
15. I am very confident in my ability to deal with any possible mobile payment fraud attempt	1	2	3	4	5
16. For me, taking protective action is very easy	1	2	3	4	5

Perceived Effectiveness (This refers to mobile payment users' belief about whether or not recommended protective measures can effectively protect them against fraud attacks)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
17. The success rate of my protective actions against mobile payment fraud is very high	1	2	3	4	5
18. The chances of stopping fraudulent attacks by taking protective actions is very high	1	2	3	4	5
19. The likelihood to neutralize mobile payment fraud threats is very high	1	2	3	4	5
20. All information on protective measures can effectively stop any mobile payment fraud attack	1	2	3	4	5
21. My knowledge on protective measures will make it easier to deal with mobile payment fraud attacks	1	2	3	4	5

Perceived Security Threat (This refers to mobile payment users' degree of worry/fear about fraud threats. It manifests as security concern.)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
22. My fear of exposure to mobile payment fraud attacks is very high	1	2	3	4	5

23. The extent of my worry about mobile payment attacks is very high	1	2	3	4	5
24. Trouble caused by mobile payment fraud threatens me	1	2	3	4	5
25. I feel it is very risky to use mobile payment system for transactions nowadays	1	2	3	4	5
26. Using mobile payment system for transactions makes me anxious because it is not safe anymore	1	2	3	4	5
27. The extent of my anxiety about potential loss due to mobile payment fraud attacks is very high	1	2	3	4	5

Part C: Measuring Avoidance Behaviour

The following questions describe how you have or would cope with a potentially threatening mobile payment fraud attempt on you. Using the same scale in Part B, kindly circle one which best describes your degree of agreement or disagreement to the following statements.

Avoidance Behaviour (This refers to mobile payment user avoiding the use of mobile payment systems in order to prevent mobile fraud threats)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

28. I have avoided using mobile payment services in order to prevent mobile payment fraud attacks	1	2	3	4	5
29. I have reduced my reliance on mobile payment services in order to prevent mobile payment fraud attacks	1	2	3	4	5
30. I am always on the lookout of any mobile payment fraud attempt to in order to avoid being defrauded	1	2	3	4	5
31. I have been gathering more information on mobile payment fraud strategies in order to avoid possible fraud attacks	1	2	3	4	5
32. I have reduced the frequency with which I use mobile payment services	1	2	3	4	5

Part D: Intention to Continuously Use the Service

The following questions describe whether you would continue to use mobile payment system based on the assessment of your avoidance behavior. Kindly circle one which best describes your degree of agreement or disagreement to the following statements.

Intention on Continuous Usage (This refers to mobile payment users' intention to continuously use mobile payment system)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

33. I intend to continue using mobile payment systems rather than discontinue its use.	1	2	3	4	5
34. My intentions are to continue using mobile payment system than use any alternative means	1	2	3	4	5
35. I have in mind to continue using mobile payment system	1	2	3	4	5
36. In the future, I would not hesitate to use mobile payment system for transactions.	1	2	3	4	5
37. In the future, I will consider mobile payment system to be my first choice when sending money	1	2	3	4	5
38. In the future, I intend to increase my use of mobile payment systems	1	2	3	4	5

Part E: Generation X, Y or Z

Kindly indicate which generation group best suits your age by ticking one of the age ranges provided below. Generation X are people born early 1960s to 1974, Generation Y are people born between the period 1975–1989, and Generation Z are people born from the mid-1990s to the late 2000s.

Generation X	46 – 60 years	[ ]
Generation Y	31 – 45 years	[ ]

Generation Z	30 years – Below [ ]