AN INVESTIGATION OF THE ADEQUACY OF CONTROL MEASURES IN COMBATTING MOBILE MONEY FRAUD IN LUSAKA DISTRICT

BY

NYAMBE GABRIEL MUBITA (721000251)

A DISSERTATION SUBMITTED TO THE UNIVERSITY OF ZAMBIA IN COLLABORATION WITH THE ZIMBABWE OPEN UNIVERSITY IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTERS IN BUSINESS ADMINISTRATION

UNIVERSITY OF ZAMBIA

LUSAKA

2023

DECLARATION

I, **Nyambe Gabriel Mubita** of Student number **721000251** of the University of Zambia in collaboration with the Zimbabwe Open University, and author of this dissertation entitled "An investigation of the adequacy of control measures in combatting mobile money fraud in Lusaka District" do hereby declare that I am the sole author of this dissertation, and that this is an outcome of my own effort and that its contents partly or wholly have never been presented elsewhere. Where other people's work was consulted and/or used, they have been duly acknowledged.

--- --- ---

Name of Candidate Signature Date

Certified by:

Prof. William Abwino Phiri – PhD --- ---

Supervisor Signature Date

COPYRIGHT

DEDICATION

I wish to dedicate this work to the almighty God for the strength, knowledge and for the grace of wisdom he has given me this far. It is also important for me to dedicate this work to my dear wife Thandiwe Mkandawire Mubita for her support and encouragement rendered to me during the study period leading to the success of this work.

ABSTRACT

The purpose of the study was to investigate the adequacy of control measures in combatting mobile money fraud in Lusaka District.

The three specific objectives of the study were (1) to determine the types of control measures employed in combatting mobile money fraud in Lusaka District (2) to establish the extent of implementing control measures of combatting mobile money fraud in Lusaka District and (3) to establish policy best practices in combating mobile money fraud in Lusaka District.

The study drew a sample size of 271 using mixed sampling methods of purposive and simple random. The study adopted a convergent parallel mixed research design and data was collected using a structured questionnaire and an interview guide. Data obtained were analysed using correlation and multivariate regression analysis with the help of SPSS (Version 27). In addition, content and thematic analysis was used to derive meanings from the qualitative data. The findings of the study were: the types of the control measures in the fight against mobile money fraud include sensitization of both the users and the agents, apprehension and prosecution of the offenders, enhancement of mobile money security through the adoption of appropriate technologies among others. It was also found that majority (145; 54%, N=271) of the users do not even implement the control measures that are recommended for them. On the issue of policies and laws, most of the respondents were not aware about them, and could therefore, not comment much on their efficacy. A Cronbach alpha test was carried out to test the reliability of the research outcomes for internal consistency. The Cronbach alpha produced a reliable measure of .744 which is a moderate indicator and the standardized items of 0.757. One of the recommendation of the study is that the various stake holder organizations such as ZICTA, MNOs and Law Enforcement Agencies should intensify their sensitisation programs and even conduct joint campaigns on how the users of mobile money services could protect themselves from the fraudsters.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my Research Supervisor **Professor William Abwino Phiri** for the great support rendered to me during this study. His passion for research, patience, motivation and good guidance during the study provided an umbrella for all the support I needed to succeed in this work. In addition, the Course Co-ordinator-Mr. Kingsley Namangala, the various Lecturers and staff at UNZA-IDE who played their part during my study for Masters of Business Administration, are also hereby acknowledged. It is also important to show gratitude to my intake mates in the MBA study program who also offered me their support in their own way during the whole study period.

TABLE OF CONTENTS

LIST OF ABBRVIATIONS

ZICTA	Zambia Information Communications Authority
MNO	Mobile Network Operator
SPSS	Social Package for Social Sciences

LISTS OF FIGURE

LIST OF TABLES

CHAPTER I

INTRODUCTION

1.0 Overview

This chapter presented the background of the study, statement of the problem, purpose of the study and the research objectives. This was followed by the research questions, the significance, and scope of the study. In addition, it also presented the limitations as well as the ethical considerations of the study, and the theoretical framework, while the definition of key terms was the last part of the chapter.

1.1 Background to the Study

The development of connectivity through telecommunications has changed the lifestyle of many people in the World. Over the years, the use of mobile handsets has had a tremendous impact on our very existence. In many countries world over, one can do anything from having a virtual medical appointment with a doctor, undertaking all forms of commerce and virtually everything that one can imagine through the use of mobile handsets. As such, one important innovation brought about by mobile handsets is the ability to perform financial transactions using mobile devices. For example, in China, WeChat and Alipay are important applications that can be used to undertake quite a number of financial transactions using a mobile phone (Botchey et. al, 2020).

The advancement in technology in the world has brought on board many interventions that have benefitted the livelihoods of many people particularly in countries like Zambia. One major area where technology has impacted the lives of people is the mobile money services, which have led to financial inclusion of people who were not associated with conventional banking systems such as commercial banks. Many people especially in rural and high density areas had difficulties in engaging in conventional banking due to the requirements put in place to access banking services (Kabala et.at, 2021; Okello et.al, 2020). Over the years, Zambia has seen an improvement in the unbanked population from 40.7% in 2015 to 30.6% in 2020 (BOZ, 2020:15).

Mobile money was introduced in Africa in 2007 with the launch of the M-PESA (M for mobile, PESA for money in Swahili) service by Safaricom and Vodafone in Kenya. M-

PESA was started as a public/private sector initiative after the United Kingdom (UK) based Telephone Company Vodafone won funds from the Financial Deepening Challenge Fund competition established by the UK Government's Department for International Development to encourage private sector companies to engage in innovative projects so as to deepen the provision of financial services in emerging economies. "Originally, M-PESA was designed as a system to allow microfinance-loan repayments to be made by phone, reducing the costs associated with handling cash. After the pilot testing, it was broadened to become a general money-transfer scheme. The service then quickly gained popularity, initially with urban populations as a mean of sending money to family members in remote and underserved rural areas. Once the ability to buy airtime using M-PESA was introduced, the transaction volume increased rapidly as well as the adoption of the service by all population demographics" (Interpol, 2020:6).

Over the years, there has been an increase in the number of people that are using mobile money banking services. "According to the 2022 GSMA Mobile Money Industry Report, there were over 1.35 billion registered mobile money accounts by the end of 2021 reflecting an increase of 18 percent since 2020 and 10 times more than there were in 2012" (ZICTA, 2022:4). As of 2022, globally, there were 1.6 billion registered mobile money accounts, indicating, a growth rate of 13% from 2021 and Africa accounted for 781 million of those. The major growth rate in Africa occurred in sub-Saharan Africa, which experienced 763 million accounts in registered mobile money accounts. On the other hand, in 2022, Southern Africa had a total of 65 million registered mobile money accounts. As regards Zambia, the total number of active mobile money subscriptions in the country increased from 9.8 million in 2021 to 11.2 million subscribers in 2022 representing a growth rate of 13.98 percent (ZICTA, 2023: 7). These statistics indicate that indeed the usage of mobile money has been increasing globally, at the African level, in Southern African and indeed at Zambian level and this trend is expected to continue over time.

The volume of the mobile money transactions as of 2022 was 65 billion per year and the value of transactions, grew by 22% between 2021 and 2022, from $1 trillion to around $1.26 trillion respectively, indicating a value of $3.45 billion transactions on a daily in 2022 globally. In Africa, the volume of the transactions was 44.9 billion, resulting in the value of $836.5 billion. As for Southern Africa, the volume of the transactions in 2022 was 3.7 billion resulting in the transaction value of $57.6 billion (GMSA, 2023: 10). Zambia has also experienced a significant increase in the volume of mobile money transactions

from 834 million transactions at the end of 2021 to 1,581 million transactions at the end of 2022 reflecting an improvement of 89.60 percent. This resulted in the increase of the transactions value from ZMW 169.4 billion recorded at the end of 2021 to ZMW 295.8 billion at the end of 2022 reflecting an increase of 74.63 percent (ZICTA, 2023: 7).

The major transaction methods are person to person and through facilitation by the mobile money agents. These agents play a very important role as intermediaries in the mobile money business. Apart from their core business of facilitating transactions, they are responsible for onboarding and educating hundreds of millions of customers. In 2022, the number of registered agents was 17.4 million, of which 7.2 million were active globally. In 2022, mobile money agents in the world were responsible for digitizing $294 million thereby leading to an increase by 17% from 2021. On the other hand, in 2022, Zambia's record of registered and active Mobile Money Agents grew by 59% to 247,665 from 2021, of these, 38% of them were active at end of 2022 (BOZ, 2023:19). From the foregoing, it is worth to note that this trend is expected to continue over a period of time.

The notable increase in mobile money transactions has been necessitated by the increase in the number of people owning and using mobile phones. According to the ITU (2023), 73% of the world population aged 10 years and above are subscribed to a cell phone network by a owning a cell phone indicating 7.33 billion users. In sub-Saharan Africa, the number of mobile phone subscribers as measured per 100 people was 84 in 2021. At the rate that the world is progressing, it is headed towards a cashless society. This is because many people are now using mobile phones to conduct transactions, thereby increasing financial inclusion levels among the unbanked.

In Zambia, for many years, banking services were more prevalent in urban areas where commercial banks and other financial institutions had presence. However, with the introduction of mobile phones and mobile money services, people in rural areas are now able to access banking services. In relation to this, according to ZICTA (2021: 16), "the number of active mobile network subscriptions was expected to increase from 20.3 million reported at the end of 2021 to 20.9 million subscriptions at the end of 2022 and subsequently 21.2 million in 2023". The increase in mobile subscribers has so far led to an increase in the users of mobile money too and this is expected to increase over time.

Mobile money fraud has been a major problem facing the mobile money business in the world. As the mobile money industry grows, it faces greater risks relating to mobile money

fraud as many users keep falling prey to mobile money fraud scams. In 2020, nearly $4 billion was lost to fraudulent mobile money activity and scams, a figure that is expected to grow over time as fraudsters adopt increasingly sophisticated methods. For instance, in Uganda, the country lost about U$ 3.2 million mobile money in 2020, where criminals used over 2,000 SIM cards in perpetuating the crime (Cambridge Intelligence, 2023).

The most common types of mobile money fraud include sim swaps from the customer's SIM to that of the fraudster, enabling the fraudster to gain access to the consumer's mobile account. In addition, false promotions, phishing, or social engineering scams, such as fraudsters impersonating providers and advising customers they won a prize in a promotion and to send money to the fraudster's number to claim the prize are among the major types. Some Agents are also involved in theft by asking for the customer's personal identification number (PIN), thereby making consumers more vulnerable. In recent times, provider impersonation by fraudsters who call consumers purporting to represent the provider has become common. These induce them to reveal their PIN or other personal information about their mobile money accounts, which can be used to defraud the customer. On the other hand, Agents have also been victims of fraud mainly involving float loss in the agent's account arising from unauthorized use, compromising of PINs, and scams involving impersonation of Mobile Network Operators staff by fraudsters who gain unauthorized access to the agent's float account. Fraud within providers is also a concern. Internal fraud involving employees of the MONs is also quite rampant and puts users' accounts at risk and raising financial integrity concerns for the system (CGAP, 2017).

The increase in mobile money fraud has been attributed to several reasons that include, inadequate internal controls (facilitating internal data hacking), inadequate audit processes, poor corporate governance structures, lack of employee fraud education, and lack of whistle blowing mechanisms. In addition, poor or lack of public awareness on how consumers can protect themselves from fraud criminals is also an issue of concern. Further, there is also lack of information on where consumers can lodge their complaints about fraud related issues. In many cases, the MNOs and government agencies lack automated fraud management systems that can help to monitor, screen and detect fraud. The levels of literacy among the consumers especially in remote areas make it difficult for them to fully understand the ways through which they can protect themselves (CGAP, 2017). These are among the many reasons that have made it possible for the criminals to take advantage of the vulnerabilities found in the mobile money business and defraud the unsuspecting users.

Many MNOs and relevant government agencies around the world have tried to devise measures that aim at preventing and combatting the scourge of mobile money fraud. This is despite the scourge being on the increasing trajectory. Zambia is one of the countries that has experienced an increase in the number of mobile money users in the recent past. As the number of mobile money users has been increasing over the years, the necessity to devise appropriate measures to secure the mobile money platforms as well as to protect the users from the fraudsters, has become inevitable in Zambia. The attractiveness of mobile money and the increase in its users has also led to an increase in mobile money fraudsters, thereby posing a great threat to this key innovation that is meant to benefit many people in a country like Zambia through financial inclusion particularly among the unbanked population that especially live in the rural areas.

Mobile money fraud is part of the main stream cybercrime where criminals use computer systems and mobile phones to commit crimes. In order to combat this trend, the Zambian government has enacted some key legislations and policies that include the Cyber Security and Cyber Crimes Act, No.2 of 2021 which provides for cyber security including protecting persons and Critical Information Infrastructure against cybercrime in general. It also enacted the Electronic Communications and Transactions Act No.4 of 2021 which seeks to provide a safe and effective environment for electronic transactions. In addition, there is also the Data Protection Act No. 3 of 2021 which seeks to provide an effective system of protection and regulation of personal data, and the National Cyber Security Policy of 2021 whose major objective is to create a safer cyberspace in Zambia (National Assembly of Zambia, 2022).

It is worth to note that just like in other countries, Zambia has put in place certain measures both at MNO level and government agency level to prevent mobile money fraud as well as combatting it. Despite these measures, the country has continued to experience cases of mobile money fraud, hence the need to examine such measures in combatting the scourge.

1.2 Statement of the problem

The mobile money services are supposed to lead to an increase in the levels of financial inclusion in Zambia and improve the business activities and the general livelihood of the citizenry. For instance, instead of physically going to the bank to withdraw money to pay someone or indeed for the goods and services, which could be both risky and costly, mobile money services can be conducted from the comfort of one's location. This is a less risky

and cost-effective way of transacting in the modern world. It is also a platform that many stakeholders such as government and the private sector can use when making payments such as the social cash transfer, pension benefits and loan disbursements to members of the public, especially those in rural areas who do not have access to conventional banking services.

According to the Zambia Information Communication Technology Authority (ZICTA) (2022), there were K50.4 billion worth of mobile money transactions entailing 277 million volume of individual transactions from January to July, 2022. Mobile money usage is expected to increase as the mobile service providers continue to expand their network coverage to rural areas and the people adopt mobile money as a form of banking. It is expected that mobile money services are supposed to be less risky as compared to the traditional methods of financial services. However, there has been an increase in mobile money fraud related incidents in the country.

The Zambian government through the enactment of various legislations and formulation of policies, ZICTA as the sector Regulator, and the mobile money service providers such as Airtel, MTN and Zamtel, have all taken measures to protect the public from mobile money fraud. It is therefore, expected that with such measures at hand, the levels of mobile money fraud should be reducing in the country. However, despite taking such control measures, in 2021, ZICTA received a total of 29,523 complaints from members of the public on issues related to cybercrime. Of these cases, 45.21% were involving mobile money scams (ZICTA, 2021: 49). It was therefore very important to investigate the adequacy of control measures employed to combat mobile money fraud and thereby protecting the public.

1.3 **Purpose of the study**

This study was carried out in order to investigate the adequacy of control measures put in place by the various stake holders and being implemented by them to control mobile money fraud among the residents of Lusaka.

1.4 **Research Objectives**

- To determine the types of control measures employed in combatting mobile money fraud in Lusaka District.

- To establish the extent of implementing control measures of combatting mobile money fraud in Lusaka District.
- To establish policy best practices in combating mobile money fraud in Lusaka District.

1.5 Research Questions

- What types of control measures are employed in combatting mobile money fraud in Lusaka District?
- To what extent are the control measures of combatting mobile money fraud implemented in Lusaka District?
- What are policy best practices in combating mobile money fraud in Lusaka District?

1.6 Significance of the study

This study may help the authorities to ascertain the effectiveness of the control measures that they have put in place to control mobile money fraud. As such, it may help to enhance the existing policies as regards combatting mobile money fraud in Zambia. In general, cybercrime is a world problem which requires concerted international efforts to fight it, as such, this study may help in devising the best practices that can be adopted in combatting this vice. The public may also benefit from the study in that ultimately, the recommendations may help them to protect their transactions from criminals when implemented. In addition, the study may add to the body of knowledge in Zambia, where not much research has been undertaken on the subject. It is also important to conduct the research within the course of the year in order to reduce the occurrences of mobile fraud among the members of the general public.

1.7 Scope of the study

This study covered the geographical boundaries of Lusaka District and was conducted among two hundred and seventy-one (271) participants. In this study, each participant was asked a set of questions through the in-depth interview guide and a self-administered questionnaire. The study was conducted within a period two (2) months in the first quarter of the year 2024 and focused on the control measures meant to combat mobile money fraud.

1.8 Limitations of the Study

The sample size of 271 participants which was drawn because of time and budget constraints, may not have been a good measure against the population of the area, which is estimated to be above 20,000. However, in order to mitigate this, most of the sample was drawn randomly so as to ensure the representativeness of the sample to the population. The study findings represent a picture of what is obtaining in Lusaka District, therefore, generalizing them to other areas would need to be taken with caution.

1.9 Theoretical Framework

This study was guided by the Prevention Motivation Theory (PMT). This theory was developed by Rogers, 1975 and further revised in 1983 (Rodgers 1975; 1983) and was premised on explaining the impact of persuasive communication on behaviour. Its major emphasis is on cognitive mechanisms underpinning the rationale to follow or not to follow a recommended behavior. Although the theory was originally conceptualized to explain phenomena in the healthcare context by explaining human protective behaviour as regards health care provision, it can be used in many disciplines as the case was with the study at hand (Conner & Norman, 2015).

The theory explains the tendency of people to adhere to measures put in place to protect themselves against danger and posits the following: The belief that the adaptive response will work, that taking the protective action will be effective in protecting the self or others; The perceived ability of the person to actually carry out the adaptive response; The costs associated with taking the adaptive coping response (Floyd, Prentice-Dunn & Rogers, 2000). It also considers Perceived Threat Severity, that is how serious the individual believes that the threat would be to him or herself and how personally susceptible an individual feels to the communicated threat (Milne, Sheeran & Orbell, 2000). Further, it considers a purposeful choice of a danger-control response to a fear appeal and choosing a behavior that protects against the danger (Boss et al., 2015).

1.10 Definition of key terms

Control measures: This is simply any activity or programme that has been put in place by the Government, ZICTA, the Mobile Network Operators and individuals to protect the users against mobile money fraudsters.

Mobile money: This refers to financial transactions and services that can be carried out over the telecommunication network using a mobile device such as a cell phone or a tablet.

Fraud: Fraud occurs when an individual deceives another by inducing them to do something or not do something that results in a financial loss. In this study, it means all the mobile money scams that fraudsters engage in in order to steal money from users of mobile money platform.

1.11 Summary

This Chapter looked at the background of this study where it discussed the innovations that have taken place in the telecommunications industry resulting in not only the use of phones for communication, but also to perform financial transactions called mobile money. The ability to perform financial transactions over the phone has created a problem where fraud has emerged using the same mobile phone platforms. The Chapter also looked at the statement of the problem, where it was presented that despite the measures put in place, cases of mobile money fraud had continued to rise with ZICTA reporting 29,523 complaints from members of the public on issues related to cybercrime, of which 45.21% were involving mobile money scams (ZICTA, 2021: 49).

The Chapter also looked at the purpose of the study which is simply to investigate the adequacy of the control measures in combatting mobile money fraud. It further looked at the three research objectives that include to determine the types of control measures, to establish the extent of implementing control measures, and to establish policy best practices in combating mobile money fraud in Lusaka District. The main theory adapted for the study was the Prevention Motivation Theory (PMT). This theory was developed by Rogers, 1975 and further revised in 1983 (Rodgers 1975; 1983) and was premised on explaining the impact of persuasive communication on behaviour. Its major emphasis is on cognitive mechanisms underpinning the rationale to follow or not to follow a recommended behavior.

CHAPTER II

LITERATURE REVIEW

2.0 Overview

This chapter critically reviewed relevant literature on the subject of cybercrime in general and mobile money fraud in particular, derived from themes that were based on the research objectives. It must however, be stated that since the phenomenon of cybercrime is relatively a new topic, which has been necessitated by the advancement in technology in the world that has mainly occurred in the last few decades, there is an information gap on the subject. The logical approach was the model used to conduct the critical review of literature and it took take a global, regional and local approach.

2.1 Empirical studies

There are not so many empirical studies on the control of mobile money fraud in the world, as most of them focus on how mobile money contributes to financial inclusion and factors that determine its usage, especially among the unbanked population. This situation has been exacerbated by the fact that the phenomenon of mobile money in its strictest sense, meaning the use of a mobile phone to conduct a financial transaction, has been more prevalent in the developing world, particularly in Africa than the developed one. In the developed world, the most prevalent payment methods over the years have been credit and debit cards, which also help to facilitate electronic payments. It is therefore worth to note that in the developed world, where they have better record keeping abilities, most studies have been focusing on credit, debit cards and internet banking fraud.

Just like crimes such as fraud, cybercrime and money laundering are global issues in nature, mobile money fraud is equally in the same category, and as such, all require concerted efforts from shareholders at a world level to combat them. This is because there is a global threat of criminals using mobile money to engage in money laundering and terrorist financing due to the billions of transactions in US dollar value that pass through the mobile money payment platform, The African continent is the “world leader” in the mobile money industry, accounting for nearly half of all registered mobile money accounts globally (Interpol, 2020).

As indicated already above, mobile money is a phenomenon of the developing world, particularly Africa, as such, there is scarcity of study literature in the developed world bordering on the topic and its related issues. However, a few studies on the topic are worthy noting from across the globe.

2.1.1 Literature review: World perspective

In a study by Iyer (2017), dubbed "a case study on monetary fraud in a cashless economy", Sweden, United States and India were surveyed. The study found that the policies, tools and techniques to detect and mitigate fraud in the digital spectrum such as mobile money are insufficient and struggling to catch up with the rapid technological advancement made in the field, making it difficult to check for fraud that occurs across channels.

The above study is relevant to the proposed one in that both are delving into digital or electronic payments, of which mobile money is just a subset, as in both cases, transactions are done cashless and over the air. However, this study creates a gap in research in that its major focus was on credit card fraud. In addition, studying three countries out of the many can not generalise such findings to include Zambia, which is in a different continent with different socioeconomic characteristics.

Mudiri (2021: 8-12) placed mobile fraud into various key categories and provided examples of how mobile money fraud is perpetuated in each category as follows:

"MOBILE FINANCIAL SERVICE PROVIDER FRAUD; This is a range of fraudulent activities perpetrated by the mobile financial service providers' employees. The fraudulent activities will be carried without authorisation of the business. The key types of fraud in this area include fraud on the mobile money operator, mobile money operators' employees defrauding agents, businesses and consumers. Fraud in the ecosystem is less prevalent at the beginning of the deployment and becomes common during the customer activation and value stages of the deployment. At this stage, substantial electronic money has been invested in the system and it therefore becomes attractive to fraudsters. Examples of the most common types of fraud include the following;

Corruption within the mobile money business; John is a teacher and is looking an avenue to invest in his spare financial resources. He has recently been told that

operating an agency business for a leading mobile financial service provider is lucrative. He decides to try his hand at it and submits the relevant application / documentation. He receives a call advising him that for his business to be given rights to operate the outlet some payment is required as a ―facilitation fee‖. If the bribe is not given, the outlet will not be approved.

Mobile operators' employees stealing funds from the business; Baku is a leading master agent with 30 outlets and has transacted mobile financial services for over 3 years. Baku is declared insolvent and the business has to undergo liquidation process through the court of law. Baku's mobile money account is frozen pending completion of administration process. Access to the account by the original owners of Baku is cancelled and they can neither view nor transact the account. The liquidation process takes 5 years to finalise, during which the account is largely forgotten. An employee of the mobile money operator with super-user rights accesses the account and over time transfers funds to himself. By the time the liquidation process is finalised the account has no funds.

Collusion between fraudulent mobile money employees and other fraudsters to carry out unauthorised SIM swaps; Jackie is seated in her grocery shop. She decides to make a call to her husband who works in another city. She tries to make her call but is unable to connect. ―Another network issue‖ she mutters and stops trying. She attributes the failure to poor network and continues with her work. Suddenly her neighbour appears extending her phone to Jackie. ―It is your husband‖, she says. She informs her that her husband has been unable to reach her all morning. Jackie realises that she has a problem with her line. When she contacts the mobile operator's call centre using her friend's handset, she is informed that her line has been swapped … and soon discovers that her mobile money balance has been withdrawn.

Unauthorised access of financial records for personal gain; Paul and Michelle are going through a divorce process. Paul suspects that Michelle has more money in her mobile money account than she has declared. He seeks out a customer care employee who agrees to share details at a fee. He pays and he is given the account balance. ν Unauthorised transfer of funds from customers' accounts John has been depositing funds in his account and transacting quite frequently. He grows suspicious one day when he checks his balance and realises that what he deposited the previous day is

missing. He decides to check at the nearest operators' shop and finds that funds have disappeared from his account. He requests for his statement and realises that a withdrawal of which he has no record or recollection has been made from his account. He lodges a complaint with the mobile money operator specifying that funds have been transferred from his account without his consent. The mobile service provider investigates the transaction and finds that one of the employees accessed the account and transferred funds from John's account into his own personal account. The employee is unable to provide a justification for this action and his service is duly terminated.

SYSTEM RELATED FRAUD**;** System related fraud covers all fraud activities that affect the mobile money deployment through system weaknesses and processes. System related fraud will cut across different stakeholders including agents, businesses, and mobile money operators. System related fraud is highest when a platform has inadequate controls to guide in transaction processing. This fraud is prevalent during transaction activation stage of the deployment and continues to grow into the value addition stage. The key occurrences of fraud include:

Password/PIN sharing; Chantal runs an agent outlet with two employees. Each employee is required to apply for his/her own PIN in order to transact the mobile money business. However, Chantal encourages employees to use the same PIN. Even when employees are terminated from employment, the same PIN is used by newly recruited employees. One day, Mark, one of the employees takes the day off work. He however, passes by the business to check on something and finding the handset lying on the counter, transfers money to a fraudulently registered number. The money is withdrawn at an ATM location. It is very hard to pin the blame on Mark since he should have been off duty on that day.

Weak password and transaction PIN strength; Michi transacts a lot on his mobile banking account. He finds it convenient to do so. His son, Daudi gambles a lot and needs money to feed his habit. Daudi knows his father's year of birth. He has on a previous occasion been instructed by his father to unlock his phone using the year of birth as his PIN. Daudi guesses, correctly, that his father's mobile money PIN is his year of birth. He tries it and is able to send money to himself which he subsequently withdraws.

Creation of fake and non-existent users on the mobile financial services platform; John works for a third party vendor contracted by a leading financial institution. He has been given administrator rights in order to facilitate integration between the mobile money platform and the financial institution. He creates two unauthorised users with rights to initiate and verify transactions, and transfers funds from the organisation to his associates' wallets, effectively stealing money from the financial institution

Individual users with multiple rights; Jim is the Money Transfer Manager with a leading master agent owner. The owner, to save costs, decides not to hire additional staff. He creates himself and Jim as the only persons authorised to transact the main mobile money account. Being a busy man, the owner entrusts his password with Jim, allowing him to act as initiator and verifier on the account. Jim uses this access to transfer funds fraudulently to his friends.

Fraud on multiple access channels; At some point in the business, a leading master agent lost his computer and had to temporarily transact from a computer located inside a cyber café. Subsequently, in an unrelated event, he fires two of his employees Navaro & Sadiki. Even though he now has a new computer he forgets to disable the secure certificate in the cyber café. Navaro & Sadiki being aware, use their access to illegally transact from the cyber café".

The above categories by Mudiri (2021) shows the various types of mobile money fraud and the ways in which they are perpetuated by the criminal elements. This is very relevant to the study at hand. However, the article does not provide solutions of how the scourge of mobile money fraud could be controlled.

Volodymyr et.al, (2022) studied the operational risk management of using electronic and mobile money in Ukraine and they found five key types of risks associated with the use of mobile money, that include information/cyber security risk, information risk, risk of errors in management processes, risk of user errors and risk of errors in managing the network of agents. To the researchers, these are responsible in creating vulnerabilities in the usage of mobile money. To them, addressing these risks can help to reduce operational risks, thereby ultimately making mobile money safe.

This study is relevant to the proposed one, in that it brings out the major issues that are associated with mobile money fraud and recommends measures on how to resolve

them. However, it presents some gaps that need to be filled. For instance, the methodology that was used simply analysed data for Ukrainian banks with electronic money in 2014–2021. This left out key stakeholders such as the regulators, mobile money operators, the mobile money agents and the public. Therefore, this limits the findings to the situation in Ukraine and cannot be generalised to Zambia.

Uddin et.al (2022) studied the effects of fraud call on mobile banking transactions in Bangladesh. The major focus of this study was the calls that fraudsters make to unsuspecting users of mobile money services, where they inform them that they had wrongly deposited money into their mobile money account, when in fact not, hence asking them to send it back to them. At this point, users would be prompted to send the money to them without conducting due diligence on the transaction to ascertain whether or not such money was sent to them.

This study is very relevant to the topic at hand as it brings out one of the major ways in which mobile money fraud is conducted by the criminals. However, notwithstanding the above, the study has some limitations in that it was conducted in a different geographical area (Bangladesh), which may have different characteristics to Zambia. In addition, its focus is mainly only on one type of mobile fraud (fraud calls), and it did not recommend solutions on how such a fraud could be abetted. Furthermore, the selection of the sample was purely voluntary based which raises questions on validity on objectivity and representativeness as the volunteers may not have been the best group to be studied on as they were drawn using the convenience approach.

"Since the early days of the Internet, online scammers have been using social engineering techniques to scam individuals and organizations; a notable example is the Nigerian advance fee scam (Nigerian Scam, 2020). Social engineering is defined as "The Science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity." (Francois et.al, 2014). To persuade (or manipulate) individuals, attackers use techniques that exploit human cognitive biases (tom, et.al, 2007). Depending on the underlying technique, social engineering can be classified into five categories: i) Social Engineering via telephone communication, which is characteristic of smishing and vishing; ii) Dumpster diving (i.e., office or electronic waste); iii) Online social

engineering (i.e., on the web through browsing); iv) Persuasion (face to face communication), and; v) Reverse Social engineering (Jonny, 2011). Even though social engineering attacks vary, they follow a common pattern consisting of four phases: i) Gather information about the target; ii) Build rapport with the target; iii) Exploit the available information and execute the attack and; iv) Exit leaving no evidence (Francois, et. al, 2016). The availability of affordable mobile phones has provided access to the majority of the previously hard-to-reach populations (Meeker, 2019). This increasing number of mobile users with varying socioeconomic, literacy, and language barriers is vulnerable to privacy and security attacks as the technology usage, information utilization, and sharing practices of the population living in the Global South are notably different from those in the Global North. There have been many efforts to understand and mitigate these threats including password construction (Chiasson, at.al, 2011), deducing preference by social network behaviour (Chiasson, et.al, 2011) studying privacy on mobile devices (Roundy, et.al, 2009) and helping privacy through design (Chiasson, et. al, 2011). However, these studies focused primarily on Western privacy concepts that do not encapsulate the privacy practices in developing regions. There is a need to study the privacy and security practices in the Global South, understand the technology usage differences and resulting unique security and privacy implications, and address those unique challenges (Nissenbaum, 2004, Vashistha, 2018). Some previous works in developing countries have attempted to highlight the unique security and privacy challenges. For example, Ahmed, et. al, 2016) provide a holistic local interpretation of privacy threats users face at mobile repair shops in Bangladesh; their work re-validates Nissenbaum's notion of privacy as contextual integrity (Nissenbaum, 2004). They highlight mobile phone users' lack of awareness regarding the loss of privacy in the repair process and suggest designing solutions for preserving privacy in repair by leveraging the cultural and religious values of society (Sambasivan, 2019). To that end, (Srinivasan, 2018) explored the interactions and privacy perceptions of users with identity infrastructures in the Global South. Another study (Ahmed, et.al, 2019) noted that broad conceptualization of privacy influences the design of devices used in the Global South context but their privacy features only tend to work in stable environments (e.g., stable democracies). So privacy not only needs to be studied in different social and cultural contexts but also in a diverse political environments and settings. Proc. ACM Hum.-Comput. Interact. Vol. 5, No. CSCW1, Article 41. Publication date: April 2021. 41:6 Lubna

Razaq et al. Besides differences of perceptions around security and privacy between the developed world and the Global South, gender also impacts the semantics of security (Hanul, 2012) as women tend to have a stronger perception about security of a particular method than men (Schymik, 2018). Apart from gender, prior works suggest that individuals from low socioeconomic status have differing privacy norms, and variations in socioeconomic status are associated with differences in users' security and privacy beliefs and behaviors (Micheli, 2016). We continue this line of work to understand and describe user perception and understanding of security and privacy in the Global South. Engaging with diverse users, we identify the various actors at play in the life cycle of mobile-based frauds in the Global South and map their experiences on this life cycle. Mobile Fraud; the chances of users falling prey to mobile fraud is increasing with the growing number of mobile phone users in the Global South (GSM intelligence, 2019). Growing number of transactions on mobile devices, as compared to desktops, makes mobile users an attractive target for fraudsters. According to a recent industry report, mobile users have lost millions of USD to mobile frauds (Choi, 2017). Mobile fraud attempts grew 50% in 2018 and one common type of fraud is account takeover wherein fraudsters trick users into giving sensitive account details like PIN. Other techniques (or attacks) that fraudsters use include malware, fake mobile app, smishing, vishing, Man-In-The-Middle (MITM) attacks, SIM cloning, using Thin SIMs, and SMS spoofing (Rowan, et.al, 2018). Bowers et al. performed a comprehensive security analysis of emerging digital credit applications to identify security and privacy issues (Bowers, 2019). Phipps et al. showed the vulnerabilities in SIM cards by employing a mock attack using thin SIMs on SIM-based mobile money systems, which reliant on SMSes (Rowan, et.al, 2018). Although mobile fraud attacks happen online, they highlight how our online and offline worlds are interconnected. Offline trust such as trust in social institutions and individuals is coupled with online trust (Gustavo, 2012). From a security point of view, physical and digital space are also interrelated (Dimkov, 2012), and it is this trust that fraudster exploit in their scams. Therefore, it is significant to study users' reactions offline to understand online threats. Information required to commit crimes such as phishing and identity theft usually comes from phone conversations with the victims (10.5%). This suggests that in identity theft and fraud incidents, information was given voluntarily by the victims and was provided during direct contact instead of online contact (Ross, 2011)".

In another study that was conducted in India by Somasundaram (2020), that was analyzing perception of consumers towards digital payment, it was found that there is need to strengthen mobile money payment systems in order to improve safety and security of the financial transactions of consumers. In addition, it recommended that digital payment systems should minimize risk associated with transactions of consumers and must adopt appropriate measures to overcome undue delay in its processes.

The relevance of this study to the one at hand was visible in that both sought to address the element of safety and security of the transactions that are conducted via mobile money platforms. However, the jurisdiction of the study makes it difficult to extend its findings to a country such as Zambia. In addition, its sample size of 95 was way too low to generalize the findings to millions of mobile money users in India and later on to Zambia.

2.2.2 Literature review: Regional perspective

At the African level some of the notable studies conducted include that done by Interpol (2020), on mobile money and organized crime in Africa. This study adopted intelligence analysis methodology, which included open sources and reports from various international organizations and Interpol member countries. This study found that weaknesses in regulations and user identification systems, lack of consumer awareness, coupled with a lack of experience and resources in law enforcement made criminals to exploit the mobile money platforms for fraud. In addition, it found that criminal exploitation of mobile money perpetuates a range of crimes such as fraud, money laundering, extortion, human trafficking, the illegal wildlife trade, firearms trade, the drugs trade, stolen motor vehicle trade and terrorism. It recommended stronger partnerships amongst all law enforcement agencies, greater awareness of the overall issue at a regional level and identification of best practice responses from the member states.

The study by Interpol was very important in this discourse in that it represented the role of the law enforcement agencies as well as national governments in combatting mobile money fraud. Its findings and recommendations were important to the scope of this study. Notwithstanding the relevance, the major gap in this study was premised on the fact that it only analyzed information on crimes from Interpol member countries. There

was no actual study conducted especially qualitatively to understand the mobile money fraud phenomenon. Therefore there was need to undertake a study like the one at hand in order to qualitatively understand the Zambian scenario particularly narrowing down to the research site.

Peacock (2022: 4), argues that "It can also be argued that, as mobile money transfers are done mostly from the cities to the countryside, where most people do not have a bank account but a mobile phone is easily accessible, this could be a contributing factor for the major use of mobile money for transfer purposes. As one of the major causes of consumer driven fraud is PIN sharing, it can be seen from this research that this is not a very common practice. However, the 9% that shared their PINs did so with their relations and sometimes with customer agents to help them in transacting one service or the other from their mobile money. It can be seen from this that, PIN sharing could be done based on trust, and if any fraud should be perpetuated through acquiring of the users' PIN, the person carrying out the fraud must first try to win the trust of the user, either by pretending to be a part of the service provider or a relative who is trying to offer a help. To avert this however, the researchers believe that the MNOs must alert users to first verify from them the authenticity of any suspected request before giving out any information that could make them vulnerable to fraud. Despite users' awareness of their security measures they can take to prevent fraud, the service provider has a major task in securing the mobile money service, since as much as 13% believe the security of the service solely depends on the service provider. The researchers believe this category of users will invariably not put any blame on themselves if any fraud happens, since they believe total protection of the service depends on the service provider. It has also been found that even though there are several services available, such as pay bill and top up airtime, on the mobile money that users can take advantage of, the general usage of these other services are few. The researchers believe this could be as a result of the complex nature of using these services. The general perception that there is no direct linkage between mobile phone protection and mobile money protection could be attributed to the fact that users believe the service provider has put in place adequate measures to protect the mobile money service".

A study by Akomea-Frimpong, et.al (2019) sought to explore the main causes of fraud in the mobile money services in Ghana and the measures that were undertaken to

combat the scourge by the key stakeholders connected to the mobile money services. Their major findings were that mobile money services fraud is caused by weak internal controls and systems, lack of sophisticated tools among law enforcement to detect and combat the scourge. It was also found that there was inadequate education and training among the mobile money agents and the subscribers.

The above-mentioned study was very relevant to the study at hand as it provided insights into measures that are put in place to control mobile money fraud. In addition, both studies seek to ultimately recommend the measures that can be undertaken to curb the vice.

The study by Akomea-Frimpong, et.al (2019) presents a gap that requires the current study to fill. Firstly, the sample size of 43 was not adequate enough to draw better conclusions and generalize the findings. The current study seeks to interview 271 participants, and this allows for better results generalization and in addition the former study was undertaken in Ghana, which has different socioeconomic dynamics to that of the research site in Zambia.

Bongomin and Ntayi (2020) studied the adoption and usage of mobile money in financial inclusion, and its mediating effect on consumer protection, with focus on digital policy, regulation and Governance. The major findings were that digital consumer protection significantly affects mobile money adoption and usage. This study was relevant to the current study in that it sought to bring out the element of consumer protection among the mobile money users, which is in line with the study at hand. It also provided very key recommendations in promoting financial inclusion as well as consumer protection. However, the study presented a gap in that it focused only on small and medium enterprises, leaving out key mobile money users, such as the ordinary citizens.

In another study conducted by Mogaji and Nguyen (2022) to investigate the dark side of mobile money in Nigeria, fraud was identified as a major security concern among the users of mobile money transactions. Furthermore, the study highlighted a typology of relationships between the stakeholders in the ecosystem and their challenges and managerial implications.

This study provided theoretical insights into the topic at hand as it also brought out fraud as a major issue in the area of mobile money transactions despite having been

conducted in Nigeria. Its limit though lay in the fact that it did not include the regulator of mobile money in Nigeria, who are very important in the fight against mobile money fraud.

Ali et.al (2020) in their evaluation of key security issues associated with mobile money systems in Uganda, the researchers found that identity theft, authentication attack, phishing attack, vishing attack, SMiShing attack, personal identification number (PIN) sharing, and agent-driven fraud were the major sources of mobile money fraud.

In order to curb mobile money fraud, the study recommended the use of better access controls, customer awareness campaigns, agent training on acceptable practices, strict measures against fraudsters, high-value transaction monitoring by the service providers and developing a comprehensive legal document to run mobile money services.

2.2.3: Literature review-A local perspective

Zimba et.al, (2022), examined the level and degree of exposure of Zambian mobile phone users to mobile phone-based cyber-attacks that were usually implemented via social engineering. Their major findings were that mobile money fraud was as a result of widespread adoption of mobile phones, the adoption of mobile money, incompleteness of the law, people's low awareness of fraud prevention, and the strength of government regulation among other things. In order to control mobile money fraud, the research recommended providing awareness and education of the users about the attacks and the prevailing laws against them. They also recommended the enactment of unambiguous laws, thorough enforcement of the laws, stiffer penalties and blacklisting perpetrators from the mobile network operators (MNOs), and that the authorities should motivate users by making known, incidents where perpetrators were pursued, prosecuted and convicted.

This study was relevant to the current one in that localized the research on the topic to the Zambian case. However, there was a gap in that its sample was drawn from users of mobile phones in private and government institutions, leaving out the general members of the public and other key stakeholders who may have adequate information on the matter.

Sinkala (2023: 7-10) reviewed the following literature in relation to the adoption of mobile money in Zambia and its adoption among the people “Mobile money, an

innovative technology-based service, has garnered significant attention not only in Africa but worldwide. This digital payment system enables users to conduct financial transactions via mobile phones or related devices. While its definition varies depending on the business context, at its core, mobile money is a medium to transfer funds between accounts using mobile phones (Kombo & Tromp, 2006). It facilitates sending and receiving monetary value, offering users the flexibility and convenience to transact at anytime from anywhere (Chauhan, 2015). Additionally, mobile money transfer, sometimes known as mobile payment or mobile wallet, intersects the realms of banking and telecommunications (World Bank, 2012). It brings together stakeholders from both mobile phone service providers and financial institutions. The concept of utilizing mobile phones for financial engagements was pioneered in 1999 in Japan with NTT DoCoMo's I-Mode mobile internet service, allowing online purchases via mobiles. Some studies posit the genesis of mobile finance can be traced back to prepaid mobile services targeting Journal of Business and Strategic Management ISSN 2520-0402 (online) Vol.8, Issue No.7, pp 1 – 18, 2023 www.carijournals.org 8 those desiring anonymity and affordability (Sibwela, 2017). The shift towards a cashless transaction environment, driven by benefits like fraud reduction, decreased criminal activities, minimized cash handling costs, and less dependency on physical cash, emphasized the importance of such services. However, Africa revolutionized this domain in the early 2000s, capitalizing on the scarcity of traditional banking services. In Kenya, 2007 marked the launch of M-Pesa by Safaricom (Helix, 2018). This service, granting users the facility to transact money, settle bills, and buy goods/services using mobile phones, gained rapid popularity. By 2010, M-Pesa had over 14 million users in Kenya (Simiyu & Oloko, 2015). Today, M-Pesa stands as the most prominent mobile financial service in the developing world, boasting a clientele of approximately 83% of Kenya's adult populace, which translates to over 19.5 million individuals (Dorata, 2013). Following MPesa's inauguration in Kenya in 2007, several renowned mobile money platforms such as MTN, Airtel, Vodacom, G-CASH in the Philippines, and more emerged (UNCDF, 2014) (Julian et al., 2017).This success spurred similar ventures globally. 2.2.2 The Emergence and Growth of Mobile Money Services in Zambia In Zambia, the journey into Digital Financial Services (DFS) commenced in 2002 with the introduction of Celpay (Zambia, 2018), which primarily catered to corporate clients for bill payments. Gradually, various mobile banking services and third-party providers such as

ZOONA, Airtel, and MTN began to offer both bill payment and person-to-person transfer services (Chiti, 2018). At present, numerous commercial banks and their agent platforms like Zanaco express, First National Bank Zambia (FNB) E-wallet, Airtel money, MTN mobile money, and Zamtel money have joined the mobile banking brigade in Zambia (ZICTA, 2015) and has revolutionized the banking experience, ensuring it is both accessible and cost-effective. The proliferation of mobile phones across Africa, especially among low-income demographics, has made it feasible for mobile money services to utilize existing mobile infrastructure and distribution networks. These networks, initially set up for airtime distribution, now cater to the unbanked population, offering them accessible, convenient, and affordable financial amenities (Subia & Martinez, 2014). Mobile money has democratized financial access, especially for those who previously found traditional banking prohibitive due to minimum balance requirements and other constraints. This innovation has ushered in a secure, cost-effective means of transaction for the less privileged, leveraging existing mobile infrastructure and distribution channels (UNCDF, 2014). As a result, Journal of Business and Strategic Management ISSN 2520-0402 (online) Vol.8, Issue No.7, pp 1 – 18, 2023 www.carijournals.org 9 financial inclusion has surged, fostering economic growth as the previously marginalized segments of society embark on entrepreneurial ventures (Yousif et al., 2013). The intensifying competition between banks and mobile operators in Zambia arises from a significant segment of the population being financially marginalized due to the prohibitive costs and geographical challenges associated with traditional banking. Current data from the Zambian Central Bank reveals a marked increase in mobile money accounts, indicating the growing influence of this platform among the unbanked, especially in rural areas (Zambia, 2018). Mobile Money and SME Growth Yu (CS, 2012) employed the Unified Theory of Acceptance and Use of Technology (UTAUT) to delve into the determinants driving individuals to adopt mobile money banking services. This insightful study shed light on the nuanced factors steering mobile banking uptake. With a sample size of 441 respondents, it was empirically established that adoption intent was predominantly influenced by social factors, perceived financial implications, performance expectancy, and perceived credibility. Notably, individual intentions and facilitating conditions played a critical role in shaping adoption behaviours. The study also illuminated the nuanced role of demographics, pinpointing that gender significantly influenced performance

expectancy and financial considerations, while age moderated the influence of facilitating conditions and perceived self-efficacy on adoption. Maradung (2013) embarked on a study to discern the factors steering the uptake of mobile money services within Botswana's financial sphere. Leveraging the Technology Acceptance Model (TAM) coupled with demographic considerations, the research incorporated a diverse cohort of 190 respondents spanning users and non-users from four districts in Gaborone, Botswana. The findings painted an intriguing picture. Income levels and bank account ownership seemed inconsequential in shaping mobile money adoption. Age emerged as a defining factor, with the younger demographic showing a predilection for mobile banking. Educational attainment did not sway mobile money uptake. Gender dynamics revealed a tilt towards male users, and the employed demographic exhibited a stronger preference for mobile banking. The overarching conclusion was that mobile banking is gradually gaining traction in Botswana, especially among younger, employed males. This trend signals a promising trajectory for banking accessibility in Botswana. Yankee Group Research (2002) highlighted the nascent challenges m-commerce faced, particularly in the U.S. landscape. Survey insights revealed that U.S. consumers grappled with cost, speed, and perceived complexities of mobile services. The Asian and European markets, on the other hand, Journal of Business and Strategic Management ISSN 2520-0402 (online) Vol.8, Issue No.7, pp 1 – 18, 2023 www.carijournals.org 10 saw mobile phones as primary online gateways, bypassing traditional PCs. A prominent challenge for mobile money's ascendancy, especially in regions like Finland, was the need for multi stakeholder alignment. Service providers had the dual challenge of courting vendors to create the requisite infrastructure and convincing consumers of the system's utility".

Kabala et.al (2021) carried out an ethnographic study to analyze the influence of mobile money on financial inclusion in urban Zambia. They found that mobile money positively influences financial inclusion in urban settings. The lack of information about the safety of mobile money accounts was also a major factor in the usage of mobile money. This study was important as it provided insights into mobile money usage in urban areas, where there is higher usage of the mobile money services and fraud rates, hence necessitating the current study in order to fully understand the phenomenon. However, it created a gap in that the focus was on the urban population

making it difficult to extend the findings to rural areas. In addition, its focus was on financial inclusion and the issue of mobile money fraud was not fully addressed.

In an Ethnographic study by Brujin et.al (2017), which was conducted in Cameroon, Zambia, Congo DR and Senegal, it was found that a lack of regulation and consumer protection is holding people back from using mobile money, and the attitudes of the consumers towards low usage of mobile money services was due to mistrust of the system itself.

This study was important as it underpinned the role of attitudes and trust in adhering to the protection measures that relevant authorities may put in place in order to combat mobile money fraud. This was highly connected to the theoretical framework that underpinned the current study.

The gap that this study presented lay in the methodology itself. The ethnographic approach involved observing participants in the field. This methodology by its nature, leaves room for subjectivity on the part of the researcher as it is possible to draw wrong conclusions about a subject of study (Amuomo & Odoyo, 2020). The current study's mixed research approach to obtain both qualitative and quantitative data of the same weight provided a more objective study approach.

Kanobe and Bwalya (2021) sought to lessen the snags associated with mobile money services in developing economies. Their study found several challenges that included inadequate monitoring of the mobile money agents, insufficient confidentiality, and lack of privacy in financial transactions. Likewise, the use of generic guidelines and policies, third-party involvement in sensitive mobile money activities, and weak staff recruitment policies were cited as having contributed to the challenges. Like other works mentioned above, the details of mobile phone-based cyber-attacks were given little attention in this study.

Mwila (2020) assessed the cyber-attacks preparedness strategy for both the public and private sector in Zambia. His study found that these two sectors have low compliance levels with understaffed cyber security experts whose roles are mostly assumed by IT professionals. His study could explain why the country is still facing challenges to address cyber-attacks in the mobile money services sector. It therefore provided insights into the measures put in place to control fraud in the mobile money arena, and pointed out lack of expertise in fighting the scourge of cyber-attacks. The relevance of

this study to the current one cannot be over emphasised as mobile money fraud is a component of the main stream cyber-crime and bears similar characteristics as those of other types of this criminality. On the other hand, however, it advanced a gap in that its focus was on institutions leaving out key stake holders such as the actual users of mobile money services, who are ultimately affected by the fraudsters.

Chipa & Mwanza (2021) in their study on factors impeding mobile money expansion in Zambia, found low incomes, low educational levels, gender disparities, and the lack of ease of use and knowledge of mobile money services as being responsible. The study helps to provide insights into the topic at hand as it formed part of the body of knowledge on the topic for Zambia. However, it provided a gap by not considering the security and safety aspects of mobile money. Its major focus was on the increase of the usage of mobile money, which ordinarily comes with its own challenges of security to its users, hence the need to find lasting solutions to overcoming the scourge.

2.2 Summary of scholarly studies on mobile money fraud related cyber crime

TITLE	AUTHOR/YEAR	OBJECTIVE	METHODOLOGY	FINDINGS	GAP
"An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia."	Mwila, Kingstone Ali. 2020.	To assess a cyber-attacks preparedness strategy for Public and Private Sectors in Zambia.	An explanatory study design was adopted with a sample size of 150	Low level compliance to cyber security guidelines among private and public entities. Under staffed cyber security personnel	Focused on cyber security in general. Concentrated on institutions and left out the stakeholders in mobile money services. The sample size of 150 was lower than the current study's 271 in terms of offering better validity.
Mobile money adoption and usage and financial inclusion: mediating effect of digital consumer protection.	Okello, Candiya Bongomin, George & Ntayi, Joseph. 2020.	To establish the mediating effect of digital consumer protection in the relationship between mobile money adoption and usage and financial inclusion with data	Cross-sectional design combined with quantitative approach involving 379 MSMEs in northern Uganda.	Mobile money adoption and usage has both direct and indirect effect on financial inclusion. Financial inclusion is influenced by both mobile money adoption and usage and	Data was only collected from samples located in Gulu district, northern Uganda and specifically from MSMEs, generalization of the study findings to other population who also use mobile

TITLE	AUTHOR/YEAR	OBJECTIVE	METHODOLOGY	FINDINGS	GAP
Digital Policy, Regulation and Governance.		collected from micro small and medium enterprises (MSMEs) in Northern Uganda.		digital consumer protection.	Money services becomes risky.
Control of fraud on mobile money services in Ghana: an exploratory study	Akomea-Frimpong, Isaac; Andoh, Charles; Akomea-Frimpong, Agnes & Dwomoh-Okudzeto, Yvonne. 2020.	To explore the main causes of fraud in the mobile money services in Ghana and the measures to combat the menace by the key stakeholders connected to the mobile money services.	Qualitative research design was adopted and study sample was 43 and involved the stakeholders in mobile money services provision as well as their role in controlling mobile money fraud.	Mobile money services fraud is caused by weak internal controls and systems, lack of sophisticated I.T tools to detect fraud, inadequate education and training and the poor remuneration of the employees.	The sample size of 43 was not good enough to validly draw the conclusions. This study sample of 271 has a much higher validity rate than the one with 43 respondents. The study was undertaken in Ghana which has a different cultural and legal set up to that of Zambia

TITLE	AUTHOR/YEAR	OBJECTIVE	METHODOLOGY	FINDINGS	GAP
Emerging Mobile Phone-based Social Engineering Cyber-attacks in the Zambian ICT Sector	Zimba, Aaron; Mukupa George & Chama, Victoria. 2022.	To present a high-order analytical approach towards mobile phone-based phishing attacks in Zambia.	Adopted a hybrid descriptive research design involving 180 participants from private and public institutions	A lot of Zambians are victims to the mobile money attack campaign by the victims. Most of the respondents were aware of the different tactics that attackers use.	Its focus was on participants from private and public institutions. It lacks representation from other users of mobile money such as the general public, the ICT Regulator and indeed Law Enforcement. In addition, the sample size of 180 was lower than the current study's 271, which provides better validity test results.
Evaluation of Key Security Issues Associated with	Ali, G Ally, Dida M, and Elikana Sam A. 2020.	To evaluate the key security issues associated with mobile money systems in Uganda.	Descriptive research design, and stratified random sampling technique involving 1270 respondents	key security issues are identity theft, authentication attack, phishing attack, vishing attack, SMiShing attack,	Omitted key stakeholders. Respondents were volunteers as such may pose a bias.

TITLE	AUTHOR/YEAR	OBJECTIVE	METHODOLOGY	FINDINGS	GAP
Mobile Money Systems in Uganda				personal identification number (PIN) sharing, and agent-driven fraud	The study was done in Uganda, cannot be generalised to other areas
The dark side of mobile money: Perspectives from an emerging economy	Mogaji, Emmanuel and Nguyen, N. Phong. 2022	To qualitatively examine the dark side of mobile money by engaging with key stakeholders in the mobile money ecosystem of Sub-Saharan Africa (SSA).	Exploratory qualitative approach was adopted and 68 participants were interviewed.	Existence of four relationships between the stake holders i.e customer–developer, customer–agent, developer–agent and developer–regulator – was found along with issues of fraud, security, information privacy and emotional connections with money.	Regulators were left out of this study. It focuses on Nigeria and hence the findings cannot be generalized to other areas such as Zambia. The sample size of 68 did not derive a better measure of validity as compared to this study's 271.
An Ethnographic Study on Mobile Money attitudes, perceptions and	Bruijn, M., Butter, I., & Fall, A. 2017.	To study the usage, perceptions and attitudes towards digital	Qualitative ethnographic research method. Participant	Technology was observed to interact with users and non-users alike, and in	The ethnographic approach that was conducted within a period

TITLE	AUTHOR/YEAR	OBJECTIVE	METHODOLOGY	FINDINGS	GAP
usages in Cameroon, Congo DRC, Senegal and Zambia.		financial services (DFS) in four selected countries namely Cameroon, DRC, Senegal and Zambia.	observation of un quantifiable sample size.	relation to 'trust', reveals the potential of DFS to change patterns of power, social relations.	one year in four different countries. The sample size was not determined due to the approach adopted.
"An Ethnological Analysis of the influence of Mobile Money on financial inclusion: The case of urban Zambia.	Kabala, Edna; Mapoma, Rosemary; Nalutongwe, Chitimba; Muyani, Diana; and Lungu, John. 2021.	To investigate the influence of mobile money on financial inclusion using urban Zambia.	Employed ethnological study approach and interviewed 112 respondents.	-Mobile money positively influences financial inclusion in urban settings. -There is lack of information about the safety of mobile money accounts.	The research methodology is susceptible to subjectivity. The focus on urban population makes it difficult to extend the findings to rural areas. In addition, the validity derived from sample size of 112 was far below this study's 271.
Factors impeding Mobile Money	Chipa, Natalie & Mwanza, Bupe. (2021	To investigate factors impeding Mobile Money	The study adopted a mixed methods approach, which	Agents' location contributed to fraud risks or thefts	The study mainly focused on factors impeding the growth of mobile money

TITLE	AUTHOR/YEAR	OBJECTIVE	METHODOLOGY	FINDINGS	GAP
expansion in Zambia		expansion in Zambia	utilized both qualitative and quantitative research approaches on 100 respondents.	when using mobile money services.	and not the security aspects of it.

2.3 Summary

This Chapter looked at the critical review of literature on the subject matter. The review of the literature took a global perspective, where studies that were conducted in other parts of the world were analysed. It also took a continental view, where several studies from Africa were reviewed. In addition, the local view looked at studies that were done in Zambia. The main thematic issue drawn from the literature review was that mobile money fraud is both international and local phenomenon. The research instruments of measurement applied is different in each and every study. The methodology, objectives, sample size and scope of the various studies among others were found to be different, as such, the findings from these studies are different. The implication is that similar studies can be conducted in different study sites the outcomes cannot be generalised to other parts of the globe. However, overally, literature review helped the study to be focussed.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Overview

This chapter dealt with the research methodology. The first component that was discussed was the research design. This was then followed by the target population where the data was collected from. The third component that was presented was the sample size and this was followed by sampling techniques, which discussed how the sample was drawn from the population. The fifth element of discussion under this chapter was data collection instruments which were used in the research. After this, there was a presentation of the techniques that were used to analyze the data that was collected.

3.1 Research Design

In general, this study adopted a mixed research design and particularly, the convergent parallel research design, which was ideal for collecting both quantitative and qualitative data at the same time during the data collection process in the study area.

3.1.1 Research approach (Philosophical underpinnings)

Basic approaches to research can be categorized into quantitative, qualitative and mixed methods. This study adopted the mixed design as indicated above. In most cases, the quantitative research design is generally associated with the positivity paradigm and uses deductive techniques and involves analysis of numerical variables, the qualitative research approach is generally associated with the social constructivist paradigm, uses inductive techniques to measure non-numerical variables in order to understand phenomena. Considering the nature of this study, in order to collect and analyze both quantitative and qualitative data, the study adopted the Pragmatic approach.

3.2 Study Area

The study was carried out in Lusaka District, Zambia. The choice of Lusaka was based on the fact that it is the capital city of Zambia, where all the key stakeholders such as the Regulator, the Mobile Network Operators, the Zambia Police Service, are all based, making it easier to collect data from them. In terms of the individual mobile money users and the mobile money agents, Lusaka being the most populated city in the country was conveniently selected due to its potential to have more cases of mobile money fraud

because it has majority number of subscribers thereby attracting more fraudsters than any other District in the country.

3.3 Target Population

The study population encompassed all the major stakeholders in the usage of mobile money in Zambia. These included participants from the Regulatory Authority (Zambia Information and Communications Authority), the Zambia Police Service, all the three Mobile Network Operators, the mobile money transactions agents and the members of the general public. This population was targeted mainly because of the role they play in the provision of both usage of mobile money and in combatting fraud in mobile money. The mobile money business is quite dynamic in nature in that it is very difficult to ascertain the actual population of both individual users and the mobile money agents in a particular District. As such, the actual population of the participants in this study could not be determined, but is estimated to be above 20,000.

3.4 Sample Size

A sample size of two hundred and seventy one (271) participants was drawn in this study. Of these, six (6) were from the MNOs, four (4) from the Zambia Police Service, two (2) from ZICTA, Fifty (50) from the mobile money agents and Two hundred and nine (209) from members of the general public.

The population for the mobile money agents and individual mobile money users in Lusaka District could not be established, as such, the formula to draw the sample was derived from Cochran (1977) for infinite population as indicated below:

$$n_o = \frac{Z^2PQ}{e^2}$$

where:

- n is the sample size
- Z is confidence level at 90%, the z-score =1.645
- P is the population proportion at 50% (0.5)
- e is the margin of error 5% (0.05)

$$n_o = \frac{1.645^2 * 0.5\ (1-0.5)}{0.05^2}$$

$$= \frac{2.7060*0.5*0.5}{0.0025}$$

Sample size = 271

3.5 Sampling Techniques

The study adopted a mixed sampling method. Purposive sampling method was used to draw participants from ZICTA, Zambia Police Service and MNOs. This method was utilized because of the need to collect data from the actual participants who deal with issues related to mobile money in general and mobile money fraud in particular. This was important to ensure that data was collected from the participants who had the knowledge as well as the experience in dealing with matters of mobile money fraud. On the other hand simple random sampling method was used in drawing participants from the mobile money agents as well as the general public.

The simple random sampling method was adopted due to the nature of the target population, which was homogenous in nature, as such, randomization was necessary to ensure validity and generalization of the sample results. Under this sampling design, every item of the population has an equal chance of inclusion in the sample. The results obtained from probability or random sampling can be assured in terms of probability, that is the measuring the errors of estimation of the significance of the results obtained from a random sample.

3.6 Research Instruments

In order to collect primary data, structured questionnaires were used on participants from the aforementioned institutions. On the other hand, interview guides were used to collect data from the mobile money agents and the general public.

As indicated above, the research instruments that were used in this study design were a questionnaire and interview guide. The questionnaire was adopted in this study because of its main advantage of enabling the Researcher to collect data from a large sample and diverse regions within a short period of time as it saves time in administering. In addition, questionnaires provide structured and standardized responses, making the analysis process more streamlined and less time-consuming. It eases the analysis by ensuring that it provides the ability to use statistical software and tools to process the

data quickly. Further, since the questionnaire is presented on paper format or online, there is no opportunity for interviewer bias.

It is worthy indicating however, that, a questionnaire has some limitations in that there is no opportunity to ask further information related to the answers given. There is also no direct contact between the parties and as such, the researcher cannot deal with any misunderstanding that may arise during the process of responding (Rashid, 2020).

On the other hand, the interview guide helps to provide face-to-face or personal interviews and is as such ideal in the collection of high quality data. In this study, some of the questions were quite sensitive and therefore, in-depth interviews using the guide was preferable in such instances as the Researcher was able to pay attention to non-verbal behaviour and establish a rapport with the respondents over an extended period of time. As compared to other methods of data collection, in-depth interviewing offers a greater degree of flexibility as the interviewer can explain the purpose of the interview and encourage potential respondents to co-operate. They also facilitate the clarification of questions, correct misunderstandings, offer prompts, probe responses and follow up on new ideas in a way that is just not possible with other methods (Mathers, et.al, 2000).

On the other hand, secondary data was collected through reviewing existing literature as well as other relevant articles on the topic on measures that have been put in place to curb mobile money fraud in meeting the set objective,.

3.6.1: Trustworthiness and Credibility, Reliability and Validity

In order to achieve reliability in the data collected through the instruments, the Cronbach's coefficient alpha test to examine scale reliability and internal consistency was conducted. The aim was to obtain a Cronbach's alpha of .70 and above which is a good measure of proof for reliability or internal consistence. The selection of the Cronbach's alpha was due to its many advantages that include easy to compute and interpret, as it only requires the item scores and the number of items. In addition, it is widely accepted and reported in many fields and journals, so it facilitates comparison and communication of results. Further the test can be used for different types of scales and items, such as Likert scales, multiple-choice questions, both which are a party of this proposed study. Furthermore, it can be adjusted for to deal with different situations, such as when the items have different weights, when the items are nested within groups, or when the items are missing.

Credibility is simply a measure of the truth value of qualitative research, indicating whether the study's findings are correct and accurate. In order to achieve this, the study adopted triangulation and using multiple data sources, peer briefing, negative case analysis and member checks where participants could review the findings to confirm their accuracy. This was used in order to increase the credibility of qualitative component of this study.

Validity on the other hand was be achieved by conducting a thorough literature review, consulting with subject matter experts, and pre-testing the questionnaire with the target population to identify and address any gaps or ambiguities in the items. The pilot study was conducted with a group of 20 participants drawn randomly before the study could be undertaken.

3.7 Data collection procedures and Timeline

The researcher submitted the introductory letter from the University of Zambia, which was approved by the Research Supervisor, and his own letter seeking permission to conduct a study in the targeted institutions, namely the Zambia Police Service, Zambia Information Communication Technology Authority and the Mobile Network Operators. Once permission was granted, the researcher then administered the research instruments to the respondents at the aforementioned institutions. In addition, the questionnaires were replicated in google forms to provide the respondents with an option of answering them online. The collection of data was undertaken between March 23rd and March 30th of 2024.

3.8 Data Analysis Techniques

In order to understand the cause and effect relationship between variables, multivariate Regression analysis was used on the quantitative variables, as well as correlation analysis with the aid of Social Package for Social Sciences (SPSS) and Microsoft Excel, while the qualitative ones were done by using content and thematic analysis technique.

3.9 Ethical considerations

This study endeavoured to protect the privacy of the participants by holding high levels of confidentiality. The participants were engaged in order to obtain consent from them before participating in the study. In addition, the participants were informed about the purpose of the study and that it would take them about twenty (20) minutes to complete

the questionnaire and that the interviews would equally take the same duration. Further, the participants were informed that the interviews would be held at a place and time convenient to them. Furthermore, they were assured that the findings of the research would be made available to them if they were interested. In addition, clearance was obtained from the University of Zambia Ethics Committee before proceeding with the research. All this was be done in order to ensure that the research was conducted in a way that was ethical.

3.10 Summary

This Chapter looked at the research design, where it was explained that the study adopted a convergent parallel mixed research design. It also looked at the study area, which is Lusaka District due to its population size and the fact that it was easy to interview participants from the target institutions. It also looked at the target population, which included participants from ZICTA, Zambia Police Service, MNOs, individual users and mobile money agents. In addition, the Chapter looked at the sample size, which is 271, selected by using simple random randomly sampling for most of them, and convenient sampling for those from the target institutions. The Data collection instruments and the data collection procedures and timeline were also considered. The questionnaire and interview guide were the instruments of data collection used in the process.

Data analysis was also looked at, where it was explained that SPSS version 27 and Microsoft Excel were used to conduct tests such as regression and correlation, and the thematic as well content analysis were used to analyze qualitative data. On the other hand, the ethical issues were also looked at in the same chapter.

CHAPTER IV

PRESENTATION OF FINDINGS

4.0 Overview

This chapter presents the research findings. The findings are presented according to themes and sub themes derived from the research objectives.

4.1 Biographical information of the respondents

In trying to establish the adequacy of the control measures in combatting mobile money fraud in Lusaka, the study first sought biographical information of which gender was the first to be presented.

4.1.1 Gender

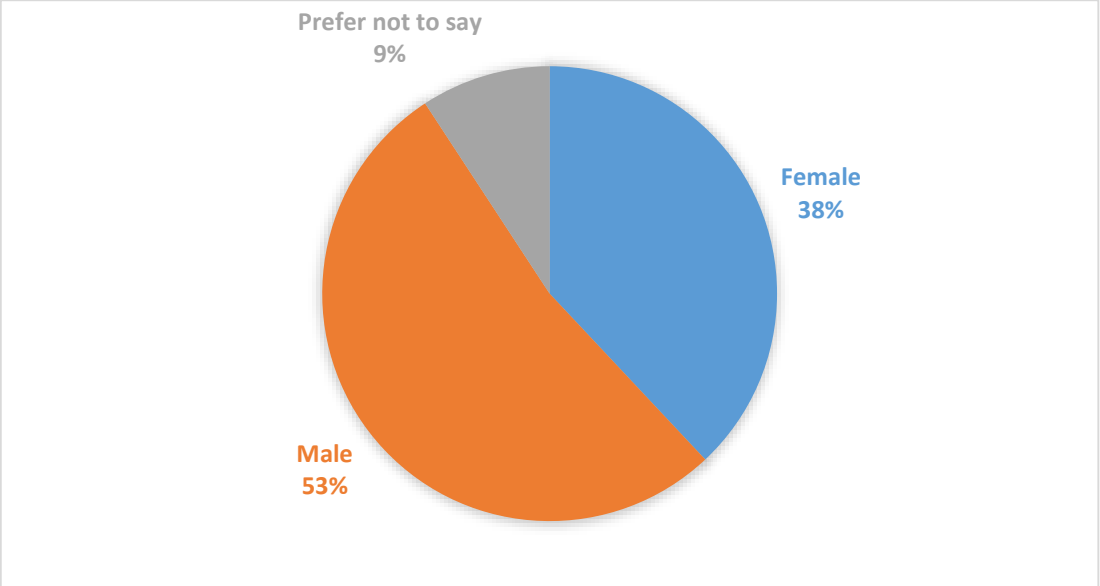

Figure 1: Respondents distribution by gender

Source: Field Data, 2024

Figure 1 above presents the gender of the participants and there were 103 (38.0%) female respondents while 143 (52.8%) were men. There were 25 (9.2%) of the respondents who opted not to say their gender. The mean and standard deviations were 1.56 and 0.657 respectively as shown table 1 below.

Table 1: Gender distribution mean and standard deviation

	Mean	Std. Deviation	N
Gender	1.56	.657	271

Source: Field Data, 2024

4.1.2 Age range

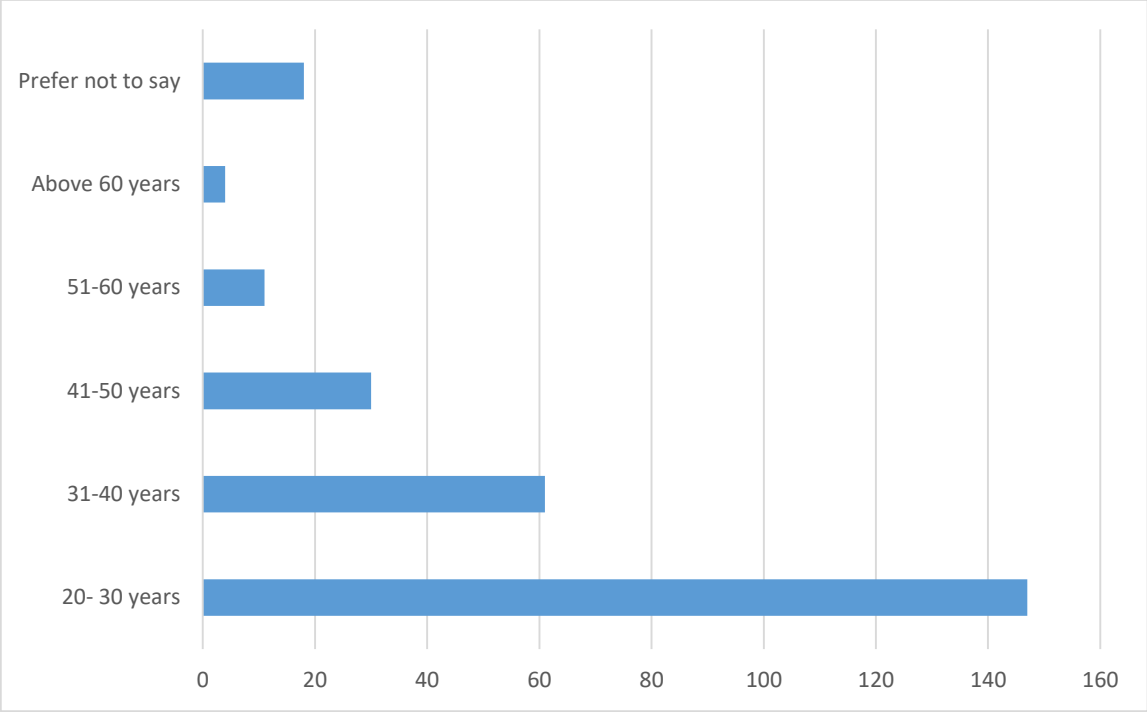

Figure 2: Respondents distribution by Age range

Source: Field data: 2024

The mode age of the respondents was ranging between 20-30 years amounting to 147 (54.2%), while 61 (22.4%) were aged between 31 and 40 years. Meanwhile, 30 (11.1%) of the respondents were aged between 41 and 50 years, 11 (4.1%) were aged between 51 and 60 years. There were 4 (1.5%) respondents who were aged above 60 years, while 18 (6.6%) respondents preferred not to disclose their age range. This information is depicted in figure 2 above.

On the other hand, the mean was 1.76 representing the age range between 20 and 30 and the median was 1.0, falling in the same age range as the mean. The standard deviation was 0.980 with a variance of 0.961. This is depicted in table 2 below.

Table 2: Descriptive statistics on age range

Age_Range		
N	Valid	271
	Missing	0
Mean		1.76
Median		1.00
Std. Deviation		.980
Variance		.961

Source: Field data, 2024

4.1.3 Level of Education

Table 3:Respondents distribution by level of education

		Frequency	Percent	
Valid	Certificate	83	30.7	
	Degree	57	21.0	
	Diploma	37	13.7	
	Grade 12	14	5.2	
	Masters	13	4.8	
	None	1	.4	
	PHD	3	1.1	
	Prefer not to say	63	23.24	
	Total	271	100.0	
	Mean	3.41	Std. deviation	2.336

Source: Field data, 2024

The above table illustrates the education level of stake holders in the usage of mobile money services in Lusaka District. The Table indicates the level of education attained and this was ranging from Grade 12 to University level as shown in the table above. The mode of the respondents was 82 from the Certificate holders, representing 30.3%, with a mean value of 3.41 and standard deviation of 2.336

4.1.4 ICT proficiency

Table 4: Respondents level of ICT proficiency

	Frequency	Percentage (%)
Very high	25	9.2
High	46	17
Moderate	101	37.3
Fair	76	28
Low	23	8.5
TOTAL	271	100

Source: Field data 2024

The above table shows the levels of proficiency of the respondents in terms of their Information, Communication and Technology (ICT) skills. The mode of this

distribution was 101 (37.3%) indicating that most of them had moderate ICT proficiency levels.

4.2 Mobile money fraud control measures types

Having presented respondents' biographical data, next are the types of control measures that are employed in combatting mobile money fraud in Lusaka District.

4.2.1 Types of mobile money fraud

Table 5: Respondents distribution by types of mobile money fraud

	Frequency	Percentage (%)
Sim card swap	47	8.3
Identity theft	79	14
Fake promotions	146	25.9
Fake money transfers	199	35.3
Phishing	29	5.1
Fake product/service delivery	64	11.7
TOTAL SCORES	564	100

Source: Field Data, 2024

Table 5 above illustrates the overall Score for the respondents on the types of mobile money fraud that they knew of. Of them, 47 (8.3%) identified sim card swap, 79 (14%) indicated identity theft, 146 (25.9%) cited fake promotions. On the other hand, 199 (35.3%) identified fake mobile money transfers, 29 (5.1%) cited phishing and 64 (11.7%) were able to point out fake product/service delivery. From this, the most notable type of mobile money fraud was identified to be fake mobile money transfers with the mode of 199.

4.2.2 Most common type of mobile money fraud

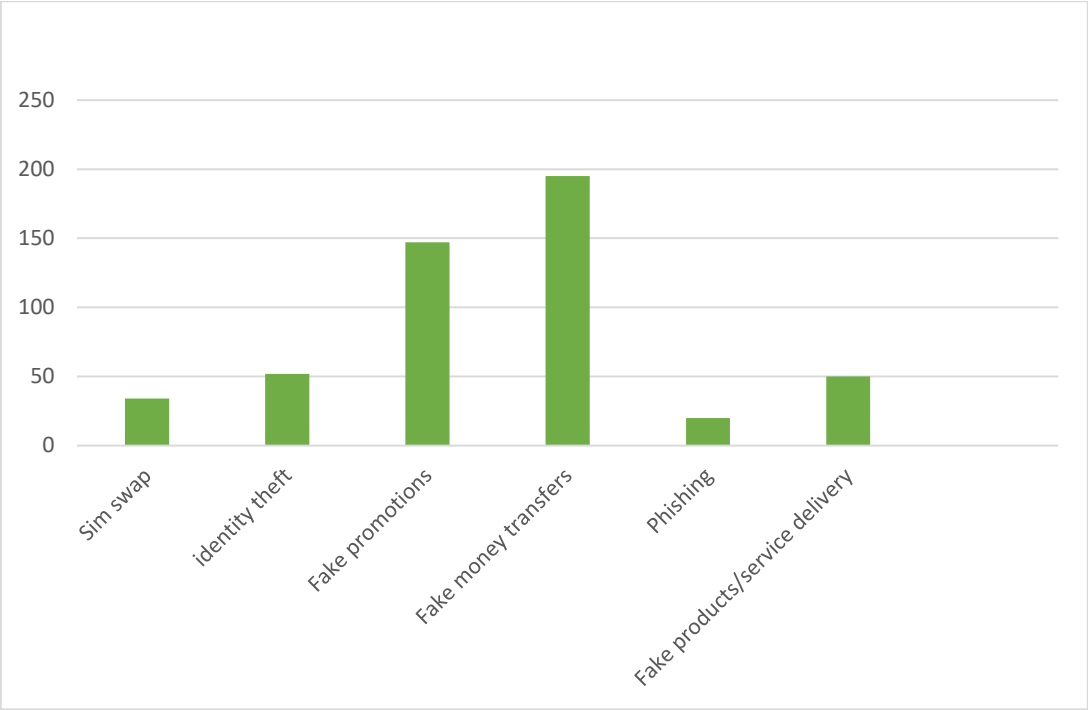

Figure 3: Respondents distribution by most common type of mobile money fraud

Source: Field data, 2024

Figure 3 above illustrates the overall score for the respondents on the most common types of mobile money fraud. 34 (6.8%) identified sim card swap, 52 (10.4%) indicated identity theft, 147 (29.5%) cited fake promotions. On the other hand, 195 (39.2%) identified fake mobile money transfers, 20 (4.0%) cited phishing and 50 (10.7%) pointed out fake product/service delivery. From this, the most common type of mobile money fraud was identified to be fake mobile money transfers with the mode of 195.

4.2.3 Measures to combat mobile money fraud

Having presented the types of mobile money fraud that the respondents were familiar with, the next section presents the measures that are used to combat mobile money fraud.

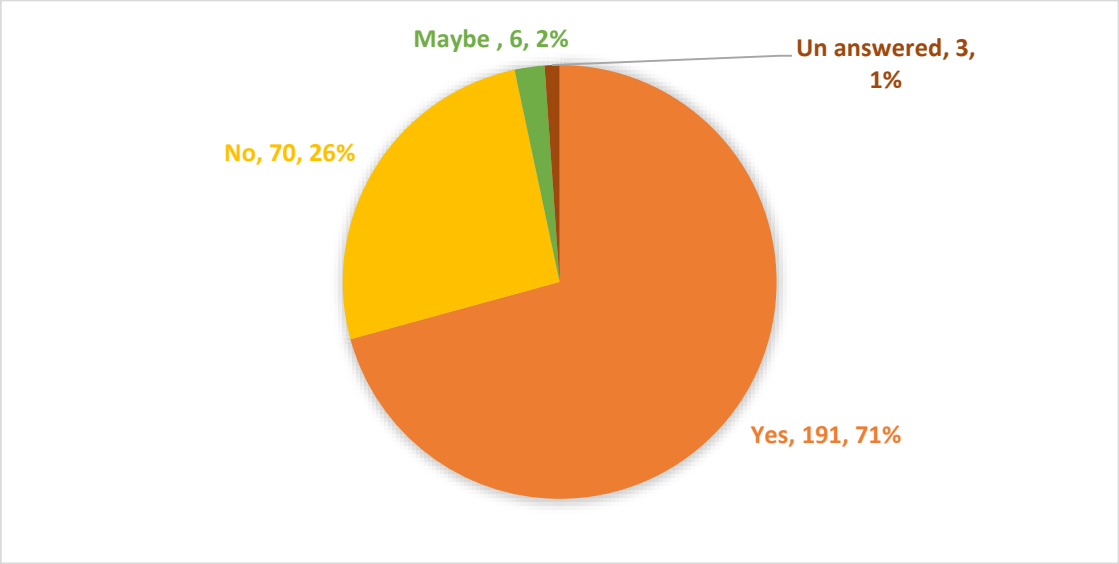

Figure 4: Respondents distribution by employing control measures

Source: Field Data 2024

When asked on whether the respondents employed any control measures to combat mobile money fraud, the majority 191 (71%) indicated that they did, while 70 (26%) stated that they do not undertake any control measures. On the other hand, 6 (2.2%) stated that maybe they did, while 3 respondents (1.8%) did not respond to the answer. These results are depicted in figure 4 above.

4.2.4 Mobile money fraud control measures

Table 6: Type of control measures used in combatting mobile money fraud

Control Measure	**Frequency**	**Percentage (%)**
Implementing the measures outlined in the sensitization of users	115	32.6
Sensitization and training of mobile money agents	23	6.5
Fraud detection by being alert	76	21.5
Enhancement of mobile money security by using technology	31	8.8
Apprehension/arresting of offenders	36	10.2
Reporting the fraudsters to the relevant authorities	72	20.4
TOTAL SCORES	353	100

Source: Field data, 2024

From the above table, 115 (32.6%) disclosed that they combat mobile money fraud by implementing the measures outlined in the sensitization of the users, while 23 (6.5%) stated that they attended trainings and sensitization programs meant for the mobile money agents. This target group belonged to the mobile money agents. On the other hand, 76 (21.5%) stated that they combat mobile money fraud by simply being alert as users and mobile money agents. Further, 31 (8.8%) stated that mobile money fraud could only be combatted by enhancement of mobile money security by using technology, while 36 (10.2%) indicated that the apprehending the offenders is the best way to curb the scourge of mobile money fraud. However, 72 (20.4%) stated that they report the fraudsters to the relevant authorities and in so doing curb mobile money fraud.

4.2.5 Control measures implementation

Table 7: Respondents distribution by frequency of implementing the control measure

Responses	**Frequency**	**Percentage (%)**
Very frequently	27	9.6
Frequently	114	42.1
Rarely	98	36.2
Not at all	32	11.8
TOTAL	**271**	**100**
Mean 2.51	Standard deviation	.834

Source: Field data, 2024

From Table 7 above, it is indicative of the fact that 27 (9.6%) of the respondents stated that they implemented the measures to curb mobile money fraud very frequently, 114 (42.1%) stated that they frequently do so, while 98 (36.2%) stated that they rarely do so, and 32 (11.8%) stated that they do not implement any control measure at all.

4.2.6 Most effective control measure

Table 8: Respondents distribution on the most effective control measure

Measure	Frequency	Percentage (%)
Sensitization of users	108	39.8
Sensitization and training of mobile money agents	34	12.5
Fraud detection	47	17.3
Enhancement of mobile money security by using technology	23	8.5
Apprehension/arresting of offenders	52	19.2
Not sure	7	2.7
TOTAL	271	100

Source: Field data 2024

As regards the most effective control measure used to curb mobile money fraud, of 108 (39.8%) respondents chose sensitization, while 34 (12.5%) stated that sensitization and training of mobile money agents was the most effective. On the other hand, mobile money fraud detection was argued to be the most effective by 47 (17.3%) respondents. Further, 23 (8.5%) of the respondents stated that enhancement of mobile money security by using technology was the most effective control measure while 52 (19.2%) commended apprehension/arresting of offenders as the most effective control measure, and 7 (2.7%) were not sure about which of the control measures they could indicate as the most effective in curbing mobile money fraud. This is depicted by table 8 above.

4.2.7 Most effective control measure

Table 9: Respondents perception on the most effective control measure

control measure	Sensitization of users	Sensitization and training of mobile money agents	Fraud detection	Enhancement of mobile money security by using technology	Apprehension/arresting of offenders	perceptions on the most effective control measure	**(%)**
Strongly Agree	150	129	91	93	137	600	44.3
Agree	94	87	87	75	76	419	30.9
Not Sure	24	55	90	95	50	314	23.2
Disagree	1	0	3	6	7	17	1.3
Strongly Disagree	2	0	0	2	1	5	0.4
TOTAL SCORES	271	271	271	271	271	1,355	100

Source: Field Data, 2024

Table 9 above illustrates the summary of the respondents' perception on the most effective control measure with total score of 1,355. The mode of the score was 600 representing 44.3%. The total numbers of respondents on the strongly agree were 600 representing 44.3% and those who agreed were 419 representing 30.9%. On the other hand, those who were not sure were 314 representing 23.2% and those that disagreed were 17 representing 1.3%, while those who strongly disagreed were 5 representing 0.4%.

Table 10: Respondents distribution by sensitization is the most effective control measure

	Frequency	Percent
Strongly Agree	150	55.4
Agree	94	34.7
Not Sure	24	8.9
Disagree	1	0.4
Strongly Disagree	2	0.7
TOTAL SCORES	271	100
	Mean 4.435424	

Source: Field Data, 2024

4.2.8 Sensitization is the most effective control measure

Table 10 illustrates the variable sensitization of users on issues related to mobile money fraud in measuring the most effective control measure. From the above table, the mode of the respondents is 150 which is 55.4% of the strongly agree. 94 respondents representing 34.7% agree, 24 respondents representing 8.9% were not sure about the issue. 1 respondent representing 0.4% and 2 of the respondents which is 0.7% strongly disagree. The sum total of the respondents were 271. The mode of the respondents of 55.4% agree and therefore with a mean of sensitization is the most effective control measure being 4.4354 above the neutral in the Likert scale which shows that most respondents perceive that the sensitization is the most effective control measure in curbing mobile money fraud, therefore the perception is high.

4.2.9 Sensitization and training of mobile money agents

Table 11: Respondents distribution by the most effective control measure being sensitization and training of mobile money agents

	Frequency	Percent
Strongly Agree	129	47.6
Agree	87	32.1
Not Sure	55	20.3
Disagree	0	0
Strongly Disagree	0	0
TOTAL SCORES	271	100
	Mean 4,273063	

Source: Field Data, 2024

Table 11 illustrates the variable sensitization and training of mobile money agents on issues related to mobile money fraud in measuring the most effective control measure. From the above table, the mode of the respondents is 129 which is 47.6% of the strongly agree. 87 respondents representing 32.1% agree, 55 respondents representing 20.3% were not sure about the issue. Meanwhile, there was no respondent representing 0% who disagrees and similarly no respondent which is 0% strongly disagree. The sum total of the respondents were 271. The mode of the respondents of 47.6 agree and therefore with a mean of sensitization and training of mobile money as the most effective control measure being 4.2731 above the neutral in the Likert scale which shows that most respondents perceive that the sensitization and training of mobile money agents is the most effective control measure in curbing mobile money fraud, therefore the perception is high.

4.2.10: **Fraud detection by being alert**

Table 12: Respondents distribution by the most effective control measure being Fraud detection by being alert

	Frequency	Percentage
Strongly Agree	93	34.3
Agree	75	27.7
Not Sure	95	35.1
Disagree	6	2.2
Strongly Disagree	2	0.7
TOTAL SCORES	271	100
	Mean 3.926199262	

Source: Field Data, 2024

Table 12 illustrates the variable fraud detection by being alert to mobile money fraud in measuring the most effective control measure. From the above table, the mode of the respondents is 95 which is 35.1% under the "not sure" category. 93 respondents representing 34.3% strongly agree, 75 respondents representing 27.7% agree, 95 respondents representing 35.1% were not sure about the issue. Meanwhile, there were 6 respondents representing 2.2% who disagree and 2 respondents which is 0.7% strongly disagree. The sum total of the respondents was 271. The mode of the respondents is 34.3% not sure and therefore with a mean of fraud detection in mobile money as the most effective control measure being 4. 2731 above the neutral in the Likert scale, which shows that most respondents are not sure if fraud detection by being alert is the most effective control measure in curbing mobile money fraud.

4.2.11 **Enhancement of mobile money security by using technology**

Table 13: Respondents distribution by the most effective control measure enhancement of mobile money security by using technology

	Frequency	Percent
Strongly Agree	91	33.6
Agree	87	32.1
Not Sure	90	33.2
Disagree	3	1.1
Strongly Disagree	0	0
TOTAL SCORES	271	100
	Mean 3.9594	

Source: Field Data, 2024

Table: 13 illustrates the variable enhancement of mobile money security by using technology to curb mobile money fraud in measuring the most effective control measure. From the above table, the mode of the respondents is 91 which is 33.6% of the strongly agree. 87 respondents representing 32.1% agree, 90 respondents representing 33.2% who were not sure. Meanwhile, there were 3 respondents representing 1.1% who disagree and no respondent which is 0% strongly disagree. The sum total of the respondents were 271. The mode of the respondents is 33.6% representing the "strongly agree" category and therefore with a mean of enhancement of mobile money security by using technology as the most effective control measure being 3.9594 above the neutral in the Likert scale, it shows that most respondents perceive the enhancement of mobile money security by using technology as the most effective control measure in curbing mobile money fraud, therefore, the perception is relatively high.

4.2.11: **Apprehension/arresting of offenders**

Table 14: Respondents distribution by the most effective control measure being apprehension/arresting of offenders

	Frequency	Percentage
Strongly Agree	137	50.6
Agree	76	28.0
Not Sure	50	18.5
Disagree	7	2.6
Strongly Disagree	1	0.4
TOTAL SCORES		100
	Mean 4.2583	

Source: Field Data, 2024

Table: 14 illustrates the variable apprehension/arresting of offenders of mobile money fraud in measuring the most effective control measure. From the above table, the mode of the respondents is 137 which is 50.6% of the strongly agree. 76 respondents representing 28% agree, 50 respondents representing 18.5% were not sure. Meanwhile, there were 7 respondents representing 2.6% who disagree and 1 respondent which is 0.4% strongly disagree. The sum total of the respondents were 271. The mode of the respondents of 50.6% strongly agree and therefore with the mean of apprehending/arresting offenders as the most effective control measure being 4.2583 above the neutral in the Likert scale, it shows that most respondents perceive apprehending/arresting offenders as the most effective control measure in curbing mobile money fraud, therefore the perception is relatively high.

4.2.12 Policies/Laws used to combat mobile money fraud

Table 15: Respondents distribution on policies/laws used to combat mobile money fraud

Policy/Law	**Frequency**	**Percentage (%)**
National Information & Communication Technology Policy 2023	21	7.7
Electronic Communications and Transactions Act No. 4 of 2021	32	11.8
Data Protection Act No. 3 of 2021	29	10.7
The Cyber Security and Cyber Crimes Act No. 2 of 2021	84	31.0
National Cyber Security Policy of 2021	15	5.5
None of the above	43	15.9
Not sure	47	17.4
TOTAL	**271**	**100**

Source: Field Data 2024

Table 15 above illustrates the overall Score for the respondents on the policies/laws used to combat mobile money fraud 55 (20.3%) the identified National Information and Communication Technology Policy 2023, 71(26.2%) indicated Electronic Communications and Transactions Act No. 4 of 2021, 60 (22.1%) identified the Data Protection Act No. 3 of 2021, while 113 (41.7%) cited the Cyber Security and Cyber Crimes Act No. 2 of 2021. On the other hand, 38 (14%) indicated the National Cyber Security Policy of 2021, while 29(10.7%) were not aware of any policy/law in the study sector. The mode was 113 representing 41.7% on the Cyber Security and Cyber Crimes Act No. 2 of 2021.

4.2.13 Most useful policy/law

Table 16: Respondents perception on the most useful policy/law in combatting mobile money fraud.

Policy/Law	Frequency	Percentage (%)
National Information & Communication Technology Policy 2023	21	7.7
Electronic Communications and Transactions Act No. 4 of 2021	32	11.8
Data Protection Act No. 3 of 2021	29	10.7
The Cyber Security and Cyber Crimes Act No. 2 of 2021	84	31.0
National Cyber Security Policy of 2021	15	5.5
None of the above	43	15.9
Not sure	47	17.4
TOTAL	**271**	**100**

Source: Field Data 2024

Table 16 above illustrates the overall Score for the respondents on the most useful policy/law used to combat mobile money fraud 21 (7.7%) identified National Information and Communication Technology Policy 2023, 32 (11.8%) indicated Electronic Communications and Transactions Act No. 4 of 2021, 29 (10.7) identified the Data Protection Act No. 3 of 2021, while 84 (31.0%) cited the Cyber Security and Cyber Crimes Act No. 2 of 2021. On the other hand, 15 (5.5%) indicated the National Cyber Security Policy of 2021, while 43 (15.9%) indicated that none of the identified policies and laws was useful in curbing mobile money fraud. The mode was 84 representing 31% on the Cyber Security and Cyber Crimes Act No. 2 of 2021.

4.1.14 Effectiveness of the policies/laws

Table 17: Respondents perceptions on effectiveness of policies/laws in combatting mobile money fraud

Source: Field Data 2022

Policy /law	National Information & Communication Technology Policy 2023	Electronic Communications and Transactions Act No. 4 of 2021	Data Protection Act No. 3 of 2021	The Cyber Security and Cyber Crimes Act No. 2 of 2021	The National Cyber Security Policy of 2021	perceptions on effectiveness of policies/laws in combatting mobile money fraud	Percentage (%)
Strongly Agree	66	62	46	89	55	318	23.5
Agree	62	77	72	56	53	320	23.6
Not Sure	139	127	148	116	153	683	50.4
Disagree	3	3	3	8	6	23	1.7
Strongly Disagree	1	2	2	2	4	11	0.8
TOTAL	271	271	271	271	271	1,355	100

Table 17 illustrates the summary of the respondents' perception on the effectiveness of the existing policies and laws in controlling mobile money fraud, with the total score of 1,355. The total number of respondents on the strongly agree were 318 representing 23.5% and those who agreed were 320 representing 23.6%. On the other hand, those who were not sure were 683 representing 50.4% and those that disagreed were 23 representing 1.7%, while those who strongly disagreed were 11 representing 0.8%. The mode of the score was 683 representing 50.4% of the respondents who were not sure on the effectiveness of the policies and laws put in place to curb mobile money fraud in Lusaka.

4.2.15 **National Information & Communication Technology Policy 2023**

Table 18: Respondents distribution by the most effective policy/law being National Information & Communication Technology Policy 2023

	Frequency	Percentage
Strongly Agree	66	24.4
Agree	62	22.8
Not Sure	139	51.3
Disagree	3	1.1
Strongly Disagree	1	0.4
TOTAL	**271**	**100**
	Mean 3.6974	

Source: field Data, 2024

Table: 18 illustrates the variable National Information & Communication Technology Policy 2023 in measuring the most effective policy/law in mobile money fraud control. While 66 respondents representing 24.4% strongly agree, 62 respondents representing 18.5% agree and 139 respondents representing 51.3% were not sure. Meanwhile, there were 3 respondents representing 1.1% who disagree and 1 respondent which is 0.4% strongly disagree. The sum total of the respondents were 271. The mode of the respondents of 139 (51.3%) not sure and therefore with the mean of the National Information & Communication Technology Policy 2023 as the most effective policy being 3.6974 above the neutral in the Likert scale, it shows that most respondents are not sure as to the National Information & Communication Technology Policy 2023 being the most effective policy control measure in curbing mobile money fraud, therefore the perception is relatively high that most of the respondents are not sure about it.

4.2.16 Electronic Communications and Transactions Act No. 4 of 2021

Table 19: Respondents distribution by the most effective policy/law being Electronic Communications and Transactions Act No. 4 of 2021

	Frequency	Percentage
Strongly Agree	62	22.9
Agree	77	28.4
Not Sure	127	46.9
Disagree	3	1.1
Strongly Disagree	2	0.7
TOTAL	271	**100**
	Mean 3.71587	

Source: Field data, 2024

Table: 19 illustrates the variable Electronic Communications and Transactions Act No. 4 of 2021 in measuring the most effective policy/law in mobile money fraud control. 62 respondents representing 22.9% strongly agree, 77 respondents representing 28.4% agree and 127 respondents representing 46.9% were not sure. Meanwhile, there were 3 respondents representing 1.1% who disagree and 2 respondents which is 0.7% strongly disagree. The sum total of the respondents were 271. The mode of the respondents was 127 (46.9%) not sure and therefore with the mean of the Electronic Communications and Transactions Act No. 4 of 2021 as the most effective policy being 3.7159 above the neutral in the Likert scale, it shows that most respondents are not sure as to the Electronic Communications and Transactions Act No. 4 of 2021 being the most effective policy control measure in curbing mobile money fraud, therefore the perception is relatively high that most of the respondents are not sure about it.

4.2.17 Data Protection Act No. 3 of 2021

Table 20: Respondents distribution by the most effective policy/law being Data Protection ACT No. 3 of 2021

	Frequency	Percentage

Strongly Agree	46	16.9
Agree	72	26.6
Not Sure	148	54.6
Disagree	3	1.1
Strongly Disagree	2	0.7
TOTAL	271	**100**
Mean	3.57934	

Source: Field data 2024

Table: 20 illustrates the variable Data Protection Act No. 3 of 2021 in measuring the most effective policy/law in mobile money fraud control. 46 respondents representing 16.9% strongly agree, 72 respondents representing 26.6% agree and 148 respondents representing 54.6% were not sure. Meanwhile, there were 3 respondents representing 1.1% who disagree and 2 respondents which is 0.7% strongly disagree. The sum total of the respondents were 271. The mode of the respondents was 148 (54.6) not sure and therefore with the mean of the Data Protection Act No. 3 of 2021 as the most effective policy being 3.5793 above the neutral in the Likert scale, it shows that most respondents were not sure as to the Data Protection Act No. 3 of 2021 being the most effective policy control measure in curbing mobile money fraud, therefore the perception is relatively high that most of the respondents are not sure about it.

4.2.18 The Cyber Security and Cyber Crimes Act No. 2 of 2021

Table 21: Respondents distribution by the most effective policy/law being the Cyber Security and Cyber Crimes Act No. 2 of 2021

	Frequency	Percentage

Source: Field Data, 2024

Strongly Agree	89	32.8
Agree	56	20.7
Not Sure	116	42.8
Disagree	8	2.9
Strongly Disagree	2	0.7
TOTAL	271	100
Mean	3.8192	

Table: 21 illustrates the variable Cyber Security and Cyber Crimes Act No. 2 of 2021 in measuring the most effective policy/law in mobile money fraud control. 89 respondents representing 32.8% strongly agree, 56 respondents representing 20.7% agree and 116 respondents representing 42.8% were not sure. Meanwhile, there were 8 respondents representing 2.9% who disagree and 2 respondents which is 0.7% strongly disagree. The sum total of the respondents were 271. The mode of the respondents was 116(42.8) not sure and therefore with the mean of the Cyber Security and Cyber Crimes Act No. 2 of 2021 as the most effective policy being 3.8192 above the neutral in the Likert scale, it shows that most respondents were not sure as to the Cyber Security and Cyber Crimes Act No. 2 of 2021 being the most effective policy control measure in curbing mobile money fraud, therefore the perception is relatively high that most of the respondents are not sure about it.

4.2.19 National Cyber Security Policy of 2021

Table 22: Respondents distribution by the most effective policy/law being National Cyber Security Policy of 2021

	Frequency	Percentage
Strongly Agree	55	20.3
Agree	53	19.6
Not Sure	153	56.5
Disagree	6	2.2
Strongly Disagree	4	1.5
TOTAL	271	**100**
Mean	3.5498	

Source: Field data, 2024

Table: 22 illustrates the variable National Cyber Security Policy of 2021 in measuring the most effective policy/law in mobile money fraud control. 55 respondents representing 20.3% strongly agree, 53 respondents representing 19.6% agree and 153 respondents representing 56.5% were not sure. Meanwhile, there were 6 respondents representing 2.2% who disagree and 4 respondents which is 1.5% strongly disagree. The sum total of the respondents were 271. The mode of the respondents was 153 (56.5) not sure and therefore with the mean of the Cyber Security and Cyber Crimes Act No. 2 of 2021 as the most effective policy being 3.5498 above the neutral in the Likert scale, it shows that most respondents were not sure as to the National Cyber Security Policy of 2021 being the most effective policy control measure in curbing mobile money fraud, therefore the perception is relatively high that most of the respondents are not sure about it.

4.2.20 Correlation of gender and frequency of employing control measures

The study further sought to establish the degree of association between gender and frequency of employing control measures. The bivariate correlation test was conducted and the results are depicted below.

Table 23: Pearson Moment bivariate correlation gender and frequency of employing control measures.

Source: Cohen (1992) proposed the following guidelines for the interpretation of correlation coefficient.

Correlations			
		Gender	How often do you implement the control measures
Gender	Pearson Correlation	1	.065
	Sig. (2-tailed)		.285
	N	271	271
How often do you implement the control measures	Pearson Correlation	.065	1
	Sig. (2-tailed)	.285	
	N	271	271

Source: Field data, 2024

**Correlation is significant at the 0.01 level (2 tailed).

Table 24: Coefficient and Association Correlation coefficient value

Coefficient and Association Correlation coefficient value	Association
-0.3 to +0.3	Weak
-0.5 to -0.3 or 0.3 to 0.5	Moderate
-0.9 to -0.5 or 0.5 to 0.9	Strong
-1.0 to -0.9 or 0.9 to 1.0	Very Strong

Table 24 above illustrates the relationship between gender and frequency of implementing the control measures. The results indicate the Pearson Correlation of 0.65 and Sig. (2-tailed) of 0.285. The total number of respondents was 271.

4.2.21 Correlation of level of education and frequency of employing control measures

The study further sought to establish the degree of association between age range and frequency of employing control measures. The test results show are shown in table 25 below.

Table 25: Pearson Moment bivariate correlation age range and frequency of employing control measures.

**Correlation is significant at the 0.01 level (2 tailed).

Source: Field data, 2024

4.2.22 Multi Variate Regression Analysis Model

Correlations			
		What_is_your_level of education	How often do you implement the control measures
What_is_your_level of education	Pearson Correlation	1	-.040
	Sig. (2-tailed)		.510
	N	271	271
How often do you implement the control measures	Pearson Correlation	-.040	1
	Sig. (2-tailed)	.510	
	N	271	271

Below is the model summary of the regression of frequency of employing the control measures and ICT proficiency, age range, gender and level of education.

Table 26: Model summary showing correlation coefficient and coefficient of determination

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.276[a]	.076	.062	.807
a. Predictors: (Constant), How would you rate your ICT proficiency, Age Range, Gender, What_is_your_level of education				

Source: Field data, 2024

R is Correlation coefficient of .276

R Square is 0.76 or 76%

Adjusted R2 is 0.062

Std. Error of 0.807

The above model summary in Table 26 has a correlation coefficient of .276, Coefficients of determination (R2) is 0.76 or 76%. The 76% increase or decrease in ICT proficiency, age range, Gender and level of education affect employment of control measures by 76%. The adjusted R-Squared is a modified version of Squared that has been adjusted for a number of predictors in the model. The adjusted R Squared of 0.62 will only increase only if the new term improves the model more than would be expected by chance. It decreases when a predictors improves the model by less than expected by chance. The Std. Error of the estimate was 0.807.

Table 27: Table of beta Coefficients

Coefficients[a]					
	Unstandardized Coefficients		Standardized Coefficients		
Model	B	Std. Error	Beta	t	Sig.
(Constant)	3.246	.244		13.297	.000
Gender	.036	.076	.028	.470	.639
Age Range	-.173	.051	-.204	-3.406	.001
What_is_your_level of education	-.019	.022	-.054	-.882	.379
How would you rate your ICT proficiency	-.148	.046	-.197	-3.184	.002
a. Dependent Variable: How often do you implement the control measures					

Table 27 illustrates the table of coefficients. The independent variables include ICT proficiency, Age Range, Gender and level of education while the dependent variable was frequency of employing the control measure(s). The Unstandardized Coefficients (B) are the regression coefficients. The regression equation is as follows,

Implementing control measures = 3.246 + 0.036 + (- 0.173) + (- 0.019) + (- 0.148) (Equation 1)

Table 27 illustrates the table of coefficients, From the Unstandardized Coefficients, the constant was 3.246, Standard error for constant was 0.244 and the t-test for constant was 13.297. The 2 sided Observed level of significance was 0.000

From table 27 above, the intercept (constant) is 3.246, the coefficient for gender is 0.036, suggesting that for a one-unit increase in gender, the dependent variable frequency of implementing the control measures increases by 0.036 units, on the other hand, the coefficient for age range is -0.173, suggesting that for a one-unit increase in age range, the dependent variable decreases by 0.173 units, and the coefficient for level of education is -0.019, suggesting that for a one-unit increase in education level, the dependent variable decreases by 0.019 units, holding all other variables constant. In addition, the coefficient for ICT proficiency is -0.148, suggesting that for a one-unit increase in ICT proficiency, the dependent variable decreases by 0.148 units, holding all other variables constant.

The variables age range and ICT proficiency have p-values of .001 and .002, respectively, indicating they are significant while Gender and level of education do not seem to be significant given their higher p-values 0.639 and 0.379 respectively.

4.2.23 Regression standardised Normal P-P Plot

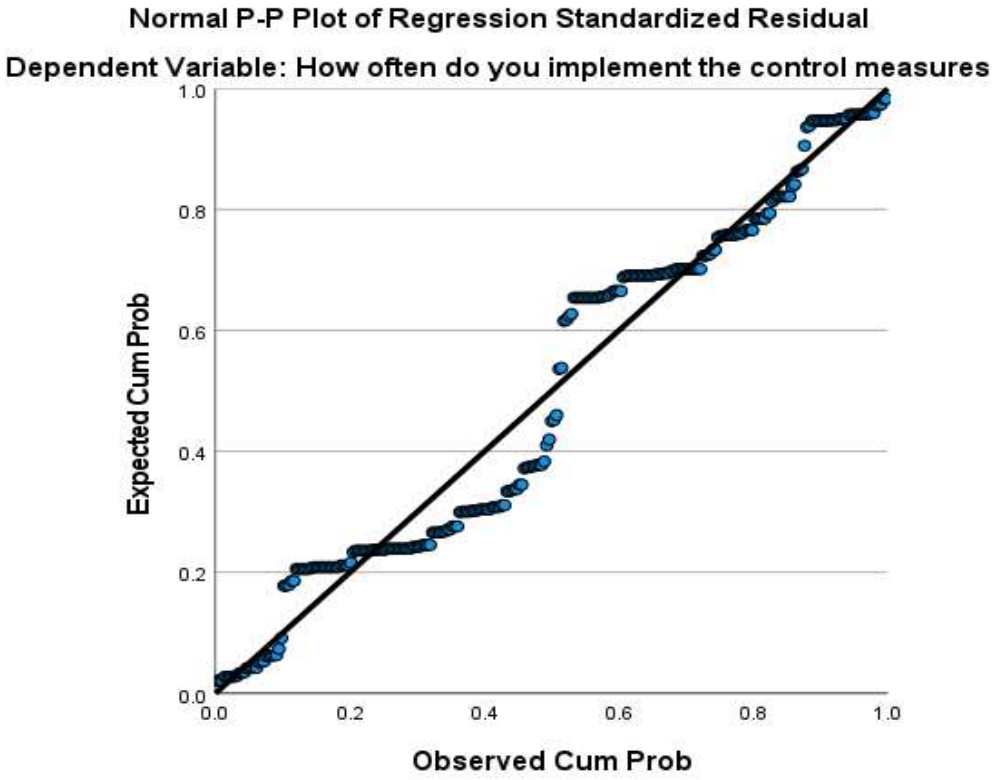

Figure 5: Regression standardised Normal P-P Plot

Figure 5 illustrates the relationship between the independent Variable age range and dependent employing control measures. The coefficient correlation indicates 0.276 which means the relationship is a positive correlation. The outcome of 0.276 is a strong coefficient and indicates a strong relationship.

4.2.24 Cronbach's Alpha Test

Table 28: Table of Reliability statistics testing internal consistency of data

Source: Field data, 2024

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No of Items
.744	.757	16

A Cronbach alpha test was carried out to test the reliability of the test items for internal consistency. The Cronbach alpha produced a reliable measure of .744 which is a moderate Indicator and the standardized items of 0.757.The total number of the test items were 16.

4.2.25 Summary

This Chapter was looking at the Presentation of Findings. The findings from the presentation were arranged in themes and sub themes in relation to the Objectives**.** It looked at the biographical data of the respondents, and the themes and sub themes included; types of mobile money fraud, most useful policy/law, effectiveness of the policies/laws, enhancement of mobile money security by using technology, apprehension/arresting of offenders, Policies/Laws used to combat mobile money fraud, most useful policy/law, effectiveness of the policies/laws, measures to combat mobile money fraud, control measures used in combatting mobile money fraud, implementing the control measures, most effective control measure, perception on the most effective control measure, sensitization is the most effective control measure, sensitization and training of mobile money agents, fraud detection by being alert, types of control measures that are employed in combatting mobile money fraud

CHAPTER V

DISCUSSION OF FINDINGS

5.0 Overview

Chapter five discusses the findings from chapter four and provides a critical analysis. The focus of this chapter is to analyse the research findings in order to provide answers to the research questions.

5.1 Types of control measures employed in combatting mobile money fraud

The study sought to find out the types of control measures that are used in combatting mobile money fraud. Overall, the respondents knew at least one type of control measure used in combatting mobile money fraud. 115 (32.6%) disclosed that they were aware about the programs meant to sensitize the users. This is in line with the literature and responses from the stakeholders who indicated that they conduct sensitizations to the users of mobile money services on how to detect fraudsters and ways of protecting themselves from such criminality. One of the messages that is frequently emphasised is the need not to share personal identification numbers (PINs) with other people. In the same regard, 23 (6.5%) stated that they attended trainings and sensitization programs meant for the mobile money agents. This target group belonged to the mobile money agents. These results are similar to those found by Akomea-Frimpong, et. al, 2020). This shows that training is a very important aspect in the securing of mobile money.

On the other hand, the majority stated that they combat mobile money fraud by simply being alert as users and mobile money agents. These provided the critical aspect of undertaking certain measures as an individual or user to ensure that the fraudsters do not take advantage of them. Further, 31 (8.8%) stated that mobile money fraud could only be combatted by enhancement of mobile money security by using technology. The role of technology that is embedded in the mobile money system to detect and combat fraud, cannot be over-emphasised as the advancement in technology has led to the improvement in the security of financial platforms, making it imperative for the MNOs and the Regulator to invest in such technologies.

Those that indicated that apprehending the offenders is the best way to curb the scourge of mobile money fraud are alive to fact that there is need for criminality in the country to be dealt with by the law, and in order to serve as a deterrent measure to would be criminals. In addition those that stated that they report the fraudsters to the relevant

authorities and in so doing curb mobile money fraud show results similar to the studies that was conducted by (Interpol, 2020, GSMA, 2024).

Accordingly, the type of control measures that are employed in combatting mobile money fraud are two-fold; those that are carried out by the institutions involved in the regulation, provision and enforcement of laws in the mobile money sector, and those that are dependent on the users and mobile money agents. In line with the theoretical framework adopted by this study, transmission of the sensitization messages is as important as the actual implementation of what is being recommended in there if the threat is to be averted (Joshua, (2015).

Therefore, in answering the question on the types of control measures used in curbing mobile money fraud, the identified ones include sensitization of the users, training and sensitization of the mobile money agents, enhancement of mobile money security by using technology by the network providers and the Regulator, fraud detection by the alertness of the users, apprehending the offenders and as well as reporting the perpetrators to the relevant authorities.

5.1.1 Types of mobile money fraud

This variable was very important in the study in that knowledge of the types of fraud is essential in determining the control measures that can be implemented in order to curtail it. The majority of the respondents were able to identify the major types of mobile money fraud. In the study, those identified include sim card swap, identity theft, fake promotions. On the other hand, the majority 199 (35.3%) identified fake mobile money transfers, while others cited phishing and fake product/service delivery. From this, the most notable type of mobile money fraud was identified to be fake mobile money transfers.

The above findings were in line with other studies such as (Akomea-Frimpong, et.,al 2020, Interpol, 2020, GSMA, 2024), who found that fake money transfer a common mobile money fraud, which involves the perpetrators sending fake messages to unsuspecting users and then calling them back to reverse the transaction indicating that the money was sent wrongly to them, when in fact no money was sent. In the same vein, just like the study that was carried by Zimba (2022), the issue of fake promotions also came out prominent. In this type, the perpetrators call a random number claiming mainly that they were from the Mobile network provider, and that the MNO had been running a promotion and the user had won something when in fact not, then they would be asked

to share their personal details such as PIN leading to the criminal to syphon money from the user's account.

The respondents also added other types of mobile money fraud and the majority indicated obtaining money by false pretences and fake job advertisements, where the perpetrators would provide a number to which the victims were to send money to. Further, mainly those from the stakeholder institutions added unsolicited electronic messages as another type of mobile money fraud. This is a situation where a criminal sends a message to a user soliciting money from them by sometimes pretending to be in a very desperate situation that needs their help. This is also confirmed in a study that was carried out by Mudiri (2021).

5.2 Extent of implementation of the control measures

The study also sought to determine the extent to which the control measures used in curbing the scourge of mobile money fraud are implemented. This was premised on the fact that in order to succeed, where the measures exist, it is always very important to correctly implement them. The variables below were used to measure the extent of implementation of the control measures.

5.2.1 Frequency of implementing the measures

The study established that most of the respondents do implement the measures frequently in their quest to curb mobile money fraud. When asked on whether the respondents employed any control measures to combat mobile money fraud, the majority 191 (71%) indicated that they did, while 70 (26) stated that they do not undertake any control measures. The majority of the respondents who were the ordinary users stated that they do their part by implementing the measures that are outlined in the sensitization messages that they receive from the other stakeholders in the mobile money business. This is in line with the theoretical framework, which argues that people tend to carry out measures to protect themselves from a perceived threat when they perceive the severity of the threat as well as benefits and costs of undertaking the preventive measure (Boss et al., 2015).

When asked to elaborate on the control measures that are carried out, the institutions pointed out sensitization as well as internal controls that they implement in order to curb mobile money fraud. Of particular interest were the respondents from the Law enforcement agency who stated that "for us, the measures we carry out to curb mobile

money fraud are mainly arresting the criminals of this kind of fraud and taking them to court as this is our mandate as Zambia Police. We also conduct sensitization programs to the public on radio and through workshops". This correlates with the findings that emanated from the study that was undertaken by Interpol (2020).

5.2.2 Extent to which gender is correlated with employing control measures

From the presentation of the results, gender is correlated with frequency of employing control measures to combat mobile money fraud. The results indicate correlation coefficient of 0.65. The coefficient of 0.65 indicates a strong association between gender and frequency of employing the control measures. According to Cohen (1992) if the Correlation coefficient falls between-0.9 to -0.5 or 0.5 to 0.9, it indicates a strong association between the variables. The strong association could be attributed to the advancement in technology, which has enabled many people to engage in technologically enhanced environments. In addition, most of the participants were the young people aged 20 to 30 and these are the same age group called the millennials who are very conversant with technological advancements particularly regarding cell phones. The results indicate the Pearson Correlation of 0.65 and Sig. (2-tailed) of 0.285. The total number of respondents was 271.

5.3 Control measures to combat mobile money fraud

When asked on whether the respondents employed any control measures to combat mobile money fraud, the majority 191 (71%) indicated that they did, while 70 (26%) stated that they do not undertake any control measures. In order to control mobile money fraud, it is important that whatever measures that are put in place are actually ultimately implemented by the various stakeholders in the sector. As stated above, most of the respondents indicated that they actually implement the control measures, however, it is important to ascertain why the cases have continued to rise, hence posing a question on whether such measures are adequate and if they are, are they being implemented correctly.

The major tenets of the Preventive Motivation Theory include the belief that the adaptive response will work, implying that taking the protective action will be effective in protecting oneself or others; the perceived ability of the person to actually carry out the adaptive response; the costs associated with taking the adaptive coping response (Floyd et. al, 2000). These resonate well with one's choice of whether to undertake the

control measure as established in the above result. Those that choose to take the control measures are less likely to fall victim to the schemes of the fraudsters.

5.3.1 Perception on the most effective control measure

As regards the most effective control measure used to curb mobile money fraud, the majority108 (39.8%) respondents chose sensitization of the users, while 52 (19.2%) commended apprehension/arresting of offenders as the most effective control measure, and least at 7 (2.7%) were not sure about which of the control measures they could indicate as the most effective in curbing mobile money fraud. This is also backed up by the report by GSMA (2024). It is worth to note that those that opted for apprehending the fraudsters appear to have been victims of such fraud, as they were emotional as they advocated for stiffer punishment for the offenders. One stated "it is very painful to lose money just like that", while others also added "these criminals should be killed".

When measured on the Likert scale, out of the overall score of 1,355, sensitisation of the users scored 600 with the respondents strongly agreeing that indeed it is the most effective control measure. This variable is important in determining the priority areas where the relevant authorities may channel their resources to in their quest to curb mobile money fraud. Therefore, sensitization was found to be the most effective control measure used in combatting mobile money fraud. This finding tarries with the results of studies that were done by (Interpol, 2020, GSMA, 2024).

As regards the views of the respondents on why they opted for sensitisation as the most effective control measure in the fight against mobile money fraud, the majority stated that it is the only way that makes the users to know about the various mobile money crimes. They also stated that sensitization helps both the users and the agents to be alert. One respondent stated "with sensitization, both the mobile money agent and users become aware of existence of various mobile money frauds and therefore will be alert to suspecting frauds at all times". Another respondent also argued that "educating users will make them to be aware and alert in instances where they receive anything unusual". Still another indicated "The authorities need to take a further step in sensitizing the public because they are in a vulnerable state and once educated they can be able to fight against mobile money fraud". On the other hand, majority of the respondents from the law enforcement sector cited sensitisation as the most common mode of control measure. One stated, "sensitisation helps to prevent crime and prevention is always better that cure".

5.4 Policy best practices/Laws used to combat mobile money fraud

The study further sought to determine the policy best practices in the fight against mobile money fraud. This was because it was ascertained through literature that such type of crimes just like the mainstream cybercrimes, are global and regional issues. As such, the best policy practices are important in benchmarking with other countries. As such, various variables were brought out to achieve the aforementioned purpose.

5.4.1 Knowledge about the existing policies and laws

In order to ascertain the best policy practices, it was important to determine if the respondents knew about the existence of such instruments. The overall score for the respondents on the policies/laws used to combat mobile money fraud, the Cyber Security and Cyber Crimes Act No. 2 of 2021 obtained the majority score while National Information and Communication Technology Policy 2023, yielded the least. On the other hand, 38 (14%) indicated the National Cyber Security Policy of 2021, while 29 (10.7%) were not aware of any policy/law in the study sector.

The lack of knowledge on the existing policies about the control of mobile money fraud can be attributed to the illiteracy levels existing in the Country as "according the Demographic Health Survey (2018), 66% of women and 82% of men aged 15 - 49 are literate. This implies that 18% of men and 44% of women aged 15 – 49 are classified as illiterate" (PMRC, 2022: 2). This is in tandem with the results of this study as indicated in table 2, where most of the respondents were moderately educated. The implication is that such category of the people are less likely to acquaint themselves with reading issues such as laws and policies, which are usually written in English.

While most of the respondents were aware about the existence of the policies and laws in the mobile money sector, the number of those who were not aware at 10.7% was quite significant. By nature, it is important that people in a given society should be aware about the existence of such tools in order to use them when need arises and propose amendments or changes where possible. The other cause of not knowing the existing of the policies and laws aimed at controlling mobile money fraud can be attributed to the low reading culture in Zambia as found by (Kafusha et.al, 2021).

When the respondents were asked on their knowledge of the policies and laws that exist in the mobile money sector, the majority of them stated that they were not sure about such policies and laws. They specifically stated that in fact they were not aware about

the existence of such policies. One stated “Iam not even aware that there are laws that deal with mobile money fraud”. In addition, another indicated that “Iam not sure whether or not such policies even exist”. One mobile money agent also added “training of agents can help to reduce mobile money fraud as many are unaware about this Act”. This situation calls for the stake holders to take keen interest and educate the public of the available instruments that are meant to curb the scourge of fraud in mobile money.

5.4.2 Most useful policy/law

This variable was one of those used to measure the interaction or knowledge of the existence of the key policies in the mobile money sector. 84 (31.0%) cited the Cyber Security and Cyber Crimes Act No. 2 of 2021 as the most useful one, while the least score was National Information and Communication Technology Policy 2023. On the other hand, 43 (15.9%) indicated that none of the identified policies and laws was useful in curbing mobile money fraud. Those who argued that none of the above was useful could be attributed to the lack of knowledge as well as non-interaction with the policies and laws.

For the MNOs, the Data protection ACT is a very useful instrument in fighting mobile money fraud due to its emphasis on the protection of personal data. For instance, section 48 of the Act requires the appointment of a Data Protection Officer to be responsible for the protection of personal data. This is in line with the MNOs such as Airtel Zambia who have developed the Data Privacy & Protection Policy to secure data on Airtel Mobile Money (Airtel, 2023). Their policy on the protection of personal data is quite significant in that it addresses all areas that impact critical information protection. For instance, emphasises system protection by using strong encryption algorithms as well as restrict physical access to areas where personal data is stored such as server rooms.

When probed further to explain their choice of the policy or law as the most useful in fighting the scourge, the majority stated that the Cyber Security and Cyber Crimes Act No. 2 of 2021 was the law that was used in the apprehension or arresting of the offenders. One stated, “this is the same law that the police use when someone is reported to be scammer of mobile money and they are caught by the Police”. Another respondent from the Police stated “Cyber Security and Cyber Crimes Act No. 2 of 2021 is one of the most utilized as section 53 clearly explains identity related crimes and section 62 also explains unsolicited electronic messages”. Those that had chosen the Data Protection Act as the most useful one simply looked at its role in protecting of data. One

respondent stated “the Data Protection Act is the law that simply protects our data from being stolen by the criminals”.

5.4.3 Effectiveness of the policies/laws

In order ascertain the adequacy of the control measures, it was apparent to also obtain the respondents’ perceptions on the effectiveness of the existing policies and laws in controlling mobile money fraud. The results from the Likert scale show that most of respondents were not sure at 50.4% and those that strongly disagreed represented 0.8%. As indicated above, most of the respondents were not sure on the effectiveness of the policies in addressing issues related to mobile money fraud. This means that the impact of such policies and laws may not be felt by the users of the mobile money.

When the views of the respondents on the effectiveness of the policies and laws in curbing mobile money fraud were sought, majority of them just stated that they were just not sure. Some out rightly stated that that they have not even heard about such policies and laws. One of the respondents stated “it is my first time hearing about the existence of the law on cyber-crime”. Another also disclosed that “Iam simply not aware about the policies and the laws”. This shows an inherent problem given the urban status of Lusaka, if most people are not aware about the policies and laws that seek to protect them, then it may be worse in the rural areas due to the information gap.

The above situation can be attributed to poor reading culture among the citizens and the considerable illiteracy levels as found by (Kafusha et.al, 2021; Akomea-Frimpong, et.al, 2020). The implication is that government should deliberately sensitive the citizens on most of the policies and laws as it also works to reduce the illiterate levels and encourage citizens to be reading a lot.

5.5 Summary

This Chapter was looking at the discussion of the findings. The first objective was to establish the types of control measures used in combatting mobile money fraud. The results indicate that those identified include sensitization of the users, training and sensitization of the mobile money agents, enhancement of mobile money security by using technology by the network providers, fraud detection by the alertness of the users, apprehending the offenders and as well as reporting the perpetrators to the relevant authorities. When measured on the Likert scale, out of the overall score of 1,355,

sensitisation of the users scored 600 with the respondents strongly agreeing that indeed it is the most effective control measure.

The second objective was to determine the extent of implementing the control measures When asked on whether the respondents employed any control measures to combat mobile money fraud, the majority indicated that they did, while 70 (26%) stated that they do not undertake any control measures.

The third objective was to establish policy best practices in the mobile money sector. When the views of the respondents on the effectiveness of the policies and laws in curbing mobile money fraud were sought, majority of them just stated that they were just not sure. The Cyber Security and Cyber Crimes Act No. 2 of 2021 was found to be the most useful law in in combatting mobile money fraud. This was also backed up with the finding that apprehending/arresting the fraudsters was the most effective way of combatting mobile money fraud in Lusaka District, scoring 137 out of 600 among those who strongly agree, and 76 from a score of 419 among those who agree. When probed further to explain their choice of the policy or law as the most useful in fighting the scourge, the majority stated that the Cyber Security and Cyber Crimes Act No. 2 of 2021 was the law that was used to in the apprehension or arresting of the offenders.

CHAPTER VI

CONCLUSION AND RECOMMENDATIONS

6. 0 Overview

The previous Chapter looked at the Discussion of findings of the research study. Chapter five linked the research objectives to literature review and the theoretical framework in order to provide answers to the research questions. Chapter six presents conclusion of the main findings in the study based on the three objectives which were to determine the types of control measures employed in combatting mobile money fraud, to establish the extent of implementing control measures of combatting mobile money fraud and to establish policy best practices in combating mobile money fraud in Lusaka District.

6.1 CONCLUSION

The findings from the specific objectives are summarised below using the scores based on the frequency obtained on each variable in order to arrive at the adequacy of the control measures in combatting mobile money fraud.

6.1.2 Types of control measures employed

The research results indicated the findings on the type of control measures that are used in combatting mobile money fraud, where, out of an overall score of 355, sensitization of the users of mobile money scored 115 (32.6%) while trainings and sensitization programs meant for the mobile money agents 23 (6.5%). On the other hand, 76 (21.5%) stated that combatting mobile money fraud requires one to simply being alert as a user or mobile money agent. Further, enhancement of mobile money security by using technology by the MNOs scored 31 (8.8%) and apprehending the offenders as a control measure scored 36 (10.2%) and in line with this, 72 (20.4%) score was for reporting the fraudsters to the relevant authorities as a measure to curb mobile money fraud.

6.1.3 Extent of implementing control measures

The research findings on this objective shows that most of the respondents do implement the control measures it. From the overall score of 271, those that frequently implement the control measures scored 27 (9.6%), while the majority scored 114 (42.1%) representing those that frequently do so. On the other hand however, 98

(36.2%) rarely do so, and 32 (11.8%) stated that they do not implement any control measure at all. Therefore, as regards this objective, the extent of implementation of the control measures was found to be 42.1% and the control measure that was recommended was apprehension of the offenders which scored 137 out of 600 and 76 out of 419 among those that strongly agree and agree respectively.

6.1.4 Policy best practices in mobile money fraud control

On this particular objective, the respondents' perception on the policy best practices were sought by considering the existing policies and laws in controlling mobile money fraud, where the total score was 1,355. Out of this that strongly agree that the existing policies and laws were adequate scored 318 representing 23.5% and those who agreed scored 320 representing 23.6%. On the other hand, those who were not sure were 683 representing 50.4% and those that disagreed were 23 representing 1.7%, while those who strongly disagreed were 11 representing 0.8%. The implication of the findings on this issue is that majority of the people in Lusaka District representing 50.4% are not sure on the adequacy of the policies and laws put in place to curb mobile money fraud in Lusaka**.**

6.1.5 Adequacy of the control measures

The purpose of this study was to investigate the adequacy of the control measures in combatting mobile money fraud in Lusaka District. From the findings, this purpose has been achieved as the control measures that have been put in place have been found to be adequate. The major problem lies on the implementation of such measures by the users and the organisations that are charged with ensuring that the mobile money sector is protected from fraudsters. On the part of the respondents, only 42.1% were found to be implementing the control measures, while the rest either rarely did or do not do so at all. The views of those that implement the measures were that they are adequate in controlling mobile money fraud, but only need to be implemented fully and enhanced in order to achieve the objectives that they are meant to.

6.2 Recommendations

From the study, the following recommendations have been brought out:

(i) The various stake holder organizations such as ZICTA, MNOs and Law Enforcement Agencies should intensify their sensitisation programs and even conduct joint campaigns on how the users of mobile money services could protect themselves from the fraudsters.

(ii) The Government, ZICTA, MNOs and the Law Enforcement Agencies should intensify their sensitization campaigns to members of the general public on the various policies and laws that exist on cybercrimes in general and mobile money in particular.

(iii) Parliament in consultation with stakeholders should amend the laws in order to stiffen the punishment that is rendered to the fraudsters upon conviction by the courts of law.

(iv) The MNOs should be compelled to invest in technologies that can enhance mobile money security within the architecture of the system. In addition, they need to enhance security within their internal structures, among the members of staff that deal with mobile money services in order to avoid the compromise of personal data.

6.2.2 Recommendations for future research

The findings from the study showed that most of the mobile money users do not implement the control measures put in place to curb mobile money fraud. The implication of this action is that the cases of mobile money fraud will continue to rise as long as the users do not take appropriate action to protect themselves by following the guidelines and implementing the recommended measures.

The study recommends that further studies be conducted on the factors that make most of the mobile money users not to fully implement the control measures meant to curb of mobile money fraud.

REFERENCES

Akomea-Frimpong, Isaac & Andoh, Charles & Akomea-Frimpong, Agnes & Dwomoh-Okudzeto, Yvonne. (2020). *Control of fraud on mobile money services in Ghana: an exploratory study*. Journal of Money Laundering Control. 22. 300-317. 10.1108/JMLC-03-2018-0023.

Airtel(2023) Airtel Mobile Commerce Zambia Data Privacy and Protection Policy https://www.airtel.co.zm/assets/pdf/Airtel-Mobile-Commerce-Zambia-Limited-Privacy-Policy.pdf. Accessed on 25th January, 2024.

Ali, G Ally, Dida M, and Elikana Sam A. (2020) *Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda.* Information. 2020; 11(6):309. https://doi.org/10.3390/info11060309. Accessed on 17th September, 2023

Amuomo, Nixon and Odoyo, Collins. (2020). *Ethnography, Its Strengths, Weaknesses and Its Application in Information Technology and Communication as a Research Design.* Computer Science and Information Technology. 8. 50-56. 10.13189/csit.2020.080203. Accessed on 17th September, 2023

Botchey, Francis Effirim, Zhen Qin, and Kwesi Hughes-Lartey. 2020. "Mobile Money Fraud Prediction—A Cross-Case Analysis on the Efficiency of Support Vector Machines, Gradient Boosted Decision Trees, and Naïve Bayes Algorithms" *Information* 11, no. 8: 383. https://doi.org/10.3390/info11080383. Accessed on 27th September, 2023

BOZ (2020) *FinScope Zambia 2020 Survey Report.* https://www.boz.zm/FinScope-2020-Survey-Report.pdf. Accessed on 17th September, 2023

BOZ (2023) National Payment Systems In Zambia, Annual Report For The Year 2022. https://www.boz.zm/2022NationalPaymentsSystemsAnnualReport_FINAL.pdf. Accessed on 18th September, 2023

Bruijn, de M.E., Butter, C. I. and Fall S. A. (2017) *Ethnographic study on mobile money.*

In cooperation with the Mobile Money Research Team & IFC-MasterCard Partnership for Financial Inclusion https://documents1.worldbank.org/curated/en/283401531295554699/pdf/128221-WP--December-2017-PUBLIC.pdf. Accessed on 18th October, 2023

Cambridge Intelligence (2023) Visualizing a timeline of mobile money fraud Warren Fitzhenry, 18th January 2022. https://cambridge-intelligence.com/mobile-money-fraud/. Accessed on 17th September, 2023

Chipa, Natalie & Mwanza, Bupe. (2021). *Factors Impeding Mobile Money Expansion in Zambia.* International Journal of Engineering and Management Research. 11. 178-186. 10.31033/ijemr.11.1.24. Accessed on 17th September, 2023

Clubb, Audrey & Hinkle, Joshua. (2015). *Protection motivation theory as a theoretical framework for understanding the use of protective measures.* Criminal Justice Studies. 28. 10.1080/1478601X.2015.1050590.

Cochran, W. G. (1977). Sampling techniques (3rd ed.). New York: John Wiley & Sons. https://www.opalco.com/wp-content/uploads/2014/10/Reading-Sample-Size1.pdf. Accessed on 17th September, 2023

Conner & Norman (2015) in Clubb, Audrey & Hinkle, Joshua. (2015). *Protection motivation theory as a theoretical framework for understanding the use of protective measures.* Criminal Justice Studies. 28. 10.1080/1478601X.2015.1050590. Accessed on 17th September, 2023

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). *A meta-analysis of research on protection motivation theory.* Journal of Applied Social Psychology, 30, 407–429. Fox, K., Nobles, M., & Piquero, A. R. (2009). Gender, crime victimization and fear of crime. Security Journal, 22, 24–39.

GSMA (2023) The state of the industry report on mobile money 2023. https://www.bing.com/search?FORM=SWBW15&q=GSMA%20(2023)The%20state%20of%20the%20industry%20report%20on%20mobile%20money%202023. Accessed on 25th September, 2023.

GSMA (2024) Mobile money fraud typologies and mitigation strategies. www.gsma.com/mobilemoney. Accessed on 20th March, 2024.

IMF (2022) Fintech: Financial Inclusion or Exclusion? Yoke Wang Tok and Dyna Heng. IMF Working Paper Institute of Capacity Development, WP/22/80. https://www.imf.org/-/media/Files/Publications/WP/2022/English/wpiea2. Accessed on 7th September, 2023

Interpol (2020) Mobile money and organized crime in Africa. https://www.interpol.int/en/content/download/15457/file/2020%2007%2015%20PUBLIC%20VERSION%20-%20Strategic%20Analysis%20Report/. Accessed on 17th September, 2023

Iyer, Swarnalakshmi M., "A Case Study on Monetary Fraud in a Cashless Economy" (2017). Open Access Theses. 1289. https://docs.lib.purdue.edu/open_access_theses/1289. Accessed on 7th September, 2023

Kabala, Edna, Mapoma, Rosemary, Nalutongwe, Chitimba, Muyani, Diana and Lungu, John (2021) *"An Ethnological Analysis of the Influence of Mobile Money on Financial Inclusion: The Case of Urban Zambia,"* Zambia Social Science Journal: Vol. 7 : No. 1, Article 4. Available at: https://scholarship.law.cornell.edu/zssj/vol7/iss1/4. Accessed on 19th September, 2023

Kafusha, Mary & Mwelwa, Jane & Mkandawire, Sitwe & Daka, Harrison. (2021). READING CULTURE IN ZAMBIA: PERSPECTIVES OF SELECTED HOUSEHOLDS OF ZAMBIA ON THEIR READING PRACTICES. 5. 80-106. https://www.researchgate.net/publication/357735513_READING_CULTURE_IN_ZAMBIA_PERSPECTIVES_OF_SELECTED_HOUSEHOLDS_OF_ZAMBIA_ON_THEIR_READING_PRACTICES/citation/download. Accessed on 28th December, 2023.

Kanobe, Fredrick and Kelvin Joseph Bwalya. 2021. *"Snags in Mobile Money in Developing Economies."* Electronic Journal of Information Systems in Developing Countries.

Milne, S., Sheeran, P., & Orbell, S. (2000) Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. In Clubb, Audrey & Hinkle, Joshua. (2015). *Protection motivation theory as a theoretical framework for understanding the use of protective measures.* Criminal Justice Studies. 28. 10.1080/1478601X.2015.1050590.

Mogaji, Emmanuel & Nguyen, Nguyen Phong (2022) "*The dark side of mobile money: Perspectives from an emerging economy,"* Technological Forecasting and Social Change, Elsevier, vol. 185(C).

MoneyFM Radio Business Radio (2022) *ZICTA heightens awareness about mobile money scammers* https://www.moneyfmzambia.com/2022/02/03/zicta-heightens-awareness-about-mobile-money-scammers/. Accessed on 24th September, 2023

Mudiri, Joseck (2021) Fraud in Mobile Financial Services. Microsave https://www.microsaveindiafoundation.net/wp-content/uploads/2021/04/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf. Accessed on 14th December, 2024

Mwila, Ali & Lubobya, Charles (2019). *An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia.* 8. 10.15680/IJIRSET.2019.0812041.

National Assembly of Zambia (2022) *Information brief on cyber security and cybercrime trends in Zambia*, Research Department, September, 2022.

Okello Candiya Bongomin, George & Ntayi, Joseph. (2020). *Mobile money adoption and usage and financial inclusion: mediating effect of digital consumer protection. Digital Policy, Regulation and Governance. A head-of-print.* 10.1108/DPRG-01-2019-0005. https://nru.uncst.go.ug/xmlui/bitstream/handle/123456789. Accessed on 17th September, 2023

Peacock Morris Ayodele."An Analysis of the Potential Risk and Fraud Involved in Mobile Money Transaction in Freetown Sierra Leone." J Telecommun Syst Manage 11 (2022) : 10. https://www.hilarispublisher.com/open-access/an-analysis-of-the-potential-risk-and-fraud-involved-in-mobile-money-transaction-in-freetown-sierra-leone.pdf. Accesed on 17th February, 2024

Phiri, Mwiza Norina; Banda, Dani Eliya. *Emerging mobile phone-based social engineering cyber-attacks in the Zambian ICT Sector*.International Journal of Advanced Studies in Computers, Science and Engineering; Gothenburg Vol. 8, Iss. 2, (2019): 13-20.

Policy Monitoring and Research Centre (2022) 2022 International Literacy Day. https://pmrczambia.com. Accessed on 13th January, 2024.

Razaq, Lubna & Ahmad, Tallal & Ibtasam, Samia & Ramzan, Muhammad & Mare, Shrirang. (2021). "We Even Borrowed Money From Our Neighbor": Understanding Mobile-based Frauds Through Victims' Experiences. Proceedings of the ACM on Human-Computer Interaction. 5. 1-30. 10.1145/3449115.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In Clubb, Audrey & Hinkle, Joshua. (2015). *Protection motivation theory as a theoretical framework for understanding the use of protective measures.* Criminal Justice Studies. 28. 10.1080/1478601X.2015.1050590.

Sinkala, Nambela (2023) Mobile Money and SME Growth: A Zambian Perspective. Journal of Business and Strategic Management ISSN 2520-0402 (online) Vol.8, Issue No.7, pp 1 – 18, 2023. https://orcid.org/0009-0009-1668-3356. Accessed on 14th January, 2024

Somasundaram, M. & Litt, D. (2020). A Study on perception of consumers towards Digital payment. https://www.researchgate.net/publication/342178714_A_STUDY_ON_PERCEPTION_OF_CONSUMERS_TOWARDS_DIGITAL_PAYMENT/citation/download. Accessed on 17th September, 2023

Uddin, Md & Chowdhury, Mohammed & Zahin, Fariha. (2022). Effects of fraud call on mobile banking transaction: Empirical evidance from Bangladesh. https://www.researchgate.net/publication/359905350_Effects_of_fraud_call_on_mobile_banking_transaction_Empirical_evidance_from_Bangladesh/citation/download. Accessed on 14th September, 2023

Volodymyr Mishchenko, Svitlana Naumenkova, Andrii Grytsenko and Svitlana Mishchenko (2022). Operational risk management of using electronic and mobile money. Banks and Bank Systems, 17(3), 142-157.doi:10.21511/bbs.17(3).2022.12

World Bank (2017) https://documents1.worldbank.org/curated/en/249151504766545101/pdf/119208-BRI-PUBLIC-Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf. Accessed on 7th October, 2023

ZICTA (2022) *Annual Report, 2021*. https://www.zicta.zm/storage/posts/attachments/ppUYrWF3rnsG3o3eslcULkpRJQm70aBQmJxpjFR9.pdf. Accessed on 7th October, 2023

ZICTA (2023) ICTs Sector 2022 Annual Market Report: A Supply Side Assessment of Developments in the Information and Communications Technology Sector. February,

2023. https://www.zicta.zm/storage/posts/attachments/. Accessed on 14th October, 2023

Zimba, Aaron; Mukupa, George and Chama, Victoria (2022). Emerging mobile phone based_social_engineering_cyberattacks_in_the_Zambian_ICT_Sector https://www.researchgate.net/publication/366656282_. Accessed on 7th October, 2023

APPENDICES

Appendix A: Timeline of the study

	November 30th	**January 31st**	**February 29th**	**March 31st**	**April 15th**
Proposal submission					
Pre-Testing of tools					
Data collection					
Data analysis					
Report writing					
Submission of report					

Appendix B: Budget

S/N	ACTIVITY	COST (K)
1.	Developing and Submission of proposal	200
2.	Printing and pre-testing of the data collection tools	400
3.	Data collection logistics	4000
4.	Data analysis	600
5.	Report printing and submission	500
	TOTAL	**5, 700.00**

DATA COLLECTION TOOLS

Appendix C: The self-administered questionnaire

QUESTIONNAIRE No: ……

THE UNIVERSITY OF ZAMBIA IN COLLABORATION WITH ZIMBABWE OPEN UNIVERSITY

STRICTLY PRIVATE & CONFIDENTIAL
MASTER OF BUSINESS ADMINISTRATION

QUESTIONNAIRE

TITLE	**AN INVESTIGATION OF THE ADEQUACY OF CONTROL MEASURES IN COMBATTING MOBILE MONEY FRAUD IN LUSAKA DISTRICT**
RESEARCHER	**NYAMBE GABRIEL MUBITA** C/O University of Zambia in collaboration with Zimbabwe Open University Lusaka +260979470651
DATE	2024

Dear Participant,

You have been selected to participate in the University of Zambia academic research study. The purpose of the research is to **investigate the adequacy of the control measures in combatting mobile money fraud in Lusaka.** This research has been necessitated by the rising levels of mobile money fraud in the country and Lusaka in particular.

To participate in this study, simply fill out the assessment questionnaire attached to this letter. Kindly fill in the questionnaire as honest and open as you can as your participation is vital to our ability to accurately discover the above phenomena.

I anticipate that this questionnaire should take no more than 30 minutes to complete. You may choose to skip any question you feel uncomfortable in answering. While you may not experience direct benefits from participation, information collected in this study will benefit UNZA and for academic purposes and also the authorities in order to make informed decisions. Return of the questionnaire will be considered consent. Participation in this survey is completely voluntary. All questionnaires are received anonymously and will be treated as such.

I wish to thank you for your participation in this study!

If you have any comments, questions, or concerns with regards to the survey, the questions, or the purpose of the study, please contact me on email *mubbydocs2013@gmail.com* and cell phone no. +260979470651

Yours Faithfully,

Nyambe Gabriel Mubita

PART A

DEMOGRAPHIC DATA

1. What is your gender?

Male	Female	Prefer not to say

2. What is your age range?

20-30	31-40	41-50	51-60	Above 60	Prefer not to say

3. Level of education

Certificate	Diploma	Degree	Masters	PHD	Prefer not to say

4. How would you rate your ICT proficiency?

Very high	High	Moderate	Low	Prefer not to say

PART B: TYPES OF MOBILE MONEY FRAUD

5. What are some of the types of mobile money fraud that are dealt with by your Organization?
   - ☐ Sim card swap
   - ☐ Identity theft
   - ☐ Fake promotions
   - ☐ Fake money transfers
   - ☐ Phishing
   - ☐ Fake product/service delivery
   - ☐ Other, please specify

   ---

6. Which of type(s) of mobile money fraud are mostly dealt by ~~to~~ your Organization?

- ☐ Sim card swap
- ☐ Identity theft
- ☐ Fake promotions
- ☐ Wrong money transfers
- ☐ Phishing
- ☐ Fake product/service delivery
- ☐ Other, please specify

---

7. What type of control measures is your organization conversant with in combatting mobile money fraud?

- ☐ Sensitization of users
- ☐ Sensitization and training of mobile money agents
- ☐ Fraud detection
- ☐ Enhancement of mobile money security by using technology
- ☐ Apprehension of offenders
- ☐ Others, kindly specify

PART C: IMPLEMENTATION OF CONTROL MEASURES IN COMBATTING MOBILE MONEY FRAUD

8. Does your Organization employ any type of control measures to combat mobile money fraud? Yes ☐ No ☐

   If yes, which of the following type of control measures are used by your Organization to combat mobile money fraud?

   - ☐ Sensitization of users
   - ☐ Sensitization and training of mobile money agents
   - ☐ Fraud detection
   - ☐ Enhancement of mobile money security by using technology
   - ☐ Apprehension of offenders
   - ☐ Others, kindly specify

---

9. How often does your organization implement the control measures) to combat mobile money fraud?

Very frequently	frequently	Rarely	Not at all

10. Which of the above control measure do you think is most effective in combatting mobile money fraud?
    - ☐ Sensitization of users
    - ☐ Sensitization and training of mobile money agents
    - ☐ Fraud detection
    - ☐ Enhancement of mobile money security by using technology
    - ☐ Apprehension of offenders
    - ☐ Other, please explain

    ---

11. Kindly explain the choice of your answer in question 8 above

    ---

    ---

12. The following control measures are effective in combating mobile money fraud. Tick as many as they apply to your organization.

Type of control measure	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
Sensitization of users					
Sensitization and training of mobile money agents					
Fraud detection					

Enhancement of mobile money security by using technology					
Apprehension of offenders					
Other, please explain					

PART D: POLICY BEST PRACTICES

13. Which of the following policies and laws are utilized by your Organization to combat mobile money fraud?

☐ National Information & Communication Technology Policy 2023

☐ Electronic Communications and Transactions Act No. 4 of 2021

☐ Data Protection Act No. 3 of 2021

☐ The Cyber Security and Cyber Crimes Act No. 2 of 2021

☐ National Cyber Security Policy of 2021

☐ Others, please specify

---

14. In your view, which of the above policy/law is the most useful in combatting mobile money fraud?

☐ National Information & Communication Technology Policy 2023

☐ Electronic Communications and Transactions Act No. 4 of 2021

☐ Data Protection Act No. 3 of 2021

☐ The Cyber Security and Cyber Crimes Act No. 2 of 2021

☐ National Cyber Security Policy of 2021

☐ Others, please specify

---

15. Please kindly explain the choice of your answer in question 13.

---

16. The following policies/laws are effective in combating mobile money fraud. Tick as many as they apply to your organization.

Policy/Law	**Effectiveness in combatting mobile money fraud**				
	Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
National Information & Communication Technology Policy 2023					
Electronic Communications and Transactions Act No. 4 of 2021					
Data Protection Act No. 3 of 2021					
The Cyber Security and Cyber Crimes Act No. 2 of 2021					
The National Cyber Security Policy of 2021					
Other, please explain					

17. What other best policy practices should be put in place in order to combat mobile money fraud?

    ---

18. What other measures do you think should be put in place in order to control mobile money fraud in Lusaka?

END

THANK YOU FOR YOUR TIME AND PARTICIPATION

Appendix D: Interview guide

Dear Participant,

You have been selected to participate in the University of Zambia academic research study. The purpose of the research is to **investigate the adequacy of the control measures in combatting mobile money fraud in Lusaka.** This research has been necessitated by the rising levels of mobile money fraud in the country and Lusaka in particular.

To participate in this study, simply fill out the assessment questionnaire attached to this letter. Kindly fill in the questionnaire as honest and open as you can as your participation is vital to our ability to accurately discover the above phenomena.

I anticipate that this questionnaire should take no more than 30 minutes to complete. You may choose to skip any question you feel uncomfortable in answering. While you may not experience direct benefits from participation, information collected in this study will benefit UNZA and for academic purposes and also the authorities in order to make informed decisions. Return of the questionnaire will be considered consent. Participation in this survey is completely voluntary. All questionnaires are received anonymously and will be treated as such.

I wish to thank you for your participation in this study!

If you have any comments, questions, or concerns with regards to the survey, the questions, or the purpose of the study, please contact me on email *mubbydocs2013@gmail.com* and cell phone no. +260979470651

Yours Faithfully,

Nyambe Gabriel Mubita

PART A: DEMOGRAPHIC DATA:

1. What is your Gender?

   ---

2. What is your Age range?

   ---

3. What is your highest level of education?

   ---

4. How would you rate your ICT proficiency?

PART B: TYPES OF MOBILE MONEY FRAUD

5. What are some of the types of mobile money fraud that are dealt with by your Organization?

   ---

6. Which of type(s) of mobile money fraud are mostly dealt by ~~to~~ your Organization?

PART C: IMPLEMENTATION OF CONTROL MEASURES IN COMBATTING MOBILE MONEY FRAUD:

7. What type of control measures is your organization conversant with in combatting mobile money fraud?
8. Does your Organization employ any type of control measures to combat mobile money fraud? Yes ☐ No ☐

   If yes, what type of control measures are used by your Organization to combat mobile money fraud?

   ---

9. How often does your organization implement the control measures) to combat mobile money fraud?

   ---

10. Which measure (s) do you think is most effective in combatting mobile money fraud?

    ---

11. Kindly explain the choice of your answer in question 8 above

    ---

PART D: POLICY BEST PRACTICES

12. List and explain some of the policies and laws which are being utilized by your Organization to combat mobile money fraud.

---

13. In your view, which of the policy/law listed in 10 above is the most useful in combatting?

    ---

14. Please kindly explain the choice of your answer in question 11.

    ---

15. What other measures do you think should be put in place in order to control mobile money fraud in Lusaka?.....

THANK YOU FOR YOUR TIME AND PARTICIPATION

Appendix E**:** Interview guide for mobile money agents and individual users

Dear Participant,

You have been selected to participate in the University of Zambia academic research study. The purpose of the research is to **investigate the adequacy the control measures in combatting mobile money fraud in Lusaka.** This research has been necessitated by the rising levels of mobile money fraud in the country and Lusaka in particular.

To participate in this study, simply fill out the assessment questionnaire attached to this letter. Kindly fill in the questionnaire as honest and open as you can as your participation is vital to our ability to accurately discover the above phenomena.

I anticipate that this questionnaire should take no more than 30 minutes to complete. You may choose to skip any question you feel uncomfortable in answering. While you may not experience direct benefits from participation, information collected in this study will benefit UNZA and for academic purposes and also the authorities in order to make informed decisions. Return of the questionnaire will be considered consent. Participation in this survey is completely voluntary. All questionnaires are received anonymously and will be treated as such.

I wish to thank you for your participation in this study!

If you have any comments, questions, or concerns with regards to the survey, the questions, or the purpose of the study, please contact me on email *mubbydocs2013@gmail.com* and cell phone no. +260979470651

Yours Faithfully,

Nyambe Gabriel Mubita

PART A: DEMOGRAPHIC DATA:

1. What is your Gender?

   ---

2. What is your Age range?

   ---

3. What is your highest level of education?

   ---

4. How would you rate your ICT proficiency?

PART B: TYPES OF MOBILE MONEY FRAUD

5. Have you experienced any type of mobile money fraud before?

   Yes ☐ No ☐

6. If yes, what are some of the types of mobile money fraud that you have experienced before?

   ---

7. What are some of the types of mobile money fraud that are dealt with by your Organization?

   ---

8. Which of type(s) of mobile money fraud are mostly dealt by ~~to~~ your Organization?

PART C: IMPLEMENTATION OF CONTROL MEASURES IN COMBATTING MOBILE MONEY FRAUD:

9. Do you employ any type of control measures to combat mobile money fraud? Yes ☐ No ☐

   If yes, what type of control measures do you use to combat mobile money fraud?

   ---

10. How often do you implement the control measures to combat mobile money fraud?

    ---

11. Which measure (s) do you think is most effective in combatting mobile money fraud?

    ---

12. Kindly explain the choice of your answer in question 8 above

    ---

PART D: POLICY BEST PRACTICES

13. List and explain some of the policies and laws which are being used by the authorities to combat mobile money fraud.

    ---

14. In your view, which of the policy/law listed in 10 above is the most useful in combatting?

    ---

15. Please kindly explain the choice of your answer in question 11.

    ---

16. What other measures do you think should be put in place in order to control mobile money fraud in Lusaka?.....

THANK YOU FOR YOUR TIME AND PARTICIPATION

Appendix F: Application for ethical clearance approval

18th March, 2024

Nyambe Gabriel Mubita

P/Bag 476x RW,

LUSAKA

mubbydocs2013@gmail.com

0979470651

UNIVERSITY OF ZAMBIA ETHICS COMMITTEE GREAT EAST ROAD CAMPUS LUSAKA, ZAMBIA

Dear Members of the Ethics Committee,

Subject: Ethical Clearance Request for Research - "An investigation of the adequacy of control measures in combatting mobile money fraud in Lusaka District.

I am writing to seek ethical clearance for my proposed research study bearing the above title. The primary objective of this study is to investigate the adequacy of control measures in combatting mobile money fraud in Lusaka District

The research will involve conducting detailed interviews by way of questionnaires and interview guides to participants from ZICTA, Zambia Police Service, Mobile Network Providers, Mobile Money Agents and individual users of Mobile Money.

Throughout the research process, I commit to adhering rigorously to the following ethical considerations:

1. **Informed Consent:** Ensuring that all participants are thoroughly informed about the study's purpose and procedures. Written consent will be obtained before the commencement of the study, emphasizing voluntary participation and the right to withdraw at any time without repercussions.

2. **Anonymity and Confidentiality:** Safeguarding participant privacy by anonymizing all collected data. Strict confidentiality measures will be implemented, and personal identifiers will be either removed or altered in the reporting of research findings.
3. **Non-Maleficence:** Ensuring that the research causes no physical or psychological harm to participants. The study will be conducted in a manner that minimizes stress or discomfort for participants.
4. **Integrity:** Upholding the highest standards of honesty and integrity throughout the research process. Findings will be reported accurately and transparently, without manipulation or misinterpretation.
5. **Feedback:** Offering participants the option to receive a summary of research findings if they express interest.

Attached to this letter, you will find a comprehensive research proposal, necessary forms and the data collection tools for your review. Your guidance and approval are indispensable for the ethical and successful execution of this research.

I am available to provide any additional information or clarifications you may require and eagerly await your positive response.

Thank you for your consideration.

Yours sincerely,

Nyambe Gabriel Mubita

Student Number: 721000251

Appendix G: Letter to the Zambia Police Service

TRN

Approved

DIC - Ops

25/03/24

18th March, 2024

The Inspector General of Police

Zambia Police Service

LUSAKA

REPUBLIC OF ZAMBIA
ZAMBIA POLICE HEADQUARTER
25 MAR 2024
DEPUTY INSPECTOR GENERAL OF POLI
OPERATIONS
P. O. BOX 50103, LUSAKA - ZAMBIA

RE: PERMISSION TO INTERVIEW FOUR (4) OFFICERS IN AN ACADEMIC RESEARCH ON MOBILE MONEY FRAUD

Sir,

Reference is made to above captioned matter.

Iam a Zambian male who is studying for a degree in Masters of Business Administration at the University of Zambia in Lusaka. Iam currently conducting an academic research entitled "an investigation on the adequacy of control measures in combatting mobile money fraud in Lusaka District. This study has been necessitated by rampant reports of mobile money fraud by members of the general. It is hoped that the finds will help to curb this criminality which may increase if not addressed as the number of people using mobile money services keep increasing.

In view of the above, I wish to request for permission to interview four (4) officers that are in the department that is responsible for dealing with mobile money fraud related cases, who will be identified by your good office.

The mode of the interview is the questionnaire attached hereto, which each of the participants will be required to complete. I can also make the questionnaire available to them through google forms in case they want to fill it in online to save time. Each participant will also be required to complete the attached consent form.

Your assistance in this matter will be appreciated.

Yours faithfully,

NYAMBE GABRIEL MUBITA

097947051/0964022937

REPUBLIC OF ZAMBIA
ZAMBIA POLICE SERVICE
MAR 2024
DEPUTY INSPECTOR - TRD
OF POLICE
LUSAKA.

Appendix H: Letter of ethical clearance approval

THE UNIVERSITY OF ZAMBIA
DIRECTORATE OF RESEARCH AND GRADUATE STUDIES

Great East Road Campus | P.O. Box 32379 | Lusaka10101 | Tel: +260-211-290 258/291 777 **Fax**: (+260)-211-290 258/253 952 | **E-mail**: director.drgs@unza.zm | **Website**: www.unza.zm

APPROVAL OF STUDY

IORG No. 0005376
HSSREC IRB No. 00006464
REF NO. HSSREC-2024-MAR-044

8th April, 2024

Mr. Nyambe Gabriel Mubita
The University of Zambia
P.O. Box 32379
LUSAKA

Dear Mr. Mubita

RE: **"AN INVESTIGATION IN THE ADEQUACY OF CONTROL MEASURES IN COMBATING MOBILE MONEY FRAUD IN LUSAKA DISTRICT".**

Reference is made to your submission of the protocol captioned above. The HSSREC resolved to approve this study and your participation as Principal Investigator for a period of one year.

REVIEW TYPE	ORDINARY **REVIEW**	**APPROVAL NO. HSSREC:- 2024- MAR– 044**
Approval and Expiry Date	Approval Date: 8th April, 2024	Expiry Date: 7th April, 2025
Protocol Version and Date	Version - Nil.	7th April, 2025
Information Sheet, Consent Forms and Dates	☐ English.	To be provided
Consent form ID and Date	Version - Nil	To be provided
Recruitment Materials	Nil	Nil
Other Study Documents	Questionnaire.	
Number of Participants Approved for Study		

Specific conditions will apply to this approval. As Principal Investigator it is your responsibility to ensure that the contents of this letter are adhered to. If these are not adhered to, the approval may be suspended. Should the study be suspended, study sponsors and other regulatory authorities will be informed.

CONDITIONS OF APPROVAL

- No participant may be involved in any study procedure prior to the study approval or after the expiration date.
- All unanticipated or Serious Adverse Events (SAEs) must be reported to HSSREC within 5 days.
- All protocol modifications must be approved by HSSREC prior to implementation unless they are intended to reduce risk (but must still be reported for approval). Modifications will include any change of investigator/s or site address.
- All protocol deviations must be reported to HSSREC within 5 working days.
- All recruitment materials must be approved by HSSREC prior to being used.
- Principal investigators are responsible for initiating Continuing Review proceedings. HSSREC will only approve a study for a period of 12 months.
- It is the responsibility of the PI to renew his/her ethics approval through a renewal application to HSSREC.
- Where the PI desires to extend the study after expiry of the study period, documents for study extension must be received by HSSREC at least 30 days before the expiry date. This is for the purpose of facilitating the review process. Documents received within 30 days after expiry will be labelled "late submissions" and will incur a penalty fee of K500.00. No study shall be renewed whose documents are submitted for renewal 30 days after expiry of the certificate.
- Every 6 (six) months a progress report form supplied by The University of Zambia Humanities and Social Sciences Research Ethics Committee as an IRB must be filled in and submitted to us. There is a penalty of K500.00 for failure to submit the report.
- When closing a project, the PI is responsible for notifying, in writing or using the Research Ethics and Management Online (REMO), both HSSREC and the National Health Research Authority (NHRA) when ethics certification is no longer required for a project.
- In order to close an approved study, a Closing Report must be submitted in writing or through the REMO system. A Closing Report should be filed when data collection has ended and the study team will no longer be using human participants or animals or secondary data or have any direct or indirect contact with the research participants or animals for the study.
- Filing a closing report (rather than just letting your approval lapse) is important as it assists HSSREC in efficiently tracking and reporting on projects. Note that some funding agencies and sponsors require a notice of closure from the IRB which had approved the study and can only be generated after the Closing Report has been filed.

- A reprint of this letter shall be done at a fee.

- All protocol modifications must be approved by HSSREC by way of an application for an amendment prior to implementation unless they are intended to reduce risk (but must still be reported for approval). Modifications will include any change of investigator/s or site address or methodology and methods. Many modifications entail minimal risk adjustments to a protocol and/or consent form and can be made on an Expedited basis (via the IRB Chair). Some examples are: format changes, correcting spelling errors, adding key personnel, minor changes to questionnaires, recruiting and changes, and so forth. Other, more substantive changes, especially those that may alter the risk-benefit ratio, may require Full Board review. In all cases, except where noted above regarding subject safety, any changes to any protocol document or procedure must first be approved by HSSREC before they can be implemented.

Should you have any questions regarding anything indicated in this letter, please do not hesitate to get in touch with us at the above indicated address.

On behalf of HSSREC, we would like to wish you all the success as you carry out your study.

Yours faithfully,

DR. J. I. Ziwa
CHAIRPERSON
THE UNIVERSITY OF ZAMBIA HUMANITIES AND SOCIAL SCIENCES RESEARCH ETHICS COMMITTEE - IRB

cc: Director, Directorate of Research and Graduate Studies
Assistant Director (Research), Directorate of Research and Graduate Studies
Assistant Registrar (Research), Directorate of Research and Graduate Studies