A FRAMEWORK FOR ADDRESSING SECURITY VULNERABILITIES EXPERIENCED BY REGISTERED MOBILE MONEY CLIENTS IN LUSAKA, ZAMBIA.

BY

TANJE DAVID SAKALA

A DISSERTATION SUBMITTED TO THE UNIVERSITY OF ZAMBIA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION GENERAL.

THE UNIVERSITY OF ZAMBIA,

LUSAKA

2024

DECLARATION

I, **Tanje David Sakala,** do hereby declare that this dissertation is my own original work and has not been submitted to any other college, institution or university other than the University of Zambia. All sources of data used and literature on related works previously done by others, used in the production of this dissertation have been duly acknowledged. If any omission has been made, it is not by choice but by error.

Signature: .... Date: ....

COPYRIGHT

APPROVAL

This Dissertation, by Tanje David Sakala has been approved as a fulfilment of the requirements for the award of the Degree of Master of Business Administration General

Examiner 1	Signature	Date
…………………………..	………………………	…………………..
Examiner 2	Signature	Date
…………………………..	……………………..	……………………
Examiner 3	Signature	Date
…………………………..	………………………	…………………….
Chairperson Board of Examiners	Signature	Date
…………………………..	………………………	……………………..
Supervisor	Signature	Date
…………………………..	………………………	…………………….

ABSTRACT

The rapid expansion of mobile money services has transformed financial transactions across developing economies, providing convenient access to banking for unbanked populations. However, this growth has also introduced significant security vulnerabilities, raising concerns over data privacy, fraud, and system vulnerabilities. This study investigates prevalent security vulnerabilities associated with mobile money transactions, analysing common threats, and potential mitigation strategies. Using a survey research methodology, the research conducted a review of security incidents of mobile money users, complemented by a quantitative analysis of user behaviour response to security vulnerabilities. A sample of 380 registered mobile money users from Lusaka, Zambia, who were conveniently chosen using the Slovins formula, participated in the study. (Raphael. G, 2016) Mobile Money Transaction Variables Relationship Framework served as the foundation for the study. The Statistical Package for Social Scientists (SPSS) was used to analyse the data. Pearson correlation tests with a p-value of < 0.05 was deemed statistically significant. The results showed that there is a significant compromise in the security of mobile money transactions due to the following vulnerabilities: Smishing, Stolen/Lost Mobile Phone, and Agent Driven Fraud, with t values of .011, .005, and .000, respectively. A significant positive relationship between mobile money security vulnerabilities and transactions was indicated by an aggregate coefficient correlation of .430. As a contributing element to safe mobile money practices, the study also found considerable gaps in user awareness, underscoring the need for service providers to improve user education and strengthen security measures. This dissertation aims to contribute to mobile money security by proposing a framework that integrates solutions to improve user safety in mobile money transactions. The research concludes that addressing these security issues is essential for ensuring trust and long-term sustainability in the mobile money ecosystems, contributing to policy recommendations for regulators and practical guidance for service providers.

Keywords: Mobile Money, Registered Client, Transaction, Security Vulnerability, Mobile Money Crime, Mobile Money Operator, Regulatory Authority

ACKNOWLEDGEMENTS

I want to express my gratitude to the Almighty God for his unwavering grace and compassion in enabling me to complete this degree. I also want to express my sincere gratitude to my supervisor, Professor Jackson Phiri, for taking the time to review my work on a regular basis and for offering helpful criticism and suggestions that kept me focused throughout the entire process.

I am extremely grateful to my mother, Mary Chisanga Sakala, for her unwavering moral, material, and financial support, without which this research would not have been achievable. I am also grateful to my siblings, family, and close friends Mark Chicha and Samson Nzobokela, for their love, support, and prayers, which enabled me to persevere through every phase.

DEDICATION

To my mother, Mrs. Mary Chisanga Sakala, my sister Tipezenji Sakala, and my brothers Kapya Sakala and Bwalya Samuel Sakala, your unwavering love, boundless support, and endless encouragement have been my guiding lights throughout this journey. With heartfelt gratitude, I dedicate this thesis to you, for your sacrifice, your belief in me, and your constant inspiration. Your strength has been my foundation, and your wisdom my compass. This achievement is as much yours as it is mine. Thank you for always being my rock.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
API	Application Programming Interface
BOZ	Bank of Zambia
CAGR	Compound Annual Growth Rate
FINTECH	Financial Technology
FNB	First National Bank
FSD	Financial Sector Deepening
G2P	Government-To-Person
GSB	Graduate School of Business
GSM	Global System for Mobile Communication
GSMA	Global System for Mobile Communication Association
ID	Identification
IMEI	International Mobile Equipment Identity
KYC	Know Your Customer
MITM	Man in the Middle
MMA	Mobile Money Agent
MMO	Mobile Money Operator
MMT	Mobile Money Transaction
MMU	Mobile Money User
MNO	Mobile Network Operator
MNP	Mobile Network Provider
NRC	National Registration Card
PFIP	Pacific Financial Inclusion Programme

PIN	Personal Identification Number
PUK	Personal Unlocking Key
SIM	Subscriber Identification Module
SMS	Short Messages Service
SPSS	Statistical Package for Social Scientists
SSL	Secure Socket Layer
TLS	Transport Layer Security
UPI	Unified Payments Interface
USD	United States Dollar
USSD	Unstructured Supplementary Service Data
ZANACO	Zambia National Commercial Bank
ZICB	Zambia Industrial Commercial Bank
ZICTA	Zambia Information & Communications Technology Authority

CHAPTER 1

INTRODUCTION AND BACKGROUND

1.1 Introduction

MoneyTransfer.com (2023) states Mobile money is an electronic or digital service that offers financial services that are accessible on a SIM enabled mobile device. It is often linked to your mobile network provided number, and it lets you manage your finances without having to go to a physical bank. Mobile money services can function somewhat like bank accounts, allowing you to send and receive money to peers, save it on your device in a virtual wallet, and withdraw and deposit it at authorized agents. You can use your wallet to pay bills, make purchases in-person or online, and perform the majority of other tasks that require a debit or credit card.

Worldremit.com (2017), Due to the conceptual similarities between bank accounts and mobile money, money held in mobile money accounts are protected by local financial regulations. Mobile money providers and their partners are required to confirm the identities of their clients due to financial legislation and regulations. Fraudsters and other criminals find it far more difficult to use these services illegally as a result. Mobile money services, which maintain a record of each transaction and account balance, ensure that the user's money is secure even in the event that the phone or SIM card is lost or stolen. Additionally, a secret PIN must be used to authenticate each transaction. The majority of mobile money services are offered by local mobile telecom companies that are authorized to offer electronic payment services. Some mobile money services are provided by banks and other financial institutions. A person must present identification to a local mobile money agent or mobile money operator, such as a valid passport, driver's license, or government ID, in order to register for mobile money services.

Finance Magnates (2023), Africa gave birth to mobile money, a ground-breaking technology that has completely revolutionised how individuals in underdeveloped countries access and transfer money. Instead of utilizing traditional bank accounts, customers can use mobile money to transfer and receive money. By giving millions of previously unreached people access to financial services, this has increased financial inclusion and accelerated economic growth. Mobile money has had a significant impact on the African economy. Many Africans did not have access to traditional financial services before mobile money. Money transfers were done via cash and unofficial networks, which could occasionally be expensive, inefficient, and unreliable. Mobile money, which offers a quick, reliable, and reasonably priced way to move money, has changed this. A wide range of additional financial services, including savings accounts, loans, and insurance, are now available to users. As a result, financial inclusion has increased and millions of Africans now have access to formal financial services for the first time. Mobile money has had a significant impact on the African economy. It has made funding and other financial services accessible to small businesses, allowing them to grow and thrive. Furthermore, it has enabled people to save money that they can utilize for their healthcare, education, or enterprises. Due to the rapid expansion of mobile money services, most African countries now offer mobile money options. GSMA-SOTIR (2023), According to the GSMA's 2023 State of the Industry Report on Mobile Money, mobile money transaction values in Africa reached a total of $832 billion in 2022, a significant portion of the global mobile money ecosystem. Sub-Saharan Africa alone accounted for two-thirds of global mobile money transaction values. The region saw an average of $2.3 billion transacted daily, reflecting a year-on-year growth rate of 22%.

Security is essential to mobile money services because it guarantees the availability, confidentiality, and integrity of real-time financial transactions. Users are protected from theft, fraud, and illegal access by effective security measures. Important security features that are provided by the majority of mobile money operators include two-factor authentication, encryption, fraud detection systems, dynamic passwords and PINs, secure SIM and device binding, real-time alerts and notifications, transaction limitations, and regulatory compliance. Despite the robust security precautions offered by mobile money operators, the risks associated with mobile money services include social engineering, SIM swap fraud, weak PINs, and phishing scams.

The purpose of this study is to advance mobile money security by putting forward a framework that incorporates ways to increase user safety during mobile money transactions. This will be achieved by proposing a framework for addressing security vulnerabilities experienced by registered mobile money clients by drawing inferences from Lusaka, Zambia.

The subsequent sections of chapter one includes the background of the study, statement of the problem, aim of the study, research objectives, research questions, significance of the study, scope of the study and the organisation of the dissertation. This chapter concludes with a chapter summary.

1.2 Background

According to Interpol (2020) M-PESA, a service offered by Safaricom in partnership with Vodafone, was the first mobile money service provider in Africa and originally launched in Kenya in 2007. The initiative's main goal was to create a system that would enable microloan repayments over the phone, hence lowering the expenses related to cash handling. Because of its ease of use, the service immediately became accepted by the metropolitan populace and was acknowledged as a legitimate way to send money to relatives in remote and unworthy places. Cash Essentials (2020), The use of mobile money has greatly increased over the African continent in recent years. For underbanked and unbanked people, mobile money has increased access to financial services. According to the World Bank, mobile money has significantly decreased financial exclusion, especially in sub-Saharan Africa. Subex (2021), Africa leads the world in the use of mobile money due to the absence of extensive traditional banking infrastructure in remote locations. Sub-Saharan Africa accounted for more than 70% of global mobile money transactions by 2023. Major adopters included Kenya, Ghana, Nigeria, and Uganda, where the market has been dominated by M-Pesa, MTN Mobile Money, and Airtel Money. GSMA (2023), A 2022 Sub-Region breakdown reports $277 billion worth of transactions were made in East Africa, primarily through M-Pesa in Kenya and Tanzania. West Africa recorded transactions totalling $492 billion in markets such as Ghana, Ivory Coast, and Nigeria. Smaller but increasing shares came from Southern and Central Africa, where mobile money use is still prevalent.

In African civilization today, mobile money is widely used and significant. This is because mobile devices are becoming more and more popular, mobile money services are becoming more flexible, and most businesses are using technology to reach their present and potential customers.

The Outlier (2024), The mobile money market is expected to hit over $2.3 billion in daily transactions by 2025, with a significant portion being vulnerable to fraud. Between 2021 and 2022, fraud complaints involving mobile money services rose by 25%, with Kenya, Nigeria, and South Africa reporting the highest number of cases. The most common mobile money crimes in Sub-Saharan Africa include fraud, identity theft, money laundering, and extortion. Below are some insights and statistics about these crimes:

Fraud: The most prevalent mobile money crime is fraud, which includes social engineering scams in which scammers pose as service providers to deceive clients into disclosing private information. Another common scam is SIM swap fraud, in which scammers take over a user's mobile number. Mobile money fraud complaints increased by 25% between 2021 and 2022, with South Africa, Nigeria, and Kenya reporting the most cases. Interpol (2020), According to reports from significant telecom providers in nations like Kenya and Nigeria, SIM swap fraud had increased significantly and accounted for 13–15% of all cases of mobile fraud.

Money Laundering: Interpol (2020), In nations with more relaxed regulatory monitoring, mobile money services are occasionally used to transfer illegal payments. This crime is made easier in some places by inadequate Know Your Customer (KYC) regulations. For instance, there has historically been little regulation on the use of mobile money accounts in Ghana to transfer illegal funds for cross-border activities. To combat this, however, the government and banking institutions worked to impose stricter KYC (Know Your Customer) regulations.

Identity Theft: Criminals frequently create mobile money accounts using stolen or fictitious identities, which are subsequently utilized for money laundering or fraudulent transactions.

Extortion and Cybercrime: Since mobile money is most often used in East and West Africa, cybercriminals take advantage of the anonymity and accessibility of these platforms to extort money or launch ransomware attacks.

(Chiti. M, 2018), Mobile money's revolutionary impact in financial inclusion is highlighted by its history in Zambia. Initiated by telecom firms such as Airtel and MTN, mobile money services gained popularity in the 2010s. Zamtel entered the market in 2017. With an estimated 86% of Zambians not having access to banking in 2015, these services sought to improve financial access. This initiative was greatly aided by Zoona, a 2009 startup from Zambia that targeted those without formal banking access using an easy-to-use platform that only required a phone and identification to conduct transactions. Financial Insight (2022), Mobile money increased financial inclusion from 59.3% in 2015 to 69.4% by 2020. As people turned to digital networks to avoid face-to-face interaction during the COVID-19 pandemic, the number of active accounts increased significantly. The Central Bank of Zambia made this expansion possible by putting programs like the National Financial Switch into place, which improved network interoperability and decreased the need for cash transactions.

(Mulenga. B, 2024), In Zambia, mobile money has grown rapidly, but this has also resulted in a rise in related crimes, including fraud. According to the Zambia Information and Communications Technology Authority (ZICTA), mobile money transactions hit a record K452 billion in 2023, which was 50% more than the K295.8 billion in 2022. This significant growth made the sector a target for fraudsters. But along with this expansion have come a lot more fraud cases, which is why ZICTA has warned about the need to secure personal data and implement robust security measures. TransUnion (2023), In Zambia, attempts at digital fraud are particularly common in the telecom and financial services industries. Suspected fraud in financial services transactions coming from Zambia was 12.1% during the first half of 2023. In the same time frame, fraud in the telecom industry increased by 92%. Prevalent types of fraud in Zambia include social engineering and phishing, SIM swap fraud and agent drive fraud.

GSMA-SOTIR (2023). The Zambia Information and Communications Technology Authority (ZICTA) initiatives have been launched to intensify awareness programs which advice users to protect their PINS and refrain from disclosing personal information. ZICTA also encourages the use of short codes such as *707# to report suspicious activity. In order to enhance fraud detection systems and fortify mobile wallet security procedures, regulators and service providers are collaborating in Zambia.

Current efforts in combating mobile money crimes in sub-Saharan Africa and Zambia include:

Regulatory Measures: To combat fraud, governments and telecom authorities have been strengthening Know Your Customer (KYC) laws and pushing mobile service providers to put in place more robust verification procedures.

Consumer Education: Through nationwide awareness campaigns and telecom operators' notifications, a concentrated effort has been made to inform mobile money users about the dangers and how to stay away from frauds.

Cooperation: To improve fraud detection systems and guarantee better consumer protection, mobile service providers and financial institutions have also started working together more.

1.3 Statement of the Problem

(Sichula. A, 2024), In Zambia, the emergence of mobile money services has greatly expanded financial inclusion by giving previously marginalized groups access to financial services. But along with this expansion has come an increase in crimes involving mobile money. Among the main causes of this are inadequate security measures, low user knowledge of fraud, and changing criminal strategies. In Zambia, unauthorized SIM swaps, social engineering techniques, identity theft, and phishing are common mobile money scams. Sector-specific fraud in telecoms grew by 92% through the period of 2023, often involving SIM card manipulation. TransUnion (2023), Additionally, 85% of Zambians, reported having recently been the target of fraud, according to a TransUnion study; 76% of Zambians claimed they had been targeted by a fraud scheme but had not fallen victim to it, while 9% said they had been targeted and had fallen victim according to the survey. For those who were targeted, the most common fraud schemes by which they reported being attacked were vishing (33%), phishing (35%), smishing (43%), and money or gift card scams (46%).

(Mbunji and Kaira, 2024), System flaws and user behaviour are exploited by fraudsters, who target both users and agents. As a result of the expansion of mobile money services by providers notably MTN, Airtel, and Zamtel, more transactions and larger amounts of money are now moving through digital platforms, which makes them desirable targets for scammers. Mobile money agents, who frequently serve as users' initial point of contact, have reported serious issues, such as fraud and theft. Furthermore, the ecosystem is vulnerable as a result of their inadequate training in fraud prevention.

Mobile money security refers to the measures and protocols put in place to safeguard the integrity, confidentiality, and availability of financial transactions conducted through mobile devices. With the rise of digital financial services in Zambia and the use of mobile phones for banking, payments, and transfers, ensuring the security of these transactions has become paramount. To improve mobile money security and combat fraud, the Zambia Information and Communications Technology Authority (ZICTA) currently has some security measures in place, which include:

SIM Registration and Verification: ZICTA mandates SIM card registration in order to restrict access to mobile services, including mobile money, to verified users exclusively. Deactivation of unregistered or non-compliant SIM cards lowers the possibility of fraud utilizing untraceable numbers.

Public Sensitization: To caution consumers about the dangers of mobile money fraud, including phishing and social engineering schemes, ZICTA conducts public awareness campaigns. They stress how crucial it is to keep sensitive information, such as personal identification numbers (PINs), private.

Collaboration with Other Entities: ZICTA and the Bank of Zambia have collaborated to develop a framework for reviewing complaints associated with mobile money. In order to look into and prosecute incidents of mobile money fraud, they also work with cybersecurity specialists and law enforcement.

Regulatory Oversight: ZICTA (2024). ZICTA monitors mobile network operators and mobile money providers to ensure compliance with security standards, focusing on protecting consumer transactions and data. This study was carried out to address security vulnerabilities in the mobile money eco system. The findings of this study aim to contribute to policy recommendations for regulators and practical guidance for service providers.

1.4 Aim of the Study

To reduce the increasing number of mobile money crimes by developing a framework for addressing security vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia.

1.5 Research Objectives

The research was guided by the following objectives:

i. To assess the availability and utilization of mobile money services in Lusaka, Zambia.
ii. To identify security vulnerabilities associated with mobile money transactions in Lusaka, Zambia.
iii. To propose a framework that addresses security vulnerabilities associated with mobile money transactions in Lusaka, Zambia

1.6 Research Questions

The research questions were as follows:

i. What is the availability and utilization of mobile money services in Lusaka, Zambia?
ii. What security vulnerabilities are associated with mobile money transactions in Lusaka, Zambia?

iii. How can security vulnerabilities associated with mobile money transactions in Lusaka, Zambia be addressed?

1.7 Significance of the Study

The main beneficiaries of the findings of this research include but are not limited to, the general public, registered mobile money clients, mobile money operators, law enforcement agencies, financial institutions and policy regulatory authorities. This study on security vulnerabilities associated with mobile money transactions in Lusaka, Zambia is significant for several reasons, as it addresses critical aspects of financial technology, security, and societal impact by:

Enhancing Financial Inclusion: Security flaws could deter users from adopting mobile money services, thus slowing progress toward financial inclusion.

Safeguarding Consumer Trust: The findings of this study will aid mobile money providers identify vulnerabilities and mitigate risks, ensuring customer confidence.

Mitigating Financial Loss: Mobile money systems have become a frequently targeted financial service by fraud, vishing and phishing attacks. The findings of the study will help develop strategies to prevent financial losses for customers and service providers.

Promoting Regulatory Compliance: Governments, policy regulators and financial institutions require insights to create and enforce regulations that protect users while supporting innovation.

Encouraging Innovation in Security Technologies: The findings of the study can drive innovation in secure payment technologies, such as biometric authentication, encryption, and fraud detection systems.

Economic Stability and Growth: Mobile money is essential to the economy since it makes transactions easier and lessens the need for cash. A secure system guarantees dependability and guards against significant disruptions brought on by fraud or hacking.

Impact on Global Development Goals: Mobile money directly contributes to several United Nations Sustainable Development Goals (e.g., no poverty, reduced inequalities). Addressing security challenges ensures that mobile money remains a sustainable and effective tool for development.

Strengthening Collaboration: Insights from this study on mobile money security will encourage collaboration among stakeholders, including telecom companies, financial institutions, policy regulators, and researchers. This will foster a collective approach to building resilient and secure financial ecosystems.

1.8 Scope of the Study

The study's target demographic was registered mobile money clients of network-based mobile money operators, specifically Airtel, MTN, and Zamtel, in Lusaka, Zambia. Lusaka being the capital and largest city in Zambia is the administrative and economic centre. It represents a high concentration of mobile money users and also experiences a high rate of financial transactions and agent network concentration. The research primarily focused on security vulnerabilities related to mobile money transactions.

1.9 Organization of the Dissertation

The dissertation compromises of the subsequent six chapters organized as follows:

Chapter 2: Literature Review

Chapter Two offers a comprehensive review of existing literature related to the study topic, focusing on identifying gaps in current knowledge from various scholars and authors.

Chapter 3: Theoretical and Conceptual Models/Frameworks

Chapter Three presents the study's conceptual framework, theoretical review, and main hypotheses. This chapter also describes the operationalization of variables.

Chapter 4: Research Methodology

The study's research design, data gathering strategies, and data analysis procedures are all covered in detail in Chapter Three. It gives a detailed explanation of how the information was gathered and examined in order to meet the objectives of the study.

Chapter 5: Data Analysis and Presentation

The data evaluation and inferences drawn from the study are presented in Chapter Five. It offers a thorough examination of the findings from the study in relation to the research questions, supported up by relevant tables, figures, and descriptive data. Furthermore, this chapter presents the outcomes of the hypothesis testing from Chapter Three.

Chapter 6: Discussion of Findings

Chapter Six discusses the findings by integrating the literature review and primary findings together. It gives a correlation to earlier studies on the topic.

Chapter 7: Conclusion and Recommendations

The study's main conclusions are outlined in Chapter Seven, which also makes inferences based on theoretical understanding and empirical data. Based on the results and outcomes of the study, it also makes recommendations to relevant stakeholders for implementation or additional research.

By using this methodical approach, the dissertation seeks to offer an extensive and comprehensive analysis of the vulnerabilities present in the Lusaka, Zambia, mobile money ecosystem, as well as insightful recommendations for further study and policy development in the field of mobile money security.

1.10 Chapter Summary

This research study's foundation is established in this introductory chapter. It outlines the problem's background and then presents the problem statement for the investigation in an effort to find a solution and advance knowledge. The study's goals, objectives, and research questions are all made explicit while developing potential solutions for the given challenge. Furthermore, the importance of the research and its structure are emphasized. The next chapter examines pertinent research literature.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter provides a thorough analysis of the body of existing literature from a variety of sources, such as scholarly works, official government reports, publications, journals, online sections, and newspapers. It is a summary of the research on mobile money and the vulnerabilities associated with mobile money transactions. The focus of mobile money and security will be inferred from a global, regional, and local standpoint. Security issues and present regulations put in place to protect mobile money transactions will be covered in additional detail in this chapter. The conclusions and inferences drawn from the many reviewed literatures will then be presented in this chapter. This comparative literature will serve as the basis for this investigation.

The literature review is necessary to avoid replicating the findings of previous studies. Thus, by reviewing the literature, the researcher can gain knowledge about earlier research on the same subject, when it was conducted, and what was and wasn't found. This review of the literature highlights attention to the knowledge gap, which is the discrepancy between the quantity of research that has been done and the unanswered questions.

2.2 The Mobile Money Ecosystem

Mobile Money refers to the technological infrastructure and systems that enable digital financial transactions through mobile devices. It relies on a combination of mobile networks, software platforms, and financial services to facilitate secure and efficient money transfers, payments, and other financial activities. It makes use of mobile phones' extensive availability to offer easily accessible and practical financial solutions, especially in areas where traditional banking is lacking. Mobile money technology is compatible with both smartphones and standard phones and is installed on the SIM card of a device. The Mobile Money Ecosystem encompasses the following key components:

Mobile Network Operators (MNOs): GSMA (2023), Mobile Money platforms and the underlying telecommunications infrastructure that supports mobile money services are provided my MNOs. MNOs facilitate communication between users and the mobile money platform via SMS, USSD, mobile apps and internet-based services. Examples of MNOs include: MTN Mobile Money (Africa), M-Pesa (Kenya and Tanzania), GCash (Philippines), bKash (Bangladesh), Paytm (India) and Zamtel Mobile Money (Zambia). Functions of mobile money platforms include software systems that manage transactions, user accounts, and service offerings. Features include transaction processing, account management, customer service interfaces, and integration with other financial systems.

Accessibility Technology: GSMA (2021), This refers to the tools, features, and systems designed to ensure that mobile money services are usable by a broad range of people, including those in underserved or vulnerable populations. This focuses on access and enhancing usability for individuals regardless of their location, literacy level, income, disability, or technology skills. Accessibility technology in mobile money incorporates:

- USSD (Unstructured Supplementary Service Data): A menu-driven interface accessible on basic phone features. USSD does not require internet connectivity making it popular for areas with low smartphone penetration and poor internet access. USSD is accessible by dialling codes such as *115# to perform transactions.
- Mobile Applications: Specialised mobile apps for smartphones can provide improved functionality such as transaction histories, graphical user interfaces, and security measures. Apps need to be connected to the internet (either through Wi-Fi or mobile data).
- SMS (Short Message Service): This allows users to initiate transactions or receive confirmations via SMS.
- Localization and Language Options: Most MNOs have support for multiple languages and dialects to cater to diverse user bases. Localized interfaces with culturally relevant terms and formats improve usability.
- Interoperability: Ensures users are able to transact across different mobile money platforms and with banks or financial institutions. This reduces barriers for users who may need to interact with others on different systems or platforms.
- Application Programming Interfaces (APIs): This allows integration of mobile money services with third-party platforms, such as e-commerce sites, utility companies, and financial institutions.

Agent Network System: Papersoft (2023), The phrase "Agent Network System" describes the precise locations that act as intermediaries and enables clients to deposit or withdraw money. Agents serve as an interface between the cash-based economy and the mobile money ecosystem, facilitating mobile money services through mobile phones and point-of-sale devices. Agents play a major role in determining the reach of mobile money services, particularly in underserved and rural areas. The mobile money ecosystem is interconnected with scalability and profitability. Numerous significant advantages for both service providers and clients can be realised with the aid of a well-managed mobile money agent. Benefits of a well-managed agent network system include liquidity management, improved customer experience and trust, increased accessibility, and lower operating costs. Mobile money operators can achieve profitability and scalability by utilising the strength of a well-managed mobile money agent, which can change financial accessibility for a larger audience.

Security Mechanisms: Comviva (2023). Security remains a top priority for most mobile money clients despite lingering security concerns. To safeguard transactions, MNOs use multi-factor authentication (such as PINs and biometrics), encryption for safe data transfer, and fraud detection algorithms and monitoring. Avoiding spam and phishing remain significant priorities for MNOs when implementing security mechanisms.

2.3 Overview of Mobile Money Globally

Mobile money has had a significant global impact, transformed financial institutions, and aided in socioeconomic growth, particularly in areas with limited access to traditional banking services. According to a recent study by (Ngila. F, 2023), As of 2024, there were over 1.75 billion registered mobile money accounts globally, processing transactions worth $1.4 trillion annually, equivalent to $2.7 million per minute. Outside of Africa, mobile money has revolutionised South and Southeast Asia, Latin America, and the Pacific Islands, promoting innovation, economic growth, and financial inclusion. This section reviews the extent and utilization of mobile money at a global scale.

2.3.1 South Asia

FinDev Gateway (2024), Digital payments have been transformed in India by platforms like Paytm and Google Pay. With more than 300 million users, Paytm alone enables small business transactions, bill payments, and peer-to-peer (P2P) transfers. By processing 10 billion transactions per month as of mid-2024, the Indian government's UPI (Unified Payments Interface) technology has revolutionised the country's cashless economy. The Business Research Company (2024), In Bangladesh Services like bKash have reached millions, with over 50% of adults using mobile money accounts. These platforms empower rural communities by providing access to remittances and microloans

2.3.2 Southeast Asia

FinDev Gateway (2024), Maya (previously PayMaya) and GCash have made it possible for mobile wallets to be widely used in the Philippines. These platforms played a crucial role in the distribution of government subsidies during the pandemic, emphasising their function in providing social welfare, whereas in Indonesia both urban and rural residents are now familiar with digital wallets thanks to services such as GoPay. This facilitates payment of utilities, transportation, and internet shopping.

2.3.3 Latin America

Grand View Research (2024), Fintech platforms in Mexico, such as Mercado Pago and OXXO Pay, are promoting digital financial inclusion, particularly for informal labourers and small enterprises. Transactions using QR codes are on the rise around the nation. Brazil's mobile money industry has grown significantly thanks to expanding smartphone adoption, rising digital literacy, and supportive regulations. With a compound annual growth rate (CAGR) of 37.5% from 2024 to 2030, Brazil is expected to become a major player in the Latin American mobile payment market, expected to exceed amounts of over USD 13.8 billion by 2030.

2.3.4 Pacific Islands

UNCDF (2024), In the Pacific Islands, mobile money gained prominence as a potentially beneficial technology for enhancing financial inclusion. These disparate countries had particular difficulties, such as the absence of conventional banking infrastructure and exorbitant fees for financial services. These discrepancies were addressed in part by mobile money solutions, which use mobile networks to offer financial services. Mobile money services like M-Selen, launched by Our Telekom in collaboration with the UN Capital Development Fund, are allowing people in rural areas of the Solomon Islands to send and receive money, save, and pay for services without having to travel far distances to banks. Considering that just 25% of people had a bank account and 35% relied on unofficial financial services, mobile money is anticipated to greatly improve financial inclusion, particularly for marginalised populations like women and those living in rural areas. DAI Publications (2024), Mobile providers like Digicel Pacific launched affordable mobile wallets in other Pacific countries like Fiji, Samoa, Tonga, and Vanuatu, enabling users to send and receive money via international remittances, pay bills, and make transfers. Access to services like G2P (government-to-person) payments, which are essential for financial empowerment in rural regions, had been made possible by Digicel Pacific's collaborations. Because of low digital literacy, mistrust, and a lack of knowledge about mobile money services, adoption is still difficult despite these advancements. Yet, initiatives like the Pacific Financial Inclusion Programme (PFIP) and other government agencies are still working to eliminate these obstacles through better financial literacy and public-private collaborations.

2.3.5 Developed Markets (Europe and North America)

The Business Research Company (2024), Digital wallets and contactless payment methods like PayPal, Apple Pay, and Google Pay are closely linked to the adoption of mobile money. These systems effortlessly integrate with financial services and e-commerce to improve ease and promote the cashless economy. In developed markets, privacy concerns and reliance on smartphone technology continue to pose security challenges.

2.4 The Mobile Money Ecosystem's Challenges

Financial inclusion and economic empowerment have benefited greatly from mobile money globally, but there are still significant barriers to its expansion. The industry faces significant obstacles as a result of legislative and technological developments, including:

2.4.1 Digital and Financial Literacy

Many consumers in underserved or rural locations are not knowledgeable enough to make effective use of mobile money services. For instance, despite mobile wallets' promise to increase financial inclusion, their use is constrained in the Pacific Islands by low levels of digital literacy.

2.4.2 Fraud and Security Concerns

GSMA (2024), Scams, identity theft, and cybercrime directed at mobile money consumers are still common. Although fraud detection systems are getting better, ongoing investment is necessary to stay up with changing threats.

2.4.3 Limited Infrastructure

DAI Publications (2024). In remote areas, access is hampered by unreliable electricity and poor mobile network coverage. For instance, there are large infrastructure gaps in Sub-Saharan Africa and the Pacific Islands that restrict the reach of services.

2.4.4 Regulatory Barriers

Interoperability and cross-border transactions are made more difficult by diverse regulatory frameworks. Global acceptance and innovation are slowed down by fragmented legislation.

2.5 Global Innovations and Future Potential of Mobile Money

Mobile money has inspired numerous innovations globally, transforming financial services and spurring new technologies that enhance accessibility, security, and economic empowerment. Key global innovations include:

2.5.1 Interoperability and Cross-Border Payments

The Business Research Company (2024), Mobile money has lowered the cost and duration of transferring payments in areas with substantial immigrant populations. For instance, PayMaya in the Philippines and Wave in South Asia both provide inexpensive international transfers.

2.5.2 Integration with E-Commerce and Digital Services

FinDev Gateway (2024). Mobile money can drive digital economies by integrating with online marketplaces and digital financial services. In Southeast Asia, platforms such as ShopeePay combine mobile wallets and e-commerce to support a cashless society.

2.5.3 Financial Inclusion for Marginalized Groups

Services that are specifically designed for low-income customers, women, and rural regions can help close current disparities. Microloan, insurance, and savings products help underprivileged groups.

2.5.4 AI and Machine Learning for Fraud Prevention

GSMA (2024). Advanced AI algorithms can detect anomalies and prevent fraud in real-time, boosting trust in mobile money systems.

2.5.5 Government-to-Person (G2P) Payments

DAI Publications (2024), Using mobile money to distribute social benefits can decrease corruption and increase accessibility. Fiji currently distributes welfare payments effectively and transparently by using mobile wallets.

2.6 Overview of Mobile Money in Africa

Dabafinance (2023), Africa leads the world in the use of mobile money, which is a game-changing tool for financial inclusion. By bridging the gap in financial access, mobile money has had a significant impact on the economy, particularly in areas with inadequate banking systems. With almost 70% of all mobile money transactions worldwide, Africa leads the globe in mobile money usage. MTN Mobile Money (East and West Africa), Orange Money (North Africa), Airtel Money (East and West Africa), and M-Pesa (Kenya) are the main MNOs in the mobile money ecosystem. The World Bank estimates that mobile money has provided financial access to over 300 million people in Sub-Saharan Africa. In Sub-Saharan Africa, there are more than 10 million registered mobile money agents, significantly expanding their reach in comparison to traditional banks. The high level of activity of these operators is reflected in the $2.3 billion in transactions that occur on average each day in the region. By giving millions of unbanked African's accesses to digital financial services, these operators play a crucial part in financial inclusion. Through collaborations, technology advancements, and improved service offerings, they keep growing. The following are some important statistics for each prominent mobile money operator.

2.6.1 Safaricom (M-Pesa)

Euromonitor (2023), Safaricom operates in Kenya, Tanzania, Mozambique, and other East African countries. With a reach of over 51 million active users as of 2022, Safaricom processes transactions exceeding values of $314 billion annually. A notable attribute associated with M-Pesa is being the pioneer of mobile money in Africa, supporting bill payments, savings, and international remittances.

2.6.2 MTN Mobile Money

Dabafinance (2023), MTN operates in 17 African countries including Ghana, Uganda, Nigeria and Zambia. MTN has more than 69 million active users and processed $365 billion in transactions as of 2022. MTN is the leading provider of innovative finance and interoperability in West Africa.

2.6.3 Orange Money

Euromonitor (2023), Orange is predominant in West and North Africa, including Ivory Coast, Senegal, and Mali. Orange serves over 70 million customers across 17 countries and processes transactions exceeding $300 billion annually. Orange is notable for its strong presence in francophone Africa (French speaking African countries), facilitating remittances and business payments.

2.6.4 Airtel Money

GSMA (2023), Airtel operates in 14 countries, including Zambia, Uganda and Malawi. It has a reach of approximately 26 million active users, growing steadily with a focus on rural areas and SMEs. Airtel Money is well known for its low transaction fees and rural reach.

2.6.5 Wave

Wave operates in Senegal, Ivory Coast, and continues to expand in West Africa. It is rapidly gaining market share with over 5 million active users. Wave is popularized by it zero-fee transfers, disrupting traditional mobile money pricing.

2.7 Mobile Money Crimes in Africa

Mobile money crimes are a growing concern in Africa as the industry expands. Major crimes include fraud, money laundering, SIM swap scams, and unauthorized transactions. While these crimes are not unique to specific mobile money operators, they exploit vulnerabilities in mobile money systems. Below are some prominent issues associated with major mobile money operators in Africa:

2.7.1 Fraud

Fraud occurs when scammers impersonate mobile money agents or customer service representatives to trick users into divulging their personal identification numbers (PINs) or authorizing fraudulent transactions. Fraud cases have been reported extensively across operators like M-Pesa, MTN Mobile Money, and Airtel Money. In Kenya, fraudsters target M-Pesa users by pretending to offer loan services or requesting reversals for "mistaken" deposits.

2.7.2 SIM Swap Fraud

Criminals duplicate SIM cards to gain access to mobile money accounts, allowing them to siphon funds or engage in unauthorized transactions. Users of MTN Mobile Money, Orange Money, and Airtel Money frequently report this type of fraud. SIM swap fraud targeting MTN Mobile Money accounts has increased in Nigeria.

2.7.3 Money Laundering

Criminal networks take advantage of careless Know Your Customer (KYC) regulations to transfer illegal cash via mobile money services. Platforms with large transaction volumes, including Orange Money and MTN Mobile Money, are frequently targeted. Authorities in West Africa have identified mobile money networks for their role in laundering proceeds from scams and corruption

2.7.4 Unauthorized Access and Internal Fraud

Dabafinance (2023), Employees or rogue agents alter systems to steal money or enable fraudulent activities. M-Pesa agent networks and other networks have been observed to experience such problems. In Tanzania, a few mobile money agents were detained for conspiring with scammers to take advantage of a system vulnerabilities.

2.7.5 Cybersecurity Breaches

GSMA (2023). To obtain unauthorised access to funds, hackers target client devices or mobile money databases. Phishing attacks target consumers of MTN Mobile Money and M-Pesa, taking advantage of their low level of digital literacy.

2.8 Mobile Money Security Strategies

To counteract crimes including fraud, money laundering, and unauthorised access, mobile money operators use a range of strategies. These safeguards are intended to uphold user confidence, adhere to legal obligations, and protect users. Even while mobile money providers actively attempt to prevent mobile money crimes, security heavily relies on user education, strong regulatory frameworks, and technology advancements. Security strategies include:

2.8.1 Strengthening KYC (Know Your Customer) Process

Operators enforce stricter registration processes requiring valid identification and biometric data. This limits fraudulent account creation and enables better tracking of suspicious activity. MTN Mobile Money and Airtel Money require robust customer verification to activate accounts.

2.8.2 Fraud Detection and Monitoring Systems

This is the use of real-time fraud detection systems powered by artificial intelligence (AI) and machine learning (ML) to monitor transactions and flag suspicious behaviour. Safaricom's M-Pesa employs advanced analytics to detect unusual transaction patterns and halt fraudulent activities.

2.8.3 User Education and Awareness Campaigns

Mobile Money Operators regularly educate users on how to recognize and report fraud. This reduces vulnerability to phishing, SIM swap scams, and social engineering attacks. Airtel Money has been running campaigns warning customers against sharing their PINs with anyone, including agents.

2.8.4 Enhanced Agent Oversight

Mobile money operators audit and train agents to ensure compliance with operational guidelines. This is aimed at reducing internal fraud and ensures agents act responsibly. MTN Mobile Money requires agents to register with unique identification and attend regular compliance training.

2.8.5 Two-Factor Authentication and PIN Protection

Strengthening user account security is achieved with the use of two-factor authentication (2FA) and secure PIN systems. This prevents unauthorized access even if SIMs or devices are compromised. Majority of mobile money operators offer PIN-reset options that require additional verification steps.

2.8.6 Partnership with Regulators and Law Enforcement

Cooperation between mobile money operators, regulators, and law enforcement is necessary to exchange information about criminal networks, put anti-money laundering (AML) procedures into place, and bring criminal charges against offenders. This makes it easier to find and stop organised financial crimes. M-Pesa works with the Central Bank of Kenya to monitor high-value transactions and prevent illegal activity.

2.8.7 Cybersecurity

Euromonitor (2023), Mobile money operators must invest in secure server technologies, firewalls, and encryption. With a robust cybersecurity infrastructure in place, hacking, data breaches, and other cybercrimes are less likely to occur. End-to-end encryption is now used for M-Pesa transactions by Safaricom.

2.8.8 Interoperability Standards and Transaction Limits

Dabafinance (2023), This can be accomplished by imposing transaction limits and mandating platform interoperability for regulatory monitoring. This, in turn, will simplify monitoring and lessen the magnitude of financial losses in the event of fraud. Ghana has less chances of fraudulent inter-platform transfers thanks to mobile money interoperability systems.

2.9 Overview of Mobile Money in Zambia

ITWeb Africa (2020). More than 57% (11.24 million) of Zambia's population uses mobile money services as of 2022, which is significantly greater than the country's regional peers, including Malawi (35%), Zimbabwe (25.8%), and Angola (2.9%). MTN, Airtel, and Zamtel are the three primary mobile money providers in Zambia. MTN Zambia projected having more than 4.5 million mobile money users by the end of 2020, making it one of the biggest carriers in the nation. By the same year, Airtel Zambia had about 3 million mobile money subscribers, while Zamtel's mobile money base continued to grow. (Mudzingwa. F, 2023). Services offered by mobile money operators in Zambia include international remittances, bill payment, airtime purchase, merchant payments, financial products, cash withdrawal, and money transfers. The majority of transactions in Zambia's payments industry currently occur through mobile money due to its extensive range of services. The mobile money ecosystem in Zambia is supported by multiple providers, including fintech solutions. These platforms have facilitated not only everyday transactions but also remittances, which are a vital component of the economy. For instance, remittances in Zambia contribute over $400 million annually, with digital channels increasingly dominating this space. TechTrends (2024), Additionally, by fostering collaborations between fintech firms and conventional banks, mobile money has improved interoperability and made it possible for a more integrated financial ecosystem. This partnership improves cross-border transaction capabilities, bringing financial services to neglected areas and promoting regional commerce and investment. The potential of mobile money to alleviate financial difficulties and promote equitable economic development among many demographic groups is demonstrated by its sustained expansion in Zambia.

2.10 Mobile Money Crimes in Zambia

AAG (2024). According to both the National Cyber Security Index and the Global Cyber Security Index, Zambia is ranked 58th out of 161 and 73rd out of 194 countries, respectively Because Zambia is a developing nation, just 50% of its citizens own a personal computer, limiting their access to technology. However, around 75% of people use a smartphone, which makes SMS frauds a particular problem. The Zambia Computer Incident Response Team (ZM-CIRT) received 10.7 million reports of cybercrimes in 2021 alone, including social media hijacking and mobile money reversal frauds. Zambia has a GDP of $4000 per person. Over 150 million ZMK ($872,000) was lost by Zambia's finance sector between 2020 and Q2 2022. SMS fraud cost Zambians more than 1 million ZMK ($58,000) during that time. As mobile payment systems expand, Zambia is seeing an increase in mobile money crimes, which are getting increasingly complex. Registered mobile money clients in Zambia are most frequently victims of the following predominant categories of mobile money crimes:

2.10.1 Fraudulent Transactions

Criminals use false pretences to trick individuals into transferring money or sharing sensitive account details. Between 2023 and 2024, 320 cases of obtaining money through false pretences were reported.

2.10.2 Cyber Extortion

Involves threats to release sensitive data or disrupt services unless a ransom is paid. Zambia recorded 170 such cases between 2023 and 2024.

2.10.3 Unauthorized Data Access

Cybercriminals utilize counterfeit apps to steal login credentials or conduct unauthorized transactions. 184 cases of unauthorized access to data have been reported between 2023 to date.

2.10.4 Identity Theft

Fraudsters use stolen or fake identities to register SIM cards and commit crimes. This contributed to 450 reported identity-related offenses between 2023 to 2024.

2.10.5 Agent Fraud

Some mobile money agents syphon money during deposits and withdrawals or inflate transaction fees, among other unethical actions. Through colluding with agents, fraudsters are able to take money by starting a payment and then cancelling it, taking advantage of system flaws.

2.10.6 SIM Swaps

ZambiaMonitor (2023). Through fraudulent SIM swaps, criminals can gain access to a victim’s mobile number, access their mobile money accounts, and carry out illegal transactions. There have been reports of individuals losing significant amounts of money due to phishing and SIM swap fraud.

2.11 Approaches to Mobile Money Security in Zambia

Addressing mobile money security in Zambia is of high priority due to the increasing cases of fraud and cybercrime. Mobile money security describes the procedures and safeguards implemented to protect the availability, confidentiality, and integrity of financial transactions carried out via mobile devices. Below are the current key approaches to improving mobile money security in Zambia:

2.11.1 Strengthened SIM Registration Process

The Neven (2024), The Zambian government, through the Zambia Information and Communications Technology Authority (ZICTA), mandates stricter Know Your Customer (KYC) processes to ensure accurate SIM card registration. Mobile money operators like MTN, Airtel, and Zamtel have been instructed to stop issuing pre-registered SIM cards and verify customer identities thoroughly.

2.11.2 Public Awareness Campaigns

(Mudzingwa. F, 2023), Mobile money operators and regulatory bodies conduct educational campaigns to educate the general public on avoiding phishing scams, securing PINs and passwords and recognizing fraudulent messages and offers.

2.11.3 Enhanced Technology Solutions

Fraud detection systems enable mobile money operators to use advanced algorithms and monitoring tools to detect unusual transaction patterns. Some operators have introduced two-factor authentication to secure transactions.

2.11.4 Collaboration Between Stakeholders

ZambiaMonitor (2023). The Ministry of Technology and Science, law enforcement, mobile money providers, and the Bank of Zambia have partnered to better coordinate anti-fraud initiatives. Effective tracking and prosecution of scammers is the goal of the collaborative efforts.

2.11.5 Legislative Reforms

The Zambian government is working on updating the legal framework for cybersecurity, including plans to amend the Cyber Security and Cyber Crimes Act to address emerging mobile money fraud tactics.

2.11.6 Agent Oversight

Enhanced oversight of mobile money agents is crucial. Operators are implementing measures to monitor and penalize agents found engaging in fraudulent activities.

2.11.7 Data Encryption and Security Protocols

Data protection measures, such as encrypting sensitive information and ensuring secure communication channels, are being implemented to safeguard transactions.

2.11.8 Recovery Mechanisms

Mobile operators and banks collaborate to improve systems for dispute resolution and recovery of stolen funds.

By addressing the weaknesses in Zambia's mobile money ecosystem, the above-mentioned strategies promote the country's ongoing development and financial inclusion objectives. Reports from ZICTA, the Bank of Zambia, and mobile money operators provide more detailed information regarding the strategies.

2.12 Other Related Studies

This section discusses some related scholarly research carried out on mobile money security.

A study by (Ali et al. 2020) evaluated the main security concerns related to Ugandan mobile money systems. According to the report, despite the vast advantages of mobile money, adoption and acceptability of the system are generally low because of security flaws and systemic difficulties. Therefore, the goal of the study was to conduct a survey in order to assess the main security concerns related to Ugandan mobile money systems. Identity theft, authentication attacks, phishing attacks, vishing attacks, smishing attacks, sharing of personal identification numbers (PINs), and agent-driven fraud were identified as the main security concerns. According to the study's findings, mitigation strategies could include improved access controls, customer awareness campaigns, agent training on appropriate behaviour, stringent measures against fraudsters, service providers monitoring high-value transactions, and creating a thorough legal document to operate mobile money services. In order to assist governments and Mobile Network Operators (MNO) who would like to establish safe mobile money systems, this study offered a baseline survey. However, this study was restricted to Uganda and did not represent the opinions of other pertinent parties, including banks, regulatory bodies, and financial institutions.

In Dodoma City, Tanzania, a study was carried out by (Kitime, E. 2018) to provide the optimal security procedures for mobile money users. To do this, a framework for cybersecurity threats to Dodoma City's mobile money users was created. The study was carried out because cyber threats are becoming more sophisticated due to the desire of people with financial and criminal motivations to gain private and sensitive data. The data collected was analysed, and the findings indicated that the following risks are associated with using mobile money transactions: denial of service, data copying (data leakage), data alteration, lack of liquidity, hackers, lost mobile phones, viruses and worms, theft and fraud, lost passwords, inadequate networks, and sending cash or float to the incorrect number. The results also showed that mobile money carriers are not doing enough to reduce the risks for both mobile money agents and users, and that customers are not adequately aware of the risks involved.

The most common and possible dangers for mobile money transactions in Tanzania are counterfeit money, fake transaction requests, and password loss, according to (Raphael G. 2016), in order to receive authentication to use the mobile money application and complete transactions, the majority of users were seen to be at danger of forgetting their passwords. The data also showed that the incidence of risk factors was mostly the fault of mobile money users, who simply exposed themselves to dangerous situations by being unaware or uneducated. However, the study did show that, even if average incidences were seen, risk occurrences are not a major issue. The survey once again demonstrated that, despite the average rate of barrier occurrences in mobile money transactions, poor network performance seemed to be the most frequent problem, followed by a shortage of liquidity and the need for a legal document to complete the transaction. The three challenges were found to be major barriers that Tanzanian mobile money service users must overcome.

(Gombiro et al. 2015) presented a conceptual framework for identifying financial crime associated with mobile money. The framework included, among other things, historical databases, a knowledge base, Know Your Customers, big data analytics, and data mining tools. Based on the several frameworks and techniques for identifying financial crime, the imaging problem required a comprehensive strategy to reveal hidden dangers in mobile money. The study also found that financial crime involving mob money was difficult to combat since many internal control systems had significant control weaknesses. But crucial elements were the technology's ability to keep thorough records of all actions taken and electronic transactions involving fraud or increased fraud risk. However, the only focus of this study was fraud detection mechanisms.

A study by (Ambore et al. 2017) suggested that despite the inherent benefits of Mobile Financial Services (MFS) products, their adoption had been slowed back by a lack of confidence. The main cause of the lack of trust in MFS was cybercrime. The current cybersecurity solutions had not been able to lower cybercrime rates or boost public confidence in the MFS. As a result, a strong framework was required to handle the risk of cybercrime while using mobile platforms for financial services. With the goal of offering the best solution to reduce the risk of cybercrime in MFS. According to a study by (Mbunji and Kaira, 2024), MMS are widely used in Zambia because of their dependability, accessibility, and ease. Numerous studies demonstrate the critical role MMS can play in enhancing resource flow in Africa's rising economies. This potential is found in the requirement that MMS provide electronic money transfers instead of physical ones, which would remove or lessen the time and location constraints on money transfers.

2.13 Chapter Summary

This chapter examined government publications, journals, online sections, newspapers, and official reports on mobile money and its security. The chapter began with the global perspective by examining related literature globally outside of the African continent, it employed the funnel approach to review literature, which allowed for a systematic examination of the material relevant to mobile money and security. Next, the African region was discussed, and ultimately Zambia, which helped to deepen the conversation. In addition to identifying possible research gaps, this assisted in creating a table of relevant studies. Based on the discussions, the majority of research found security flaws and threats related to mobile money, but little research on user behaviour. In Africa, particularly Zambia, there is an absence of thorough data on fraud trends, user behaviour, and reported mobile money crimes. Moreover, a framework that addresses potential vulnerabilities associated with mobile money for registered clients in Zambia and other African regions has not been presented by other comparable journals that were evaluated. Therefore, the purpose of the research was to close that research gap.

CHAPTER 3

THEORETICAL AND CONCEPTUAL MODELS/FRAMEWORKS

3.1 Introduction

This chapter discusses the theoretical background, conceptual frameworks and models related to the study. According to (Creswell, 2014), a theoretical framework is a fundamental structure that is employed in research to elucidate and reinforce the theories or concepts that form the basis of a study. It offers a lens through which the research problem is viewed, directing the research process and analysis and connecting the study's goals to current knowledge.

A conceptual framework is a written or visual representation that shows the relationships between the main ideas, concepts, or variables that are essential to a research investigation. By connecting theories, existing information, and novel ideas, it acts as a roadmap, assisting in the organisation and direction of the research process. The researcher's understanding of the topic, the literature review, and the suggested methodology will all be taken into consideration while developing the conceptual framework specifically for this study. The proposed model will then be used to build the hypothesis, and operationalisation of the variables will follow.

3.2 Theoretical Frameworks

This study was guided by several theoretical frameworks on mobile money security by providing a lens to analyse risks, user behaviours, and systemic issues. Below are some of the relevant frameworks and how they apply to this study.

3.2.1 Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT), developed by (Rogers, 1975) is a psychological theory used to explain how individuals respond to perceived threats and how they adopt protective behaviours. PMT consists of two primary appraisal processes:

Threat Appraisal: Evaluation of the severity of a threat and the individual's vulnerability to it. This involves the perceived severity which evaluates how serious the threat is perceived to be whilst the perceived vulnerability evaluates the likelihood of being personally affected by the threat.

Threat Appraisal in Mobile Money Security: Users may evaluate the severity of threats such as SIM-swapping, phishing scams, or agent fraud in perceived severity. E.g. Educating users about the financial and personal impacts of mobile money fraud can increase their perception of the severity of the threat. Users assess their likelihood of being targeted in perceived vulnerability. E.g. Publicized fraud cases can make users feel more vulnerable, prompting protective behaviours.

Coping Appraisal: Evaluation of an individual's ability to take protective action. This incorporates the response efficacy which is belief in the effectiveness of the protective behaviour, self-efficacy which is confidence in one's ability to perform the protective behaviour, and response costs which are the barriers or sacrifices associated with adopting the protective behaviour.

Coping Appraisal in Mobile Money Security: Users must believe that security measures (e.g., PIN protection, two-factor authentication) effectively prevent fraud in response efficacy. E.g. Mobile money providers highlighting the effectiveness of biometric authentication can boost response efficacy. Users need confidence in their ability to adopt secure practices, such as creating strong PINs or recognizing phishing attempts in self-efficacy. E.g. Training and awareness campaigns help users feel capable of safeguarding their accounts. Users weigh the costs of adopting security measures (e.g., inconvenience or time) in response costs. E.g. Simplifying security procedures or automating them can lower perceived response costs.

Application of PMT to the Study

(Milne et al. 2000), PMT was used in this study to examine how users view the hazards associated with mobile money and whether or not these views influence preventative actions. The basis for developing training courses or awareness campaigns aimed at enhancing danger and coping assessments can be found in PMT. In order to improve response efficacy and self-efficacy while lowering response costs, mobile money providers can utilise PMT to create user-centric security measures.

Empirical Evidence

Digital banking systems have used PMT to evaluate how fraud education affects user behaviour. According to research, more secure behaviours (such as maintaining PIN confidentiality) are the result of growing understanding of dangers and preventative measures. The validity of PMT has been supported by studies on mobile banking security, which have demonstrated that users' adoption of security measures is highly influenced by their level of self-efficacy and response efficacy.

3.2.2 Routine Activity Theory (RAT)

(Cohen and Felson, 1979) created the Routine Activity Theory (RAT), a criminological theory that explains how crimes happen by combining three factors: An individual who intends to commit a crime is known as a motivated offender. A person, thing, or system that is appealing or susceptible to criminal activity is a good target and lack of a capable guardian which is insufficient safeguards or people to discourage criminal activity. RAT places more emphasis on the environmental and situational circumstances of crimes rather than it does on the traits of perpetrators. It is particularly relevant to contemporary situations, such as finance and cybercrimes.

Application of Routine Activity Theory to Mobile Money Security

(Leukfeldt et al. 2016), By concentrating on the contextual elements that give rise to chances for fraud or theft, RAT offers a helpful lens through which to examine how mobile money crimes transpire. The theory's application to mobile money security is as follows:

Motivated Offenders: Criminals are increasingly targeting mobile money due to its widespread use and accessibility. Fraudsters are motivated by financial gain to exploit users through phishing scams, SIM-swap fraud, or social engineering. This research will draw inferences on offender behaviours, such as the methods used to acquire users' personal identification numbers (PINs) or conduct unauthorized withdrawals.

Suitable Targets: Mobile money users and systems become suitable targets due to factors like lack of user awareness, use of weak PINs or predictable passwords and accessibility of mobile money agents handling large volumes of cash. Individuals unaware of phishing scams may unknowingly share sensitive information, making them suitable targets. By teaching users how to avoid phishing tactics and how to generate strong PINs, their vulnerability can be reduced. Operators might limit the number of transactions for new customers or high-risk accounts.

Lack of Capable Guardians: Inadequate enforcement of security protocols by mobile money operators, a lack of regulatory oversight in the mobile money ecosystem, and users failing to activate security features like two-factor authentication are just a few examples of how crimes are made easier when protective mechanisms are either non-existent or inadequate. Inadequate training for mobile money agents may lead to inadequate supervision, which raises the risk of fraudulent transactions. Operators of mobile money can improve security by putting strong authentication techniques (such biometrics) in place and making sure agents follow stringent transaction guidelines. By ensuring adherence to security standards and penalising recklessness, regulatory authorities can serve as guardians.

Empirical Examples

(Muthiora. B, 2015), In Zambia, SIM-swap fraud is prevalent when motivated offenders exploit weak identification processes implemented by mobile money operators (absence of capable guardians) to access mobile money accounts (suitable targets). Studies on mobile money scams in Kenya have highlighted how inadequate public awareness campaigns and lax regulatory enforcement create opportunities for fraud.

3.2.3 Diffusion of Innovation Theory (DOI)

(Rogers. E, 1962) created the Diffusion of Innovation Theory (DOI), which describes how new concepts, inventions, or technology gradually transcend a community. The theory specifies five major factors that affect the diffusion process: time, social systems, adopter categories, innovation, and communication channels. Understanding how people and organisations embrace and use technologies intended to lower fraud and improve security is made easier with the help of DOI.

Relevance of DOI to Mobile Money Security

(Susanto et al. 2015) A framework for examining the proliferation of security improvements in mobile money services is provided by DOI. Below is how it works:

Innovation

Rogers determined that the acceptance of innovations is influenced by five criteria. These are applicable to security technologies for mobile money:

Relative Advantage: If users believe that security solutions offer superior protection over current approaches, they will adopt them. For instance, using biometric authentication instead of standard PINs to increase security.

Compatibility: Security features must be in line with the needs, values, and habits of users. For instance, implementing fraud alarm systems that are easy to use and seamlessly interact with mobile money apps.

Complexity: Technologies that are thought to be overly complicated, like multi-step authentication, may encounter opposition. For instance, instructing consumers to lessen the apparent complexity of turning on sophisticated security mechanisms.

Trialability: Encouraging adoption can be achieved by letting consumers test new features (like fraud alerts).

Observability: Wider adoption of security features is encouraged by observable benefits, such as a decrease in fraud incidences.

Communication Channels

Mobile money providers can utilise social media, SMS marketing, and community outreach to promote security measures since effective communication is essential for raising knowledge of developments in mobile money security. Peer endorsements are important, particularly in areas with robust social networks.

Adoption Rates and Time

Different adoption rates of advancements in mobile money security can be explained by DOI. While late majority/laggards, such as users in rural areas or those with poor literacy levels, may be slower to accept modern security measures due to lack of awareness or accessibility, early adopters, or tech-savvy users, are quick to implement new features like biometric authentication.

Social System

Adoption is influenced by community dynamics and social network structure. For example, in Zambia, users 'perceptions of security technology may be influenced by cultural norms and their level of trust in mobile money agents. Through collaborations and public initiatives, governments and regulators serve as change agents, advancing security standards.

DOI Applications for Secure Mobile Money

DOI can be used to determine the obstacles experienced by laggards and investigate why some user segments adopt security measures more quickly than others. For instance, examining the rates at which rural and urban mobile money users employ fraud detection techniques. Mobile money providers can also use DOI to create focused advertising campaigns that promote the use of security measures, for instance, pilot projects that roll out two-factor authentication to early adopters before expanding to the whole public. DOI can be used by regulators to encourage the broad implementation of mobile money security requirements, such as mandatory adherence to encryption standards to guarantee the security of user data.

Empirical Examples

(Muthiora. B, 2015), According to research conducted in Kenya, perceived usability and noticeable drops in fraud occurrences are key factors in the adoption of biometric authentication. User education and visible success stories disseminated through communication channels have an impact on the adoption of fraud reporting capabilities in areas where mobile money frauds are prevalent.

3.2.4 Socio-Technical Systems Theory (STS)

(Baxter. G., & Sommerville. I, 2011) Socio-Technical Systems (STS) Theory emphasizes the interdependence between social and technical components within an organizational or technological framework. Originating in the 1950s from studies on workplace productivity by the Tavistock Institute, STS proposes that optimal system performance is achieved when social (human) and technical (technological) systems are jointly optimized. The theory includes: Technical Subsystem (tools, technologies, and workflows), Social Subsystem (people, their roles, relationships, and interactions) and Environmental Context (external factors such as policies, culture, and market dynamics). STS is especially helpful when researching systems like mobile money, where user-provider-technology interaction is essential to security and performance.

Relevance of STS to Mobile Money Security

(Gupta. S., & Xu. H, 2020). Mobile money systems function at the intersection of technology and human systems. When these components are not aligned, security issues frequently arise. Using STS theory aids in providing a thorough response to these issues:

Technical Subsystem and Mobile Money Security: The technological subsystem is supported by fraud detection systems, encryption technologies, and mobile money platforms. Systems that have weak encryption standards may be more susceptible to attacks like SIM-swap fraud. Fraud prevention requires the use of security tools such as biometric technologies, transaction monitoring, and two-factor authentication. For these technologies to work, user behaviour must be smoothly integrated with them.

Social Subsystem and Mobile Money Security: Users who are unaware of security precautions (such as not revealing their PIN) are vulnerable to fraud. For instance, scams frequently take advantage of people's ignorance about phishing or illegal transactions. Although mobile money agents are essential to cash-in and cash-out services, if they are not properly trained or supervised, they may also serve as entry sites for fraud. Thus, procedures for accountability and training are essential to preserving security and confidence. To improve system security, governments and central banks enact laws like Know Your Customer (KYC) requirements.

Environmental Context: Accessibility may be more important to users in rural locations than rigorous security, thus customised actions are required. Accountability for mobile money carriers is ensured by the strict implementation of security regulations. To safeguard users, authorities in Zambia, such as the Bank of Zambia, implement mobile money security regulations.

Applications of STS in Mobile Money Security

(Trist. E. L, 1981), A holistic system design ensures that technical solutions align with user needs and behaviours such as designing fraud alerts that are simple for low-literacy users to understand. Stakeholder integration brings together regulators, mobile money operators, and users to co-develop security protocols, for instance, collaborative efforts to implement secure agent networks. Training and awareness campaigns strengthen the social subsystem through user and agent education on mobile money fraud prevention. Iterative policy and technology development uses feedback from users and agents to improve security features and regulatory measures.

Empirical Examples

(GSMA 2020), In Kenya the success of M-Pesa's mobile money security relied on integrating advanced fraud detection with robust user education campaigns, whereas in Zambia efforts by the Bank of Zambia to strengthen SIM registration policies highlight the importance of regulatory guardianship as part of the socio-technical system.

3.2.5 Institutional Theory

(Scott. W. R, 2008), Institutional Theory explains how structures, norms, rules, and processes within organizations and societies influence behaviour. It focuses on how these elements are established, maintained, and changed over time. This theory highlights three key pillars that drive institutional behaviour which are regulative pillar which describes formal rules, regulations, and policies that govern behaviour, normative pillar which describes social values, norms, and expectations shaping organizational or individual conduct and the cultural-cognitive pillar that describes shared beliefs and cultural frameworks that influence how people perceive and act. The theory is often applied to understand organizational compliance with rules, societal expectations, and the adoption of practices in response to institutional pressures.

Relevance of Institutional Theory to Mobile Money Security

Bank of Zambia (2020), Institutional Theory provides a framework for examining the socio-political and organizational factors that influence the adoption and implementation of mobile money security measures.

Regulative Pillar and Mobile Money Security: To stop fraud, governments and central banks implement security regulations, such as Know Your Customer [KYC] requirements. To guarantee that only verified customers can access mobile money systems, the Bank of Zambia enforces SIM registration procedures in Zambia. Mobile money providers are held accountable for non-compliance with regulatory security standards through sanctions and compliance, which encourages adherence to security procedures.

Normative Pillar and Mobile Money Security: Standards like user education, moral agent conduct, and customer-focused security procedures serve as guidelines for the mobile money industry. To stop phishing and other cybercrimes, top providers like MTN and Airtel follow industry best practices. Customers want mobile money providers to protect their money, which forces businesses to implement innovative, user-friendly security measures.

Cultural-Cognitive Pillar and Mobile Money Security: Users' perceptions of the advantages and disadvantages of mobile money security mechanisms are influenced by cultural norms. Adoption rates in Zambia may be impacted by rural customers prioritising convenience over stringent security measures. Users, operators, and regulators all agree that strong security measures are necessary to ensure the long-term viability of mobile money services.

Applications of Institutional Theory in Mobile Money Security

Regulatory Compliance Analysis: The impact of regulatory frameworks on the security strategies used by mobile money companies can be assessed using institutional theory. For instance, examining how Zambia's anti-money laundering (AML) laws affect the country's efforts to combat fraud

Security Standards Development: The impact of regulatory frameworks on the security tactics used by mobile money companies can be assessed using institutional theory. For instance, examining how Zambia's anti-money laundering (AML) laws affect the country's efforts to combat fraud

User Education Campaigns: The cultural-cognitive pillar's insights can direct the creation of security awareness initiatives that are appropriate for regional settings.

Behavioural Studies: (DiMaggio et al. 1983), Using institutional theory, researchers may examine how consumers react to security aspects of mobile money in light of governmental requirements and societal norms.

Empirical Examples

(Muthiora. B, 2015), While the implementation of mandatory SIM registration has helped reduce identity-related fraud, demonstrating the role of regulatory pressures in Zambia, Kenya's Safaricom's M-Pesa introduced KYC and transaction limits in accordance with regulatory requirements, addressing issues like money laundering and fraud.

3.3 Conceptual Framework

The connections between the main variables and procedures in this research study will be illustrated and described using a conceptual framework. This paradigm will offer a methodical approach to problem analysis and solution development for tackling mobile money vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia.

The conceptual framework was adopted from (Raphael. G, 2016). It implied that the success or occurrence of the transaction depends on the existence or lack of risks and obstacles as well as the financial rules and policies established by the government. According to the study's findings, using the internet on a mobile device puts users of mobile money at danger. As a result, optimum security procedures were suggested. However, the study's focus was solely on cybersecurity and Dodoma City, Tanzania. The security flaws relevant to the mobile money ecosystem were not specifically addressed in the study. Raphael's Mobile Money Transaction Variables Relationship Framework, which is depicted below, was used in this investigation.

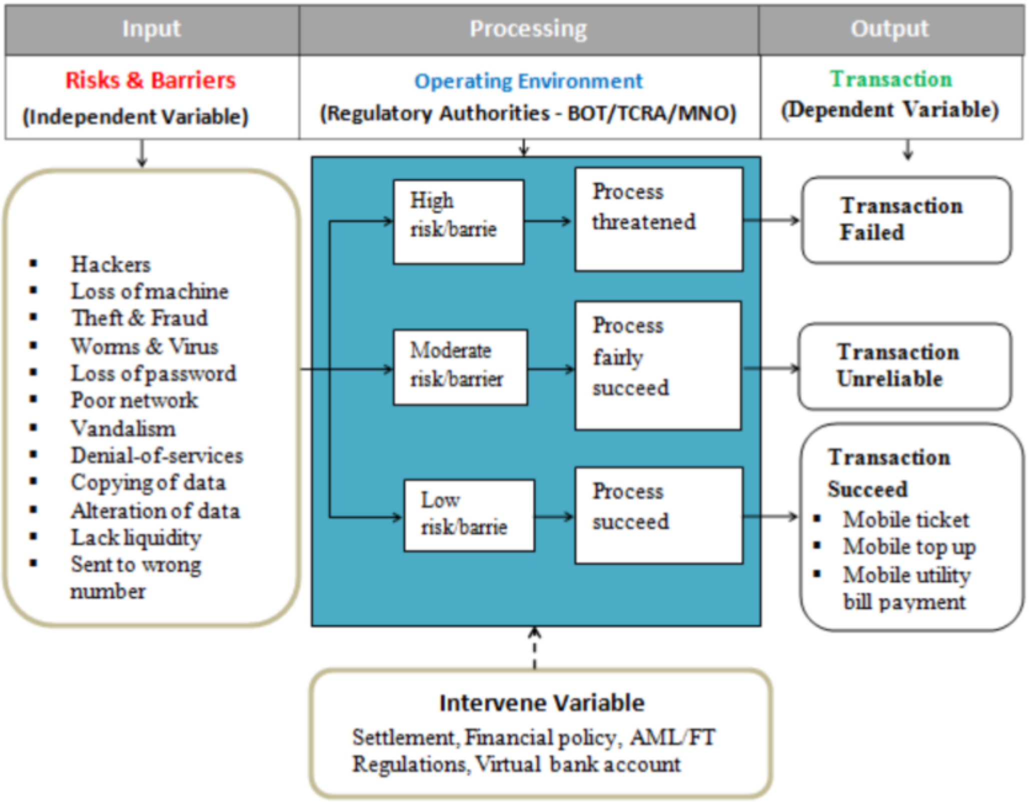


Figure 1: Mobile Money Transaction Variables Relationship Framework (Raphael. G, 2016)

3.4 Proposed Conceptual Framework

The framework consists of key variables, their relationships, and the processes that address mobile money security vulnerabilities. It incorporates technological and human dimensions. The independent variables refer to the root causes of mobile money security vulnerabilities. The dependent variable refers to the outcome of a mobile money transaction that has been affected by a mobile money security vulnerability(s). Due to the nature of this research, mediating variables such as multi-factor authentication, fraud detection systems and data encryption were not taken into consideration.

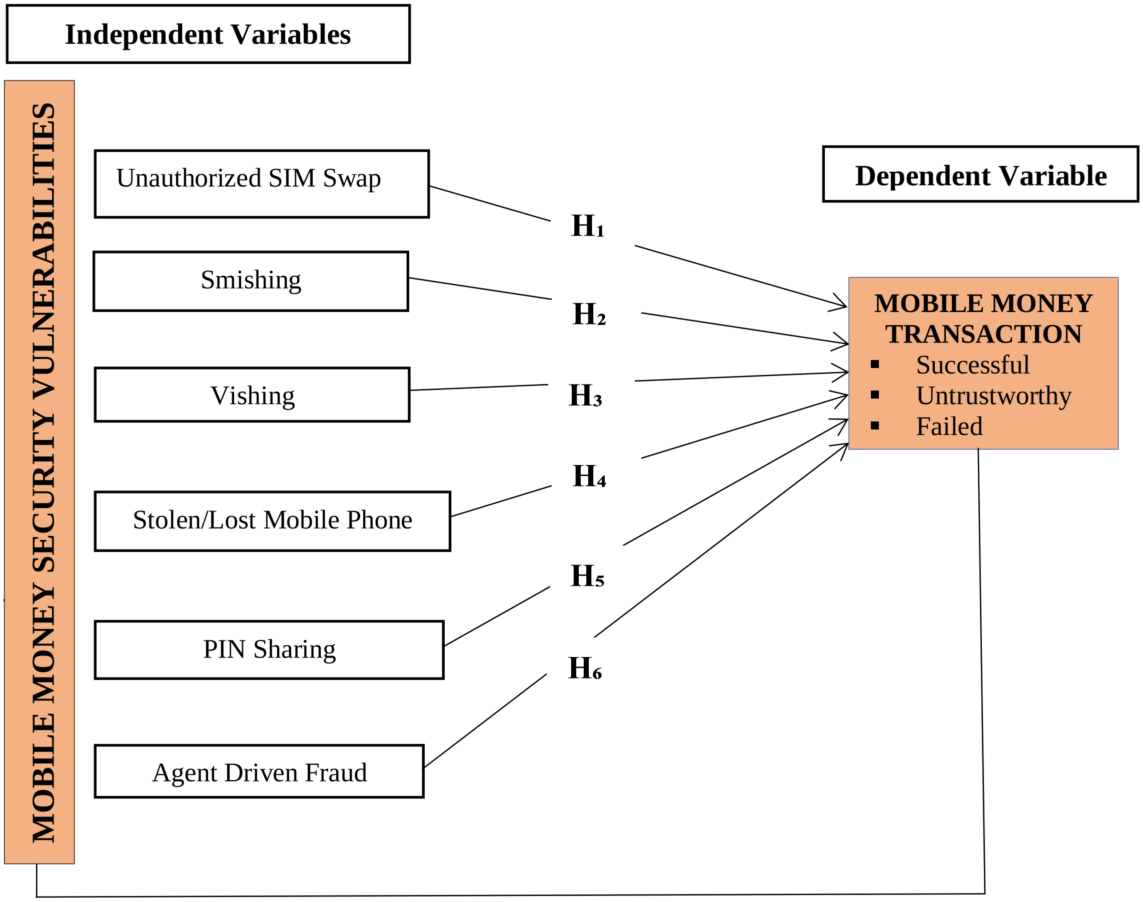


Figure 2: Conceptual Framework for Addressing Security Vulnerabilities Experienced by Registered Mobile Money Clients in Lusaka, Zambia. Source (Author)

3.5 Theoretical Foundations for the Framework

The conceptual framework was underpinned by various theories to strengthen its rigor:

Protection Motivation Theory (PMT): Focuses on how perceived vulnerabilities influence behaviour. Clients adopt secure practices when they understand the risks (e.g., phishing) and the benefits of protective measures.

Routine Activity Theory (RAT): Explains that crime occurs due to the convergence of motivated offenders, suitable targets (e.g., uneducated mobile users), and lack of guardianship (e.g., weak regulations). Interventions address these conditions by increasing guardianship (e.g., enforcement) and reducing vulnerability.

Socio-Technical Systems Theory (STS): Highlights the interaction between technical solutions (e.g., fraud detection systems) and human behaviour (e.g., user education).

Institutional Theory: Emphasizes the role of policies, regulations, and institutional collaborations in addressing systemic challenges like mobile money fraud.

3.6 Research Hypothesis

The study's research hypothesis involved formulating testable statements that explored the relationship between mobile money vulnerabilities (independent variables) and the outcome of a mobile money transaction (dependent variable). The hypotheses served as a foundation for empirical research aimed at enhancing the security and adoption of mobile money services. By investigating these relationships, the researcher was able to recommend strategies to mitigate vulnerabilities and improve user confidence in mobile financial transactions. The following section looks at how the hypothesis was formulated.

Null Hypothesis **(H_0)**: Assumes the mobile money security vulnerabilities related to this research have an effect on the outcome of a mobile money transaction. This will be used to test the relationship between the independent variables and the dependent variable.

Independent Variables

i. **H_1**: An unauthorized SIM Swap has an effect on the outcome of a mobile money transaction.
ii. **H_2**: Smishing has an effect on the outcome of a mobile money transaction.
iii. **H_3**: Vishing has an effect on the outcome of a mobile money transaction.
iv. **H_4**: Stolen/Lost Mobile Phone has an effect on the outcome of a mobile money transaction.
v. **H_5**: PIN Sharing has an effect on the outcome of a mobile money transaction.
vi. **H_6**: Agent Driven Fraud has an effect on the outcome of a mobile money transaction.

Dependent Variable – Mobile Money Transaction

3.7 Operationalization of Variables

(Bryman. A, 2015), Operationalisation is the process of turning abstract ideas or variables into quantifiable, observable terms so that data can be gathered and theories may be tested. It ensures that abstract concepts are well-defined and measurable and other researchers can use the same measurements to repeat the study. Validity and reliability ensure that the study measures what it is intended to measure, and data collection makes it easier for researchers to gather data in an organised manner.

Operationalisation guarantees that variables may be examined and analysed in a methodical manner in research. The steps taken in operationalizing variables include:

Identify the Key Variables: Distinguish between independent, dependent, and mediating variables.

Define the Variables Conceptually: Provide theoretical definitions based on literature.

Translate the Variables into Measurable Terms: Identify indicators and instruments for measurement.

Develop Measurement Scales: Use tools such as Likert scales, numerical scores, or dichotomous categories.

3.7.1 Independent Variables

Unauthorized SIM Swap: Refers to the fraudulent activity where an individual's mobile phone number is transferred to a new SIM card without their knowledge. This is typically done by malicious actors who aim to gain access to the victim's sensitive information, such as personal data, financial accounts, or online services.

Smishing: form of phishing attack that specifically targets individuals through text messages (SMS) or other messaging platforms (such as WhatsApp or Signal). The term "smishing" is a combination of "SMS" (Short Message Service) and "phishing." In smishing attacks, perpetrators use deceptive tactics to trick victims into providing sensitive information, clicking on malicious links, or downloading malware onto their devices.

Vishing: Also known as voice phishing, is a type of social engineering attack where perpetrators use phone calls to deceive individuals into providing sensitive information, such as financial account details, personal identification numbers (PINs), or passwords. The term "vishing" is a combination of "voice" and "phishing."

Stolen/Lost Phone – Refers to a device that has been unlawfully taken from its owner's possession (stolen) or misplaced and cannot be located (lost).

PIN Sharing – This refers to the act of exchanging personal identification numbers (PINs) with another individual, typically for access to restricted information or services. Due to security considerations, this act is frequently discouraged because exchanging PINs might jeopardize the integrity and confidentiality of critical data on the mobile phone.

Agent Driven Fraud – This refers to fraudulent activities carried out by individuals who work within the mobile phone industry. These individuals, often referred to as agents or representatives, exploit their positions or access to carry out fraudulent schemes for personal gain. Some examples of agent driven fraud include unauthorized account access and IMEI (international mobile equipment identity) cloning.

3.7.2 Dependent Variable

Mobile Money Transaction – This refers to financial transactions that are conducted using a mobile device, typically a smartphone, as the primary means of initiating and completing the transaction. Any mobile money transaction performed may be deemed as either being successful, untrustworthy or failed.

A survey questionnaire evaluating the impact and degree of knowledge of mobile money security vulnerabilities was distributed in order to measure the variables chosen for the study. A Likert scale was used for the measurement, where:

SD - Strongly Disagree, D – Disagree, N – Neutral, A – Agree and SA - Strongly Agree

3.8 Chapter Summary

The theoretical foundations upon which the conceptual framework for this study was built were explained in this chapter. The PMT, RAT, DOI, STS, and Institutional Theory were among the theories examined inside that helped build the conceptual framework. The chapter goes on to explain the adoption of Raphael's Mobile Money Transaction Variables Relationship model. The variables considered in this study to better understand the security flaws affecting mobile money transactions were also mentioned in the chapter. The conceptual framework adopted from Raphael was used to inform the creation of survey questions. Following the conceptual framework's recommendations, the following independent variables were chosen: Unauthorised SIM Swap, Smishing, Vishing, Stole/Lost Mobile Phone, PIN Sharing and Agent Driven Fraud. Mobile Money Transaction was the dependent variable. The operationalisation of variables marked the end of the chapter.

CHAPTER 4

RESEARCH METHODOLOGY

4.1 Introduction

This chapter presents the methods and procedures employed in conducting this research. The chapter begins with a discussion of the research design, followed by the research philosophy, the study population, and the sampling techniques used. Data collection methods, instruments, and procedures are then outlined. The chapter also describes the approaches for data analysis and interpretation, ethical considerations, and strategies for ensuring validity and reliability.

The objective of this research is to propose a framework for addressing security vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia. To achieve this, a survey research methodology was adopted to address the research questions and meet the objectives effectively.

In order to collect quantifiable data, the study used a survey research methodology. By using surveys, the researcher was able to effectively reach a large number of respondents and recognise trends among Lusaka's registered mobile money clients. Surveys provide statistically meaningful results with less time and effort in comparison to qualitative techniques like interviews. Because it was able to record user awareness of security measures, the frequency and impact of security breaches, and operator contentment with present security protocols, the survey research approach was pertinent to this study.

4.2 Research Design and Philosophy

(Sekaran et al. 2016), A survey research methodology was chosen as it allows for the systematic collection of quantitative data from a large sample, enabling the identification of patterns, relationships, and the prevalence of mobile money fraud. This approach ensures objectivity, generalizability, and the ability to test hypotheses related to security issues in mobile money usage. A positivist research philosophy was adopted for this research because the aim is to objectively quantify the security vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia. The study follows a deductive approach, starting with hypotheses derived from existing theories such as Protection Motivation Theory and Routine Activity Theory.

According to (Saunders et al. 2019), the survey methodology aligns with the deductive approach by facilitating structured data collection and analysis. This is particularly important for studies that aim to provide measurable insights into specific problems, such as mobile money security.

4.3 Study Population

The capital city of Zambia, Lusaka, was the subject of this study. The core business centre of Lusaka was the primary focus of the study. As of January 2022, Zambia's population of 19,534,694 was estimated to have the following age distribution by countrymeters (2022):

- 46.7% - population under 15 years of age
- 50.8% - population between 15 - 64 years of age
- 2.5% - population over 65 years of age

The population between the ages of 15 and 64 and the population over 65 were the primary age distributions of relevance for the study, according to the figures that were provided. Because they showed a person's eligibility to conduct mobile money transactions, these age distributions were of interest. To conduct mobile money transactions in Zambia, a person must be at least eighteen years old and in possession of a valid National Registration Card (NRC), according to the statutory laws and regulations of Mobile Money Operators (MMO). In order to create the study population, this study concentrated on 53.3% (50.8% + 2.5%) of the entire population.

The entire population of Lusaka City was of interest in order to achieve the set objectives of the study. The population of Lusaka City was 3,042,000, growing 4.68% from 2021, according to macrotrends, 2022. The research's study population was determined by taking 53.3% of 3,042,000. Consequently.

53.3% (eligible age distribution for mobile money transactions) * 3,042,000 (total population of Lusaka City) = 1,621,368

Therefore, the study’s target population was 1,621,368

4.4 Sample Size and Sampling Technique

The sample size refers to the number of participants selected to represent the target population. A well-determined sample size ensures that the study findings are reliable, valid, and generalizable. The target population for this study was 1,621,368 people representing eligible registered mobile money clients. The sample size will be derived using Slovins Formula with 95% precision.

$$n = \frac{N}{1+Ne^2} \qquad \text{Equation (1)}$$

Where;

- n – Sample size
- N – Population size
- e – Margin of error (5% or 0.05)

Therefore, the sample size will be calculated as follows;

$$n = \frac{1{,}621{,}368}{1+1{,}621{,}368(0.05)^2} = 400$$

Consequently, a 95% response rate was attained, making **380** respondents the sample size for this study.

The study utilized a convenience sampling technique to select 380 registered mobile money clients in Lusaka, Zambia. Participants were approached in high-traffic mobile money service points such as markets, shopping malls, and bus stations. This method was chosen due to its feasibility in accessing respondents who are directly involved in mobile money transactions. While this technique may limit generalizability, it provided valuable preliminary insights into the security vulnerabilities experienced by mobile money users in Lusaka. Similar approaches have been employed in exploratory research, as noted by (Bryman 2015) and (Creswell 2018), to generate foundational data for further analysis.

4.5 Data Collection Tools and Procedures

(Dillman et al. 2014), The study employed a structured closed-ended questionnaire administered through Google Forms to collect data from 380 registered mobile money clients in Lusaka. The questionnaire comprised multiple-choice and Likert scale questions designed to identify pertinent security vulnerabilities experienced by registered mobile money clients in Lusaka. Google Forms was chosen for its ease of use and real-time data collection capabilities, which facilitated efficient handling of responses. Some respondents received a link to complete the Google Forms survey via email whilst the majority of respondents received had the link shared with them via social media. To address the limitations of this tool, printed versions were also distributed to ensure inclusivity.

4.5.1 Questionnaires

Participants' experiences and opinions regarding mobile money security flaws were gathered through the creation of questionnaires with closed-ended questions. Questionnaires were selected because of their ease of use with huge populations, their ability to standardise replies for quantitative analysis, and their encouragement of anonymity, which may lead to more truthful responses.

Questionnaires have limitations as a data gathering technique since they run the danger of participants giving socially acceptable answers, especially when it comes to their mobile money security-related behaviours, and they may only be able to capture a small portion of systemic vulnerabilities or individual user behaviours. Due to the fact that participants are not chosen at random and might not accurately reflect the general population, convenience sampling may induce bias. Participants without smartphone literacy or internet access may not be able to complete digital questionnaires, and results may not be entirely generalisable outside of Lusaka or to other demographic groups.

In order to mitigate the drawbacks of surveys, the researcher ensured anonymity, formulated questions in a neutral manner to minimise bias, and integrated observational data with questionnaire results to provide a comprehensive perspective. In order to ensure inclusivity, the researcher offered paper-based alternatives and targeted diverse places to include individuals from a range of backgrounds. Future studies on mobile money security could adopt more representative sampling to address regions beyond Lusaka and other demographic groups.

4.6 Methods for Data Analysis

Data analysis was a crucial step in the study as it involved interpreting collected data to derive meaningful insights and answer the research questions. For this study, addressing the security vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia, the analysis methods align with the structured survey research methodology, focusing on quantitative and some qualitative aspects.

4.6.1 Quantitative Data Analysis

Using descriptive statistics, the features of the gathered data were compiled and displayed in an understandable manner. Its goals were to outline the respondents' demographic profile (including age, gender, and educational attainment), present data on the accessibility and use of mobile money services in Lusaka, and identify the most predominant security vulnerabilities encountered by mobile money clients. Frequency distributions, which illustrate the frequency of particular replies, such as the proportion of respondents who have experienced SIM card swapping, were among the techniques employed. To find average trends, measures of central tendency were employed, and for visual clarity, graphical representations such bar charts, pie charts, and histograms were used.

Inferential Statistics enabled the researcher to draw conclusions about the larger population from the sample data. Its purpose was to test hypotheses related to mobile money security, such as whether there is a significant correlation between security awareness and the likelihood of experiencing fraud. Techniques used include:

Chi-Square Tests: For relationships between categorical variables. E.g. Testing whether awareness of security practices is associated with reduced incidences of fraud.

T-tests or ANOVA: To compare means across groups. E.g. Comparing security concerns between younger and older mobile money users.

Cross-Tabulation Analysis involved analysing the relationship between two or more variables. Its purpose was to understand how demographic factors (e.g., age, income level) relate to specific security vulnerabilities. E.g. Cross-tabulating age groups and the type of fraud experienced.

4.6.2 Limitations of Data Analysis Method

The ability of the quantitative data method to offer comprehensive insights into the "why" of security vulnerabilities was restricted. Where feasible, qualitative data could be added to future mobile money security studies. Data entry mistakes or improper use of statistical tests might emerge from software dependences and produce unreliable results. Double-checking data entry and seeking advice from statistical specialists where necessary were necessary to mitigate this problem.

4.7 Tools for Gathering and Analysing Data

Below is summary of essential tools and their roles used in this study:

Tool	Purpose	Phase
SPSS	Statistical analysis for survey data	Quantitative Analysis
Excel	Data organisation, calculations, and graphs	Quantitative Analysis
Google Forms	Designing and distributing surveys	Data Collection
Printed Questionnaire	Distributing surveys	Data Collection

Table 1: Tools for Gathering and Analysing Data **Source: Author (2023)**

4.8 Ethical Considerations

(Isreal, M et al. 2006), Ethical considerations were fundamental in this research to ensure the integrity of the study and the protection of participants. This section highlights how ethical principles were applied throughout the research process, from planning to reporting findings. Below is a detailed outline of ethical considerations used in this research.

Informed Consent

Informed consent ensured that participants willingly participated in the study with full knowledge of its purpose and implications. Participants were informed about the study's objectives, the voluntary nature of their participation, and the procedures involved. Written or verbal consent was obtained, and participants had the option to withdraw at any stage without penalty. Participants were given the opportunity to ask questions before consenting. Prior to completing the survey, participants had to check a box on the Google Forms questionnaire to indicate their consent.

Confidentiality and Anonymity

Confidentiality involved safeguarding participants’ data, while anonymity ensured that individuals could not be identified. No personal identifiers (e.g., names, phone numbers) were collected. Survey responses were anonymized, and unique codes were used to represent participants.

Voluntary Participation

Participants were not coerced into participating in the study. Clear communication emphasized that participation was entirely voluntary. Participants were reminded of their right to skip questions or withdraw from the study at any time. Email and social media invitations included statements like “Your participation is entirely voluntary and will not affect your access to mobile money services.”

Avoidance of Harm

The research did not expose participants to physical, psychological, or social harm. Questions related to mobile money security were framed to minimize distress or discomfort. Participants were not required to disclose sensitive information that could in any way make them vulnerable. If participants expressed concerns about their security, general guidance on improving mobile money safety and security was shared. Neutral language was used in survey questions to avoid inducing fear, such as “What measures do you use to secure your mobile money account?” instead of “How often have you been defrauded?”

Cultural Sensitivity

In order to ensure proper and respectful participation, it was crucial to take into account the cultural context of Lusaka, Zambia. Clear, locally understood language was employed in the survey design, which took local norms into account. To make sure the questions were pertinent and culturally suitable, the researcher consulted local stakeholders. English and, where necessary, local language interpretations were provided for the surveys.

Ethical Approval

To confirm the research's ethical protections, the researcher received ethical clearance from The University of Zambia's reputable ethics review board. An ethics committee received a comprehensive proposal that included survey tools and consent forms. To validate ethical compliance, feedback from the review process was included into the study.

Responsible Data Handling

Participants' privacy was protected by data protection regulations following proper data management. Information was kept safe and utilised exclusively for the purpose of the study. There was clear adherence to retention standards, with data being erased after a predetermined amount of time. To prevent tracking down specific responses, reporting was done using aggregated data. Data exported from Google Forms was saved in password-protected files and deleted six months after the study concluded.

Transparency and Feedback

Participants were granted full access to information about the research and its outcomes. A summary of the research findings was shared with participants upon request. Transparency built trust and demonstrated the research’s value. An email address and contact number were provided for participants to request a summary of the results.

4.8.1 Limitations of Ethical Safeguard

Despite thorough explanations, several participants were unable to fully comprehend the study's objectives. Using straightforward language and offering opportunity for clarification helped to lessen this problem.

4.9 Reliability and Validity

This section addresses the reliability and validity of the research. Ensuring reliability and validity were crucial to establishing credibility of the findings and to confirm that the data accurately represented the phenomena being studied.

Reliability

Reliability refers to the consistency of the research instrument in measuring the same constructs under similar conditions. For this study, a structured, closed-ended questionnaire administered via Google Forms was used. The following approaches enhanced the reliability of the study:

Internal Reliability: Ensured that all items within the structured, closed-ended questionnaire were consistent. Questions relating to mobile money security practices should yield consistent responses if they measure the same concept. This can be achieved using a Cronbach’s Alpha to test internal consistency.

External Reliability: Ensured that the study results were consistent across different contexts or times. If the survey was repeated with a similar population, the findings should be comparable. Therefore, the research standardized data collection procedures and ensured uniform administration of the questionnaire.

Validity

Validity refers to whether the research instruments measure what they are intended to measure. For this study, the focus was accurately assessing security vulnerabilities and related factors in mobile money usage.

Construct Validity: Ensured the questionnaire truly measured the theoretical constructs it was intended to assess (e.g., security awareness, perceived risks). This was done by developing survey items based on established theories, such as Protection Motivation Theory (PMT), Routine Activity Theory (RAT), and Institutional Theory.

Content Validity: Ensured the questionnaire covered all relevant aspects of the topic. This was done by literature reviews and expert opinions to develop comprehensive survey questions. Questions on types of vulnerabilities, user security practices, and trust in mobile money providers were included in the questionnaire

Criterion Validity: Evaluated the extent to which survey results correlated with external benchmarks or established findings. This was done by comparing findings with existing data on mobile money crimes and user behaviours in Zambia.

Face Validity: Ensured the questionnaire appeared relevant and appropriate to participants and stakeholders. The questionnaire was shared with experts and mobile money clients to validate its relevance.

4.10 Chapter Summary

The research methodology chapter provided a clear and systematic outline of how the study was conducted. It integrated a philosophical stance, adopted a survey research methodology design, structured questionnaires, and statistical analysis and practical tools to address the research objectives. By emphasizing reliability, validity, and ethical principles, the methodology ensured the study was robust and capable of yielding actionable insights into mobile money security vulnerabilities in Lusaka, Zambia.

CHAPTER 5

DATA ANALYSIS AND PRESENTATION

5.1 Introduction

This chapter presents the analysis of data collected to address the security vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia. Data was obtained through structured questionnaires distributed to 380 registered mobile money clients in Lusaka, representing a 95% response rate. The survey encompassed demographic information, security vulnerabilities experienced, security practices and perceptions of mobile money security.

The demographics and mobile money utilization of respondents are described first in this chapter followed by inferential statistics that analysed the relationships between user behaviour and security vulnerabilities.

SPSS (Statistical Package for the Social Sciences) was used for advanced statistical analyses whereas Microsoft Excel was used for data cleaning and presentation of descriptive statistics. Analytical methods employed included descriptive statistics to summarize data, bivariate tests to assess associations between categorical variables, and logistic regression analyses to identify predictors of security vulnerability among users.

5.2 Demographic Information

This section outlines the main trends in the responses and provides a summary of the different demographics that were pertinent to the study. The demographic information offers a thorough understanding of the user population. This knowledge is crucial for determining which user groups are more vulnerable to mobile money security flaws and which groups are more likely to use mobile money services. The demographic information includes gender and age distribution, mobile money services – duration of use, and mobile money operators – service utilization.

5.2.1 Gender Distribution

Gender under demographics revealed 60% of respondents were male whilst 40% were female**.**

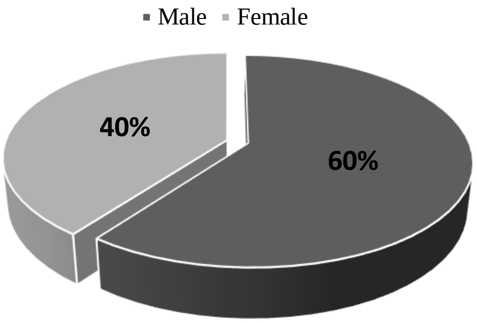
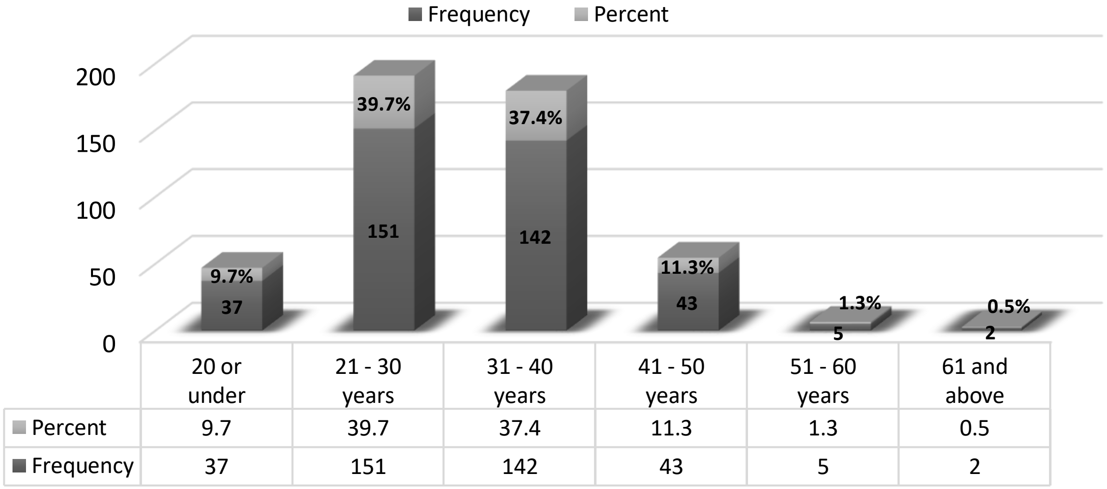


Figure 3: Gender Distribution **Source: Author (2023)**

5.2.2 Age Distribution

Age distribution revealed a majority of 151 respondents represented 39.7% aged between 21 – 30 years of age. 142 respondents represented 37.4% aged between 31 – 40 years whilst 43 respondents represented 11.3% aged between 41 – 50 years. 37 respondents represented 9.7% aged 20 years or under. 5 respondents represented 1.3% aged between 51 – 60 years and 2 respondents represented 0.5% aged 61 years and above.



	20 or under	21 - 30 years	31 - 40 years	41 - 50 years	51 - 60 years	61 and above
▨ Percent	9.7	39.7	37.4	11.3	1.3	0.5
■ Frequency	37	151	142	43	5	2

Figure 4: Age Distribution **Source: Author (2023)**

5.2.3 Mobile Money Services (MMS) – Duration of Use

Figure 5. below revealed a majority of 73% of respondents had been using mobile money services for more than 4 years. 18% of respondents had been using mobile money services for 3 to 4 years whilst 6% of respondents had been using mobile money services for 1 to 2 years. 3% of respondents had been using mobile money services for less than 1 year.

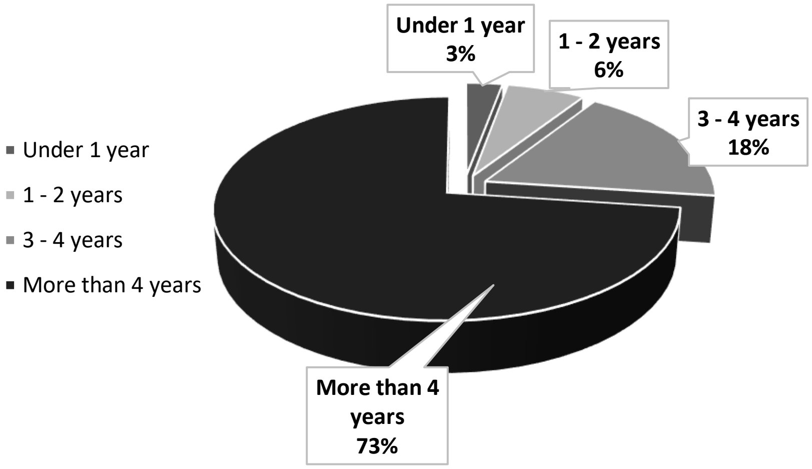


Figure 5: MMS – Duration of Service **Source: Author (2023)**

5.2.4 Mobile Money Operators (MMO) – Service Utilization

The purpose of this kind of analysis was to show how much the respondents used the services offered by the main mobile money operators in Lusaka which are Airtel Money, MTN Mobile Money and Zamtel Mobile Money. The analysis shows the percentage, cumulative percentage, valid percentage, and frequency of respondents' use of each mobile money operator.

5.2.5 Airtel Money

The analysis below shows that a majority of 223 respondents representing 58.7% always used Airtel Money. 98 respondents representing 25.8% often used Airtel Money. 29 respondents representing 7.6% sometimes used Airtel Money whilst 15 respondents representing 3.9% never and rarely used Airtel Money respectively.

Client extent of usage	Frequency	Percent	Valid Percent	Cumulative Percent
Never	15	3.9	3.9%	3.9%
Rarely	15	3.9	3.9%	7.9%
Sometimes	29	7.6	7.6%	15.5%
Often	98	25.8	25.8%	41.3%
Always	223	58.7	58.7%	100%
Total	380	100	100%	

Table 2: Airtel Money Utilization **Source: Author (2023)**

5.2.6 MTN Mobile Money

The analysis below shows a majority of 99 respondents representing 26.1% never used MTN Mobile Money. 90 respondents representing 23.7% always used MTN Mobile Money. 77 respondents representing 20.3% and 75 respondents representing 19.7%, sometimes and often used MTN Mobile Money respectively. 39 respondents representing 10.3% rarely used MTN Mobile Money.

Client extent of usage	Frequency	Percent	Valid Percent	Cumulative Percent
Never	99	26.1	26.1	26.1
Rarely	39	10.3	10.3	36.3
Sometimes	77	20.3	20.3	56.6
Often	75	19.7	19.7	76.3
Always	90	23.7	23.7	100
Total	380	100	100	

Table 3: MTN Mobile Money Utilization **Source: Author (2023)**

5.2.7 Zamtel Mobile Money

The analysis below shows a majority of 233 respondents representing 61.3% never used Zamtel Mobile Money. 52 respondents representing 13.7% rarely used Zamtel Mobile Money whilst 47 respondents representing 12.4% sometimes used Zamtel Mobile Money. 35 respondents representing 9.2% and 13 respondents representing 3.4% often and always used Zamtel Mobile Money respectively.

Client usage preference	Frequency	Percent	Valid Percent	Cumulative Percent
Never	233	61.3	61.3	61.3
Rarely	52	13.7	13.7	75
Sometimes	47	12.4	12.4	87.4
Often	35	9.2	9.2	96.6
Always	13	3.4	3.4	100
Total	380	100	100	

Table 4: Zamtel Mobile Money Utilization **Source: Author (2023)**

5.3 Inferential Statistics

(Bhandari. P, 2023). Inferential statistics involve methods that allowed the researcher to make predictions or inferences about the population using data drawn from a sample. This branch of statistics goes beyond mere description, enabling the testing of hypotheses and the estimation of population parameters. Key aspects of inferential statistics for this study involve hypothesis testing, estimation and generalization. The inferential analysis that was carried out in this research included a normality test, bivariate analysis and regression analysis.

5.4 Normality Test

The normality test assessed whether the sample data were drawn from a population that follows a normal distribution, which is a common assumption for many statistical analyses. The outcomes of the normality test are displayed below. The Shapiro-Wilk test is well suited for sample sizes (<50 samples), according to (Mishra et al. 2019). It can, however, also handle bigger sample sizes. On the other hand, the Kolmogorov–Smirnov test is used for $n \geq 50$. The null hypothesis for both tests mentioned above states that data are taken from a population that is normally distributed. The null hypothesis is accepted, and the data are referred to as normally distributed when $P > 0.05$. This research used the Kolmogorov-Smirnov test results, which were all statistically significant

($p < 0.05$), because the sample size for this population was more than 50. It can therefore be concluded that the variables were not normally distributed as a result.

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Unauthorized Sim Swap	.105	380	.000	.973	380	.000
Vishing	.135	380	.000	.964	380	.000
Smishing	.104	380	.000	.960	380	.000
Stolen/Lost Mobile Phone	.174	380	.000	.933	380	.000
PIN Sharing	.153	380	.000	.960	380	.000
Agent Driven Fraud	.131	380	.000	.963	380	.000

a. Lilliefors Significance Correction

Table 5: Normality Test **Source: Author (2023)**

5.5 Bivariate Analysis

According to (Sarangam, 2021), Bivariate Analysis is a type of statistical analysis in which two variables are observed with each other. One of the variables is independent while the other is dependent. Variables can be indicated by X and Y. In this research, bivariate analysis was done to establish the relationship between Mobile Money Security Vulnerabilities and a Mobile Money Transaction in Lusaka, Zambia. Pearson Correlation Coefficient (*r*) was used to establish the relationship between Mobile Money Vulnerabilities and a Mobile Money Transaction, by ranking the two (02) variables using an ordinal scale. This was done to establish whether there was a relationship between the independent variables and the dependent variable before addressing the main objectives of this research.

5.5.1 Pearson correlation coefficient between Unauthorized SIM Swap and Mobile Money Transaction

		Unauthorized Sim Swap	Mobile Money Transaction
Unauthorized Sim Swap	Pearson Correlation	1	.116*
	Sig. (2-tailed)		.024
	N	380	380
Mobile Money Transaction	Pearson Correlation	.116*	1
	Sig. (2-tailed)	.024	
	N	380	380

*. Correlation is significant at the 0.05 level (2-tailed).

Table 6: Pearson Correlation - Unauthorized SIM Swap **Source: Author (2023)**

Table 6. above shows a Pearson correlation coefficient that was run in order to determine the effect of Unauthorized Sim Swap on a Mobile Money Transaction using responses from the research respondents. The results revealed a weak, positive correlation between Unauthorized Sim Swap and a Mobile Money Transaction (*r* = .116*, *p* = .024). Since *p* < .05, means there is a statistically significant correlation between Unauthorized Sim Swap and a Mobile Money Transaction.

5.5.2 Pearson correlation coefficient between Smishing and Mobile Money Transaction

		Smishing	Mobile Money Transaction
Smishing	Pearson Correlation	1	.264**
	Sig. (2-tailed)		.000
	N	380	380
Mobile Money Transaction	Pearson Correlation	.264**	1
	Sig. (2-tailed)	.000	
	N	380	380

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

Table 7: Pearson Correlation - Smishing **Source: Author (2023)**

Table 7. above shows a Pearson correlation coefficient that was run to determine the effect of Smishing on a Mobile Money Transaction using responses from the research respondents. The results revealed a weak, positive correlation between Smishing and a Mobile Money Transaction (*r* = .264*, *p* = .000). Since *p* < .05, means there is a statistically significant correlation between Smishing and a Mobile Money Transaction.

5.5.3 Pearson correlation coefficient between Vishing and Mobile Money Transaction

		Vishing	Mobile Money Transaction
Vishing	Pearson Correlation	1	.226**
	Sig. (2-tailed)		.000
	N	380	380
Mobile Money Transaction	Pearson Correlation	.226**	1
	Sig. (2-tailed)	.000	
	N	380	380

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

Table 8: Pearson Correlation - Vishing **Source: Author (2023)**

Table 8. above shows a Pearson correlation coefficient that was run to determine the effect of Vishing on a Mobile Money Transaction using responses from the research respondents. The results revealed a weak, positive correlation between Vishing and a Mobile Money Transaction (*r* = .226**, *p* = .000). Since *p* < .05, means there is a statistically significant correlation between Vishing and a Mobile Money Transaction.

5.5.4 Pearson correlation coefficient between Stolen/Lost Mobile Phone and Mobile Money Transaction

		Stolen/Lost Mobile Phone	Mobile Money Transaction
Stolen/Lost Mobile Phone	Pearson Correlation	1	.260**
	Sig. (2-tailed)		.000
	N	380	380
Mobile Money Transaction	Pearson Correlation	.260**	1
	Sig. (2-tailed)	.000	
	N	380	380

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

Table 9: Pearson Correlation - Stolen/Lost Mobile Phone **Source: Author (2023)**

Table 9. above shows a Pearson correlation coefficient that was run to determine the effect of a Stolen/Lost Mobile Phone on a Mobile Money Transaction using responses from the research respondents. The results revealed a weak, positive correlation between a Stolen/Lost Mobile Phone and a Mobile Money Transaction (r = .260**, p = .000). Since $p < .05$, means there is a statistically significant correlation between a Stolen/Lost Mobile Phone and a Mobile Money Transaction.

5.5.5 Pearson correlation coefficient between PIN Sharing and Mobile Money Transaction

		Pin Sharing	Mobile Money Transaction
PIN Sharing	Pearson Correlation	1	.259**
	Sig. (2-tailed)		.000
	N	380	380
Mobile Money Transaction	Pearson Correlation	.259**	1
	Sig. (2-tailed)	.000	
	N	380	380

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

Table 10: Pearson Correlation - PIN Sharing **Source: Author (2023)**

Table 10. above shows a Pearson correlation coefficient that was run to determine the effect of PIN Sharing on a Mobile Money Transaction using responses from the research respondents. The results revealed a weak, positive correlation between a PIN Sharing and a Mobile Money Transaction (r = .259**, p = .000). Since $p < .05$, means there is a statistically significant correlation between PIN Sharing and a Mobile Money Transaction.

5.5.6 Pearson correlation coefficient between Agent Driven Fraud and Mobile Money Transaction

		Agent Driven Fraud	Mobile Money Transaction
Agent Driven Fraud	Pearson Correlation	1	.327**
	Sig. (2-tailed)		.000
	N	380	380
Mobile Money Transaction	Pearson Correlation	.327**	1
	Sig. (2-tailed)	.000	
	N	380	380

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

Table 11: Pearson Correlation - Agent Driven Fraud **Source: Author (2023)**

Table 11. above shows a Pearson correlation coefficient that was run to determine the effect of Agent Driven Fraud on a Mobile Money Transaction using responses from the research respondents. The results revealed a weak, positive correlation between Agent Driven Fraud and a Mobile Money Transaction (r = .327**, p = .000). Since $p < .05$, means there is a statistically significant correlation between Agent Driven Fraud and a Mobile Money Transaction.

5.6 Multiple Regression Analysis (MRA)

A Multiple Regression Analysis (MRA) was run to find the predictors of security vulnerabilities of Mobile Money Transactions. Regression analysis, according to (Gallo, 2015), is a methodological strategy used to determine which factors have an effect. It provides the answers to the questions: Which independent variable should be considered, and which one can be disregarded? How do these components function as a unit? How certain we are about all these elements is possibly the most crucial question? Multiple correlation coefficients are computed via MRA. (Miranda and Fernando, 2020). The percentage of variance in the dependent variable is explained by the independent variable. The beta value, which measures the contribution of the independent variable to the dependent variable, can be described using the p or t statistic.

5.6.1 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.430[a]	.184	.171	4.62272

a. Predictors: (Constant), Unauthorized Sim Swap, Smishing, Vishing, Stolen/Lost Mobile Phone, Pin Sharing, Agent Driven Fraud

Table 12: Model Summary **Source: Author (2023)**

The model above's analysis of mobile money security vulnerabilities revealed that they have the potential to compromise the safety of Mobile Money Transactions in Lusaka, Zambia (R^2 =.184). In this model, the value of R^2 indicates that mobile money security vulnerabilities, such as agent driven fraud, unauthorized sim swaps, stolen/lost mobile phones, vishing, pin sharing, and smishing, can account for 18% of the observed inconsistency in mobile money transactions. However, 82% of the variation in Mobile Money Transactions is not taken into consideration, which indicates that 82% of the variation is connected to other variables that are not shown in the model.

5.6.2 Analysis of Variance (ANOVA)

Table 13. indicates the variance was significant indicated by the F value (F = 14.063) and shows the research had a significant predictive model by $P < 0.01$

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1803.140	6	300.523	14.063	.000[b]
	Residual	7970.847	373	21.370		
	Total	9773.987	379			

a. Dependent Variable: Mobile Money Transaction

b. Predictors: (Constant), Unauthorized Sim Swap, Smishing, Vishing, Stolen/Lost Mobile Phone, Pin Sharing, Agent Driven Fraud

Table 13: Analysis of Variance **Source: Author (2023)**

5.6.3 Regression Coefficients

Coefficients^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.150	1.341		2.350	.019
	Unauthorized Sim Swap	-.063	.074	-.045	-.853	.394
	Smishing	.179	.070	.153	2.553	.011
	Vishing	.083	.078	.061	1.057	.291
	Stolen/Lost Mobile Phone	.242	.086	.144	2.826	.005
	PIN Sharing	.207	.113	.098	1.826	.069
	Agent Driven Fraud	.434	.104	.222	4.166	.000

a. Dependent Variable: Mobile Money Transaction

Table 14: Coefficients Model **Source: Author (2023)**

The Coefficients Model above illustrates which independent variables have a significant effect on the dependent variable. Taking all independent variables (Unauthorized Sim Swap, Smishing, Vishing, Stolen/Lost Mobile Phone, Pin Sharing and Agent Driven Fraud) into account and the dependent variable (Mobile Money Transaction), a P value of < .05 indicates that the independent variable has a significant impact on the dependent variable, thus smishing (.011 < .05), stolen/lost mobile phone (.005 < .05) and agent driven fraud (.000 < .05) means smishing, stolen/lost mobile phone and agent driven fraud have a significant impact on the security of a mobile money transactions whereas unauthorized Sim Swap (.394 > .05), vishing (.291 > .05) and PIN sharing (.069 > .05) have no significant impact on the security of a mobile money transaction.

5.6.4 Chapter Summary

This chapter provided a comprehensive analysis of the data collected on security vulnerabilities among registered mobile money clients in Lusaka, Zambia. Utilizing statistical tools such as SPSS and Microsoft Excel, both descriptive and inferential analyses were carried out to uncover significant patterns and relationships. Key findings included identifying security vulnerabilities, offering valuable insights into the security challenges faced by users. These results addressed the initial research questions and laid the groundwork for the subsequent discussion and formulation of recommendations aimed at enhancing mobile money security in the region.

CHAPTER 6

DISCUSSION OF FINDINGS

6.1 Introduction

This chapter discusses the findings of the study, which aimed to investigate the security vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia. The primary objectives were to assess the availability and utilization of mobile money services, identify security vulnerabilities associated with mobile money transactions and to propose a framework that addresses security vulnerabilities associated with mobile money transactions in Lusaka, Zambia. The analysis revealed significant correlations between security vulnerabilities and mobile money transactions. The discussion interprets the results, compares them with existing literature, and explores their implications for enhancing mobile money security in the region.

6.2 Discussion

This section addresses the research objectives of the study that were highlighted in chapter one. The discussions will provide a concise summary of the main results from the data analysis, focusing mainly on the findings directly related to the research questions and hypothesis.

6.2.1 Availability and Utilization of Mobile Money Services

Objective 1: To assess the availability and utilization of mobile money services in Lusaka, Zambia.

This objective aided in addressing socioeconomic disparities. Analysing utilization across different demographics helped identify and address gaps in access and utilization of mobile money services. The primary tool of choice was closed-ended questionnaires. Whilst the male population made up 60% of the respondents and female 40%, the results showed that 73% of respondents had been using mobile money services for more than 4 years, 18% had been using them for 1–2 years and 3% had been using them for less than a year. This analysis represented a nearly 100% of the sample that have been using mobile money services for at least two years. Minorities made up 9.7% of the age distribution for those under the age of 20, and 3% of those over the age of 51. These two age groups will need to be prioritised for mobile money inclusion.

In Zambia, 58.7% of respondents said they had always used Airtel Money as their preferred mobile money service provider, followed by 23.7% who said they had always used MTN Mobile Money. Most users, 61.3%, said they had never used Zamtel Mobile Money, indicating a lack of customer base for the service compared to other service providers.

The results indicated that mobile money services are widely available and well used in Lusaka, Zambia, however operator-specific services aimed at particular age groups could use some refinement.

6.2.2 Identification of Security Vulnerabilities associated with Mobile Money Transactions

Objective 2: To identify security vulnerabilities associated with mobile money transactions in Lusaka, Zambia.

The literature review addressed the security vulnerabilities associated with mobile money transactions in Zambia. In order to identify the vulnerabilities, a review of the literature on mobile money crimes in Zambia and throughout Africa was conducted. This analysis revealed common flaws, which were then further examined in chapter five. By reviewing publications that detailed mobile money crimes from 2022 to 2024 in Zambia, the precise vulnerabilities used for analysis and discussion in this study were chosen. Further knowledge of these security issues and the current solutions implemented was further aided by interactions with regulatory agencies, cybersecurity experts, and mobile money service providers. According to Ali et al. (2020), identity theft, authentication attacks, phishing attacks, vishing attacks, smishing attacks, PIN sharing, and agent-driven fraud are the main security concerns related to mobile money security in Uganda. Unauthorized sim swap, smishing, vishing, stolen or lost mobile phone, PIN sharing, and agent-driven fraud were the key vulnerabilities identified for this study.

6.2.3 Proposed Modified Conceptual Framework for Security Vulnerabilities

Objective 3: To propose a framework that addresses security vulnerabilities associated with mobile money transactions in Lusaka, Zambia.

The conceptual framework for addressing security vulnerabilities experienced by registered mobile money clients in Lusaka, Zambia was devised by adapting the mobile money transaction variables relationship model by (Raphael. G, 2016). The proposed conceptual framework for this study was discussed in the theoretical/conceptual models/frameworks section of this study and was underpinned by various theories to strengthen its rigor. It identified the security vulnerabilities in mobile money transactions that affected registered mobile money clients in Lusaka.

The regression coefficients test was run to determine which mobile money security vulnerabilities had a significant effect on a mobile money transaction. This was interpreted in the sections to follow as it played a key role in devising the proposed modified conceptual framework for addressing security vulnerabilities experienced by registered mobile money clients in Lusaka.

6.2.3.1 Interpretation of Coefficients Model

In the research's analysis and presentation section, the regression coefficients test was conducted. The purpose of the test was to determine how the independent variables affected the dependent variable. The null hypothesis (H_0) hypothesized that the security vulnerabilities in mobile money had a significant effect on the outcome of a mobile money transaction. This was used to test the relationship between the independent variables and the dependent variable. Based on the results of the coefficients model, a P value of less than .05 indicated that the independent variable had a significant effect on the dependent variable (mobile money transaction) Therefore;

a **H_1**: Unauthorized SIM Swap had a P value of .394, subsequently, this means the null hypothesis was rejected (.394 > .05). Therefore, unauthorized sim swap had no significant effect on the security of a mobile money transaction.

b **H_2**: Smishing had a P value of .011, subsequently, this means the null hypothesis failed to reject (.011 < .05). Therefore, smishing had a significant effect on the security of a mobile money transaction.

c **H_3**: Vishing had a P value of .291, subsequently, this means the null hypothesis was rejected (.291 > .05). Therefore, vishing had no significant effect on the security of a mobile money transaction.

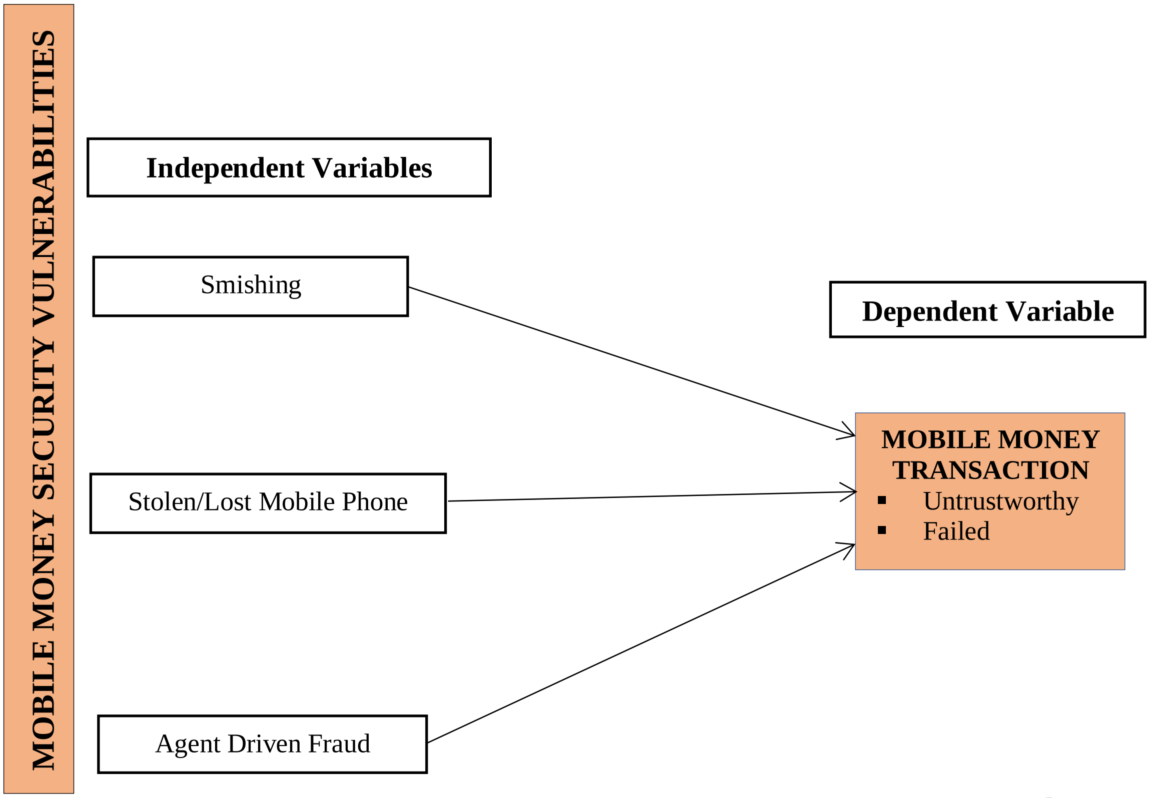
d **H_4**: Stolen/Lost Mobile Phone had a P value of .005, subsequently, this means the null hypothesis failed to reject (.005 < .05). Therefore stolen/lost mobile phone had a significant effect on the security of a mobile money transaction.

e **H_5**: PIN Sharing had a P value of .069, subsequently, this means the null hypothesis was rejected (.069 > .05). Therefore, PIN sharing had no significant effect on the security of a mobile money transaction.

f **H_6**: Agent Driven Fraud had a P value of .000, subsequently, this means the null hypothesis failed to reject .000 < .05. Therefore, PIN sharing had a significant effect on the security of a mobile money transaction.

6.2.3.2 Proposed Modified Conceptual Framework

Based on the interpretation of the regression coefficients model, variables H_2 (Smishing), H_4 (Stolen/lost mobile phone) and H_6 (Agent driven fraud) had a significant effect on the security of a mobile money transaction. The resulted in the preposition of a modified conceptual framework to address security vulnerabilities experienced by registered mobile money clients in Lusaka. This is illustrated below.



Source (Author)

Figure 6: Proposed Modified Conceptual Framework for Addressing Security Vulnerabilities Experienced by Registered Mobile Money Clients in Lusaka, Zambia.

6.3 Summary of Hypothesis Results

The results of the hypothesis that was used to determine the strength of the correlations between the variables are summarised below.

Hypothesis	Path	t	Sig.	Decision
H_1	Unauthorized sim swap has an effect on the outcome of a mobile money transaction.	-.853	.394	Hypothesis not supported
H_2	Smishing has an effect on the outcome of a mobile money transaction.	2.553	.011	Hypothesis supported
H_3	Vishing has an effect on the outcome of a mobile money transaction.	1.057	.291	Hypothesis not supported
H_4	Stolen/lost mobile phone has an effect on the outcome of a mobile money transaction.	2.826	.005	Hypothesis supported
H_5	PIN sharing has an effect on the outcome of a mobile money transaction.	1.826	.069	Hypothesis not supported
H_6	Agent driven fraud has an effect on the outcome of a mobile money transaction.	4.166	.000	Hypothesis supported

Table 15: Summary of Hypothesis Results Source: Author (2023)

6.4 Proposed Solutions to Address Security Vulnerabilities

(GSMA 2019). Resolving security vulnerabilities that affect mobile money transactions requires a combined effort of regulatory authorities, mobile money service providers and users of mobile money services. Below are some proposed solutions to address the security vulnerabilities that had a significant effect on mobile money transactions.

6.4.1 Smishing

Education and Awareness Campaigns: Content used for educating and awareness campaigns must illustrate real-life examples of smishing attempts to educate clients. Delivery channels should employ SMS, email, radio, and community outreach programs. Regular updates will keep the public informed about new fraud trends.

Sender Verification: Mobile network operators must work closely with users of mobile money services to enforce sender ID registration. MNO’s must use a whitelist of verified senders and block unregistered users. Implementing a client interface displaying a verified badge next to messages of the sender would uphold legitimate entities.

SMS Filtering: This requires development and implementation of AI and machine learning systems to analyse and block phishing SMS patterns. These systems would be capable of flagging messages with suspicious links or requests for personal data. Mobile network operators must leverage user-reported data (feedback) to improve filtering mechanisms.

Two-Factor Authentication (2FA): Implementation options can include time-based OTPs sent via SMS or generated by an application (for smartphones users). Users can also opt for a biometric validation combined with a PIN entry for more advanced security. In order to support the inclusion of both rural and urban groups, service providers must always make sure the 2FA procedure is simple and adaptable.

6.4.2 Lost/Stolen Mobile Phone

SIM Locking and Remote Deactivation: This feature allows clients to deactivate their wallets via a secure online portal or customer service hotline. This feature must be immediate, user-friendly and robust for maximum efficiency. Mobile network operators must implement rapid response times (e.g. Within 5 minutes) from time of reporting.

PIN and Biometric Security: Enhanced PIN requirements can be enforced by regular PIN updates and by prohibiting weak PINs (e.g., “1234”). Users of smart mobile devices must always opt for device-native features such as fingerprints, facial recognition and encrypting device data for additional security.

Transaction Limitations: Mobile money operators can enforce tiered limits by introducing lower limits for transactions from new or unverified devices. Higher limits can then be only enabled for trusted and verified users/devices. An emergency feature allowing clients to freeze their wallet temporarily via a self-service option should be implemented by mobile money operators.

Device Binding: The registration process must require a one-time device registration using a secure application or OTP. Alerts can notify users when a new device attempts to access their account.

6.4.3 Agent-Driven Fraud

Agent Vetting and Training: Detailed background and security checks must be conducted by mobile network operators before appointing agents. Subsequent to initial agent-operator training, mobile network operators must conduct periodic refresher courses on anti-fraud measures and customer service ethics. Agents must be required to sign and adhere to anti-fraud code of conduct.

Transaction Monitoring: This can be achieved by real-time analysis that uses AI and machine learning algorithms to identify suspicious activity, including repetitive reversals or transactions with unusually high values. Upon occurrence, flagged transactions must be automatically escalated to a compliance team for evaluation.

Client Feedback Mechanisms: Reporting channels for fraud should include SMS-based systems, mobile apps, or toll-free hotlines. It should be encouraged to report actual agent fraud by offering incentives like minor prizes.

Agent Accountability: Mobile money operators and regulatory authorities must ensure all agent transactions are logged with timestamps and GPS data. Penalties, and imposing strict consequences, such as termination or legal action for fraud must be generalized. To promote transparency mobile money operators must publish regular reports on disciplinary actions taken against fraudulent agents.

Audits and Inspections: Monthly or quarterly audits, along with random inspections, are required of mobile money operators. Technology could be used to implement auditing techniques that verify agent operations in real-time on-site.

6.5 Chapter Summary

This chapter analyzed the results of the research, providing insights into the security vulnerabilities faced by registered mobile money clients and exploring the practical implications of these findings. The key areas discussed included smishing, risks associated with lost or stolen mobile phones, and agent-driven fraud.

Education campaigns and improved SMS filtering systems were highlighted as crucial interventions for smishing. Two-factor authentication (2FA) was also identified as a robust solution to mitigate unauthorized access. Introducing remote SIM locking, transaction limits for new devices, and enhanced PIN policies were proposed as key measures to improve mobile phone security. Regular agent audits, transaction monitoring, and mandatory training programs were suggested to enhance accountability and reduce agent-driven fraud.

The chapter underscored the interconnected nature of technological, operational, and human factors in addressing security vulnerabilities. The proposed solutions aim to create a safer and more trustworthy mobile money ecosystem in Lusaka, Zambia.

CHAPTER 7

CONCLUSIONS AND RECOMMENDATIONS

7.1 Introduction

This chapter consolidates the findings of the study on security vulnerabilities in Zambia's mobile money sector, specifically in Lusaka. It presents conclusions drawn from the analysis of the challenges related to smishing, lost/stolen mobile phones, and agent-driven fraud. It further provides actionable recommendations aimed at enhancing the security framework of mobile money services in Zambia. The goal is to support stakeholders in creating a secure and reliable financial ecosystem.

7.2 Summary of Key Findings

Smishing: The study revealed that smishing is a pervasive threat, with fraudsters exploiting clients' limited awareness to steal personal data. This challenge is exacerbated by the lack of SMS filtering technologies and insufficient client education.

Lost/Stolen Mobile Phones: Inadequate security measures, such as weak PINs and the absence of remote locking or deactivation options, pose significant risks when devices are lost or stolen.

Agent-Driven Fraud: The findings highlighted gaps in agent training, accountability, and monitoring, which allow fraudulent activities by unscrupulous agents to thrive.

Cross-Cutting Themes: Limited awareness among clients and weak enforcement of security protocols were consistent across all vulnerabilities.

7.3 Conclusions for Key Findings

Smishing: The proliferation of smishing in Zambia's mobile money sector reflects systemic gaps in client education and technological defences. The absence of robust SMS filtering systems and sender verification mechanisms leaves clients vulnerable to smishing attacks.

Lost/Stolen Mobile Phones: Lost or stolen devices remain a critical security vulnerability due to weak personal identification number (PIN) policies and the lack of advanced security features such as biometrics or remote wallet deactivation. This exposes clients to unauthorized access and financial losses.

Agent-Driven Fraud: Agent-driven fraud is fuelled by inadequate training and supervision of agents, alongside ineffective monitoring systems. This not only erodes client trust but also undermines the credibility of mobile money operators in Zambia.

Systemic Issues: The findings underscore the interconnected nature of these vulnerabilities, emphasizing the need for a coordinated response involving clients, mobile operators, and regulators.

7.4 Recommendations

7.4.1 Policy Recommendations

Regulatory Oversight: The Bank of Zambia should enforce stricter compliance with mobile money security protocols, including mandatory reporting of fraud incidents and penalties for non-compliance.

Collaboration: Establish partnerships between mobile operators, financial institutions, and government agencies to develop national guidelines for mobile money security.

7.4.2 Operational Recommendations

Client Education Campaigns: Launch nationwide campaigns to educate clients on recognizing fraud, securing their accounts, and reporting suspicious activities. Leverage local languages and community networks to maximize reach.

Agent Oversight: Implement real-time transaction monitoring systems and conduct regular audits to identify and address fraudulent agent activities.

Support Services: Enhance client support services by introducing 24/7 helplines and self-service options for reporting fraud or deactivating accounts.

7.4.3 Technical Recommendations

Smishing Mitigation: Deploy SMS filtering technologies using AI to identify and block smishing attempts. Working with mobile network operators to implement sender verification mechanisms.

Enhanced Device Security: Introduce advanced authentication options, such as biometrics, and enable remote wallet deactivation through mobile apps or USSD codes.

Fraud Detection: Leverage machine learning algorithms to detect patterns of fraudulent transactions in real time.

7.4.4 Client-Focused Recommendations

Security Alerts: Send regular SMS or app-based alerts about new fraud tactics and provide tips for safeguarding accounts.

Feedback Mechanisms: Create simple reporting tools for clients to flag suspicious agents or transactions.

7.5 Research Contributions

This study makes significant contributions to the understanding of security vulnerabilities in mobile money services, focusing on smishing, lost/stolen mobile phones, and agent-driven fraud. The contributions are categorized as follows:

7.5.1 Theoretical Contributions

Expanded Knowledge of Mobile Money Security: The research adds to the body of knowledge on security challenges in mobile money ecosystems, particularly in developing countries like Zambia. It highlights unique vulnerabilities shaped by socio-economic and technological factors in Lusaka.

Framework Development: A conceptual framework was proposed to address security vulnerabilities. This framework integrates technical, operational, and user-centric approaches, providing a comprehensive model for enhancing mobile money security.

7.5.2 Practical Contributions

Guidance for Mobile Money Operators: The study provides actionable recommendations for operators to enhance security, such as implementing advanced authentication measures, SMS filtering systems, and client education campaigns.

Agent Oversight and Accountability: The research emphasizes the importance of regular audits, real-time transaction monitoring, and agent training to prevent fraud.

Client Empowerment: By identifying knowledge gaps, the study informs strategies for improving user awareness and proactive security practices.

7.5.3 Policy Contributions

Regulatory Insights: The findings offer valuable input for regulators, such as the Bank of Zambia, to develop and enforce comprehensive security policies for mobile money services.

National Security Strategy: The research aligns with Zambia’s digital financial inclusion goals, contributing to a secure and trustworthy mobile money ecosystem that supports economic growth and financial inclusion.

7.5.4 Methodological Contributions

Context-Specific Analysis: The study uses a case study approach tailored to Lusaka, Zambia, providing localized insights that can be applied to similar urban centres in sub-Saharan Africa.

Stakeholder Engagement: By incorporating perspectives from mobile money clients, agents, and operators, the study ensures that the findings and recommendations address the concerns of all key stakeholders.

7.5.5 Contributions for Future Research

Foundation for Comparative Studies: The findings serve as a baseline for comparative studies between Zambia and other countries facing similar challenges in mobile money security.

Emerging Threats: The study identifies potential areas for future research, such as the impact of mobile app-based fraud and the role of artificial intelligence in enhancing fraud detection.

By addressing a critical issue in Zambia’s financial ecosystem, this research contributes to both academic discourse and practical advancements, offering solutions that are both innovative and implementable.

7.6 Limitations and Future Research Directions

7.6.1 Limitations

While this research provides valuable insights into addressing security vulnerabilities in mobile money services, it is important to acknowledge its limitations:

Geographical Scope: The study focused exclusively on registered mobile money clients in Lusaka, Zambia. This urban-centric approach may not fully capture the challenges experienced in rural or peri-urban areas where access to resources and technological infrastructure differs significantly.

Dynamic Nature of Fraud: Mobile money fraud tactics evolve rapidly. The findings of this study are based on data collected within a specific timeframe and may not account for emerging threats or novel techniques developed by fraudsters post-study.

Limited Stakeholder Representation: Although the study included insights from clients, agents, and operators, it did not extensively incorporate views from regulators, law enforcement, or independent cybersecurity experts, whose input could provide a broader understanding of systemic vulnerabilities.

Technology-Specific Constraints: The research focused on existing mobile money platforms and technologies. It did not analyse the potential risks or security measures associated with newer technologies, such as blockchain or decentralized finance systems, which may become relevant in Zambia.

Data Availability and Reliability: Some respondents may have underreported or misrepresented their experiences with fraud due to stigma or fear of repercussions, potentially affecting the accuracy of the findings.

7.6.2 Future Research Directions

Building on the findings and addressing the limitations of this study, future research could explore the following areas:

Expanding Geographical Scope: Conduct comparative studies between urban, peri-urban, and rural areas in Zambia to understand how varying access to infrastructure, education, and economic conditions impact security vulnerabilities in mobile money services.

Emerging Threats and Technologies: Investigate new forms of fraud, such as mobile app-based attacks and fraud targeting contactless payment systems. Explore the role of advanced technologies like blockchain, artificial intelligence, and machine learning in improving mobile money security.

Regulatory and Policy Analysis: Examine the effectiveness of existing regulatory frameworks for mobile money in Zambia. Analyse how policy changes, such as mandatory fraud reporting and cybersecurity laws, influence the prevalence and mitigation of fraud.

User-Centric Research: Conduct longitudinal studies to assess the impact of security education campaigns on client awareness and behaviour. Explore the psychological and socio-economic factors influencing clients' susceptibility to fraud.

Collaboration and Stakeholder Engagement: Evaluate the role of multi-stakeholder collaborations, involving mobile operators, regulators, law enforcement, and international organizations, in combating mobile money fraud.

Rural and Vulnerable Populations: Investigate how mobile money security challenges differ among vulnerable groups, such as women, the elderly, and people with disabilities, and propose tailored solutions to address their needs.

Framework Validation: Test the proposed framework in real-world settings to evaluate its effectiveness in reducing security vulnerabilities and enhancing trust in mobile money systems.

By addressing these limitations and pursuing the outlined future research directions, a more comprehensive understanding of mobile money security in Zambia can be achieved, ultimately fostering a safer and more inclusive financial ecosystem.

7.7 Chapter Summary

The Conclusions and Recommendations chapter served as a critical synthesis of the research findings and their practical implications for enhancing mobile money security in Lusaka, Zambia. This discussion focused on connecting the study's findings to broader themes in mobile money ecosystems, identifying actionable steps to address security vulnerabilities, and highlighting the potential for systemic transformation.

This chapter underscored the transformative potential of targeted security interventions in the mobile money ecosystem. By addressing vulnerabilities systematically, Zambia can pave the way for a safer and more inclusive financial future.

REFERENCES

1. Aker, J.C. and Wilson, K., 2013. Can mobile money be used to promote savings? Evidence from northern Ghana. World Development, 55, pp.394–411.ADSource Zambia - Mobile Money Services in Zambia [www document], 2019. url:https://adsourcezm.com/mobile-money-services-in-zambia/ (accessed 9.10.20).
2. Africa's mobile money industry is infiltrated by crime [www document], n.d. Cash Essentials. url:https://cashessentials.org/africas-mobile-money-industry-is-infiltrated-by-crime/(accessed 4.25.24).
3. Airtel Zambia, 2022. Airtel Zambia Launches 'Be Fraud Alert' Campaign [www document]. Tech Trends. url:https://www.techtrends.co.zm/airtel-zambia-launches-be-fraud-alert-campaign/ (accessed 1.20.22).
4. Ali, G., Ally Dida, M., Elikana Sam, A., 2020. Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda. Information 11, 309. https://doi.org/10.3390/info11060309
5. Ambore, S., Richardson, C., Dogan, H., Apeh, E., Osselton, D., 2017. A resilient cybersecurity framework for Mobile Financial Services (MFS). Journal of Cyber Security Technology 1, 202–224. https://doi.org/10.1080/23742917.2017.1386483
6. Are the Pacific Islands Ripe for Mobile Money? · DAI Publications [www document], 2024. url:https://dai-global-developments.com/articles/are-the-pacific-islands-ripe-for-mobile-money/ (accessed 12.10.24).
7. Aron, J., 2018. Mobile Money and the Economy: A Review of the Evidence. The World Bank Research Observer 33, 135–188. https://doi.org/10.1093/wbro/lky001
8. Bada, M., Nurse, J.R.C., 2020. The social and psychological impact of cyberattacks, in: Emerging Cyber Threats and Cognitive Vulnerabilities. Elsevier, pp. 73–92. https://doi.org/10.1016/B978-0-12-816203-3.00004-6
9. Babbie, E. R. (2020). The Practice of Social Research (15th Edition). Cengage Learning.
10. Banda, G., n.d. The Development of Mobile Money Operators: Implications for ZANACO Mobile Banking Customers in Lusaka.

11. Banda, G. and Kachingwe, N., 2020. An analysis of mobile money fraud in Zambia: Causes, trends, and prevention strategies. International Journal of ICT Research, 3(2), pp.45–60.
12. Bhandari, P. (2023, June 22). Inferential Statistics | An Easy Introduction & Examples. Scribbr. Retrieved December 19, 2024, from https://www.scribbr.com/statistics/inferential-statistics
13. Berdibayev, Y., Kwon, Y., n.d. Improving digital financial services inclusion: A panel data analysis.
14. Bryman, A., 2015. Social research methods. 5th ed. Oxford: Oxford University Press.
15. Brazil Mobile Payment Market Size & Outlook, 2030 [www document], n.d. url: https://www.grandviewresearch.com/horizon/outlook/mobile-payment-market/brazil (accessed 12.10.24).
16. Baxter, G., & Sommerville, I. (2011). "Socio-Technical Systems: From Design Methods to Systems Engineering." Interacting with Computers.
17. Chisanga, J. and Kabwe, Z., 2021. Security challenges in mobile money services in Zambia: A user-centric approach. African Journal of Financial Technology, 3(2), pp.45–58.
18. Churchill, G.A. and Iacobucci, D., 2018. Marketing research: Methodological foundations. 12th ed. Boston: Cengage Learning.
19. Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications.
20. Cohen, L. E., & Felson, M. (1979). "Social Change and Crime Rate Trends: A Routine Activity Approach." American Sociological Review, 44(4), 588–608.
21. Coventry, D.L., n.d. Using behavioural insights to improve the public’s use of cyber security best practices.
22. Cybercrime weighs most heavily on financial service firms [www document], 2018. WeLiveSecurity. url:https://www.welivesecurity.com/2018/02/20/cybercrime-weighs-financial-services/ (accessed 3.19.20).
23. Cybercriminals are increasingly targeting the financial services industry [www document], 2019. SC Media. url:https://www.scmagazine.com/home/opinion/executive-

insight/cybercriminals-are-increasingly-targeting-the-financial-services-industry/ (accessed 3.17.20).

24. Cybersecurity Profile: Tanzania and Mobile Money Use, 2017. The Henry M. Jackson School of International Studies. url:https://jsis.washington.edu/news/cybersecurity-profile-tanzania-mobile-money-use/ (accessed 5.13.21).
25. Digital Finance: Cybersecurity Requires Deeper Industry Collaboration [www document], n.d. url:https://www.cgap.org/blog/digital-finance-cybersecurity-requires-deeper-industry-collaboration (accessed 3.17.20).
26. Dillman, D.A., Smyth, J.D. and Christian, L.M., 2014. Internet, phone, mail, and mixed-mode surveys: The tailored design method. 4th ed. Hoboken: Wiley.
27. DiMaggio, P. J., & Powell, W. W. (1983). "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." American Sociological Review.
28. Diogenes, Y., Ozkaya, E., 2018. Cybersecurity, attack and defense strategies: infrastructure security with Red Team and Blue Team tactics. Packt Publishing, Birmingham.
29. ERIC - ED551711 - An Exploratory Multi-Method Analysis of Cybercrime Perpetrators' Perceptions to Combat Cyber Crime in Sub Saharan Africa: The Case of Cameroon, ProQuest LLC, 2012 [www document], n.d. url: https://www.eric.ed.gov/(accessed 3.15.20).
30. ERIC - EJ981532 - Examining Willingness to Attack Critical Infrastructure Online and Offline, Crime & Delinquency, 2012-Sep [www document], n.d. url:https://www.eric.ed.go/ (accessed 3.15.20).
31. Etikan, I., Musa, S.A. and Alkassim, R.S., 2016. Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), pp.1-4.
32. Financial Inclusion through the use of Mobile Money, 2022. Financial Insights. url: https://fizambia.com/financial-inclusion-through-the-use-of-mobile-money/ (accessed 11.25.24).
33. FM Contributors, 2023. The Mobile Money Revolution: Lessons from Africa [www document]. Finance Magnates.

url:https://www.financemagnates.com/fintech/payments/the-mobile-money-revolution-lessons-from-africa/

34. Gaber, C., Gharout, S., Achemlal, M., Pasquet, M., Urien, P., n.d. Security challenges of mobile money transfer services.
35. Giandomenico, A., 2019. Cybercrime Trends and Financial Services [www document]. Fortinet Blog. URL https://www.fortinet.com/blog/industry-trends/cybercrime-trends-and-financial-services.html (accessed 3.17.20).
36. Global Mobile Money Market Report 2024 - Mobile Money Market Drivers And Scope To 2033 [www document], n.d. url: https://www.thebusinessresearchcompany.com/report/mobile-money-global-market-report (accessed 12.10.24).
37. Gombiro, C., Jantjies, M., Mavetera, N., 2015. A conceptual framework for detecting financial crime in mobile money transactions. JGR 4, 727–734. https://doi.org/10.22495/jgr_v4_i4_c6_p8
38. Griffiths, C., n.d. The Latest Cyber Crime Statistics (updated February 2024) | AAG IT Support [www document]. url:https://aag-it.com/the-latest-cyber-crime-statistics/ (accessed 2.2.24).
39. Groves, R.M., Fowler, F.J., Couper, M.P., Lepkowski, J.M., Singer, E. and Tourangeau, R., 2011. Survey methodology. 2nd ed. Hoboken, NJ: Wiley.
40. GSMA. (2020). "Mobile Money Policy and Regulatory Handbook."
41. GSMA. (2022). State of the Industry Report on Mobile Money.
42. Gupta, S., & Xu, H. (2010). "Examining the Socio-Technical Dynamics of IT Security Compliance." Information Systems Research.
43. Hazlegreaves, S., 2019. How financial services combat the threat of cyber crime? Open Access Government. url:https://www.openaccessgovernment.org/financial-services-threat-of-cybersecurity/69023/ (accessed 3.17.20).
44. How, mobile money revolutionized digital financial inclusion, 2024. url:https://zota.com/blog/payments/how-mobile-money-revolutionized-digital-financial-inclusion/ (accessed 12.11.24).

45. Iluba, E., Phiri, J., 2021. The FinTech Evolution and Its Effect on Traditional Banking in Africa—A Case of Zambia. OJBM 09, 838–850. https://doi.org/10.4236/ojbm.2021.92043
46. In Zambia, Scams on the Rise as Mobile Money Booms [www document], 2019. Global Press Journal. url:https://globalpressjournal.com/africa/zambia/zambia-scams-rise-mobile-money-booms/ (accessed 6.5.22).
47. Inambao, W., Phiri, J., Kunda, D., 2018. Digital Identity Modelling for Digital Financial Services in Zambia. ICTACT Journal on Communication Technology.
48. Invest in Africa: Mobile Money Transactions Rise 22% to $836.5bn [www document], n.d. Dabafinance.url:https://dabafinance.com/en/learn/updates/investors-update-may-22-2023 (accessed 12.10.24).
49. ‘New Mobile Money Service Welcomed as a tool for Financial Inclusion in Solomon Islands [www document], n.d. url:https://www.uncdf.org/article/8665/its-instant-and-hassle-free-new-mobile-money-service-welcomed-as-a-tool-for-financial-inclusion-in-solomon-islands (accessed 12.10.24).
50. Jack, W. and Suri, T., 2014. Risk sharing and transactions costs: Evidence from Kenya's mobile money revolution. American Economic Review, 104(1), pp.183–223.
51. Jones, n.d. Is Mobile Banking Safe? 10 Potential Risks to Know [www document]. url:https://www.identityguard.com/news/risks-of-using-mobile-banking-apps (accessed 2.1.24).
52. July 14th, C. 19th O. 2015, 2023, 2015. The basics of Mobile Money Security. Comviva. url: https://www.comviva.com/blog/references/the-basics-of-mobile-money-security/ (accessed 12.9.24).
53. Kathuria, S., 2019. Top 5 benefits of using a security framework [www document]. Medium.url:https://medium.com/microsoft-cybersecurity/top-5-benefits-of-using-a-security-framework-ab8485dec000 (accessed 11.10.21).
54. Kitime, E., 2018. A Framework of Cybersecurity Risks on Mobile Money Users in Tanzania: A Case Study of Dodoma City 124.
55. Leukfeldt, E. R., & Yar, M. (2016). "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis." Deviant Behaviour, 37(3), 263–280.

56. Luchembe, C., Siame, C.L., 2018. Mobile Money for increased financial access url: https://www.fsdzambia.org/mobile-money-for-increased-financial-access-weve-got-your-back/ (accessed 9.10.20).
57. Lusaka Population 2022 (Demographics, Maps, Graphs) [www document], n.d. url:https://worldpopulationreview.com/world-cities/lusaka-population(accessed 6.30.22).
58. Lusaka, Zambia Metro Area Population 1950-2022 [www document], n.d. url:https://www.macrotrends.net/cities/23277/lusaka/population (accessed 6.30.22).
59. Makin, P., 2018. Cybersecurity for Mobile Financial Services: A Growing Problem [www document]. CGAP (Consultative Group to Assist the Poor). url:https://www.cgap.org/blog/cybersecurity-mobile-financial-services-growing-problem (accessed 5.13.21).
60. Malakata, M., 2020. MTN Zambia notches up 4.5m mobile money customers [www document]. ITWeb Africa. url:https://itweb.africa/content/mQwkoq6PLQb73r9A (accessed 12.13.24).
61. Martin, A., 2019. Mobile Money Platform Surveillance. Surveillance & Society 17, 213–222. https://doi.org/10.24908/ss.v17i1/2.12924
62. Mbunji, P., Kaira, B., 2024. An Investigation of the Impact of Mobile Money Services on the Profitability of Commercial Banks in Zambia. IJRISS VIII, 2772–2788. https://doi.org/10.47772/IJRISS.2024.804262
63. McGill, T., & Thompson, N. (2017). "Beyond Intention: Examining the Relationship Between Security Measures and Actual Behaviours." *Computers & Security*.
64. Milne, S., Sheeran, P., & Orbell, S. (2000). "Prediction and Intervention in Health-Related Behaviour: A Meta-Analytic Review of Protection Motivation Theory." Journal of Applied Social Psychology.
65. Mkalipi, Y.S., n.d. The Effect of Mobile Network Operators on Financial Inclusion in Zambia.
66. Mobile money transfers [www document], 2023. MoneyTransfers.com. url:https://moneytransfers.com/sending-money/mobile-money (accessed 6.11.23).
67. Mobile money [www document], 2017. url:https://www.worldremit.com/en/faq/mobile-money

68. Moustafa, A.A., Bello, A., Maurushat, A., 2021. The Role of User Behaviour in Improving Cyber Security Management. Front. Psychol. 12, 561011. https://doi.org/10.3389/fpsyg.2021.561011
69. Mudzingwa, F., 2023. Mobile money in Zambia. url:https://dotzedw.com/state-of-mobile-money-in-zambia-2023/ (accessed 2.1.24).
70. Mulenga, B., 2024. Mobile money transactions hit K452.0 billion in 2023, as data consumption doubles | Zambia Monitor. url:https://www.zambiamonitor.com/mobile-money-transactions-hit-k452-0-billion-in-2023-as-data-consumption-doubles/ (accessed 12.15.24).
71. Muniz, I., n.d. Cyber security challenges in developing countries | MS&E 238 Blog [www document]. url:https://mse238blog.stanford.edu/2017/07/imunizr/cyber-security-challenges-in-developing-countries/ (accessed 3.19.20).
72. Musambo, L.K., Chinyemba, M.K., Phiri, J., 2017. Identifying Botnets Intrusion & Prevention. url:https://doi.org/10.33260/zictjournal.v1i1.28
73. Muthiora, B. (2015). "Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution." GSMA.
74. Mutambo, N.L., Phiri, D., n.d. Analysis of Cybercrime and Cyber Law Effectiveness in Zambian 28.
75. Mvula, F., Phiri, J., Tembo, S., 2020. A Blockchain based Mobile Money Interoperability Scheme. IJACSA 11. https://doi.org/10.14569/IJACSA.2020.0110117
76. Natalie Chipa, Bupe Getrude Mwanza, 2021. Factors Impeding Mobile Money Expansion in Zambia. url:https://doi.org/10.31033/ijemr.11.1.24
77. Ngila, F., 2023. Global mobile money transactions hit a record high in 2022 [www document]. url:https://qz.com/global-mobile-money-transactions-2022-record-trillion-1850351745 (accessed 2.1.24).
78. October 2015, C. 19th, 2015. The basics of Mobile Money Security. Comviva. url:https://www.comviva.com/blog/references/the-basics-of-mobile-money-security/ (accessed 2.1.24).
79. Omidosu, J., Ophoff, J., 2016. A theory-based review of information security behaviour in the organization and home context: 2016 International Conference on Advances in

Computing and Communication Engineering (ICACCE). https://doi.org/10.1109/ICACCE.2016.8073752

80. Payment Method - Mobile Money [www document], n.d. url:https://docs.paymentwall.com/payment-method/mobile-money (accessed 12.9.24).
81. Peterson, R., 2019. Mobile money in Africa: Access, regulations and risks [www document]. DLA Piper Africa. url:https://www.dlapiperafrica.com/en/africa-wide/insights/africa-connected/issue-02/mobile-money-in-africa.html (accessed 6.6.21).
82. Pierluigi, P., 2020. Cybercrime Statistics in 2019 [www document]. Security Affairs. url:https://securityaffairs.co/wordpress/96531/cyber-crime/cybercrime-statistics-in-2019.html (accessed 3.19.20).
83. R. Anthony Inman, n.d. Service Operations - strategy, organization, system, examples, model, hierarchy, business, system [www document]. url:https://www.referenceforbusiness.com/management/Sc-Str/Service-Operations.html (accessed 10.24.20).
84. Raphael, G., 2016. Risks and Barriers Associated with Mobile Money Transactions in Tanzania. BMS. url:https://doi.org/10.5296/bms.v7i2.10069
85. Rodgers, M., n.d. Assessment of Cybersecurity and the Law in Zambia.
86. Rogers, R. W. (1975). "A Protection Motivation Theory of Fear Appeals and Attitude Change." The Journal of Psychology.
87. Rogers, E. M. (2003). Diffusion of Innovations (5th Edition). Simon and Schuster.
88. Role of mobile money is rewriting the fraud landscape in Africa, 2021. url:https://www.subex.com/blog/mobile-money-is-rewriting-the-fraud-landscape-in-africa/ (accessed 11.25.24).
89. Rouse, M., 2020. What is Cybercrime? Effects, Examples and Prevention [www document]. url:https://searchsecurity.techtarget.com/definition/cybercrime (accessed 9.16.20).
90. Sakala, L., Phiri, J., 2019. Factors Affecting Adoption and Use of Mobile Banking Services in Zambia Based on TAM Model. url:https://doi.org/10.4236/ojbm.2019.73095
91. Sambaombe, J.K., Phiri, J., 2022. An Analysis of the Impact of Online Banking on Customer Satisfaction in Commercial Banks Based on the TRA Model (A Case Study of Stanbic Bank Lusaka Main Branch). url:https://doi.org/10.4236/ojbm.2022.101022

92. Scardovi, C., 2017. Digital Transformation in Financial Services. Springer International Publishing, Cham. url:https://doi.org/10.1007/978-3-319-66945-8
93. Scott, W. R. (2008). Institutions and Organizations: Ideas and Interests. Sage Publications.
94. Sekaran, U., and Bougie, R., 2016. Research methods for business: A skill-building approach. 7th ed. Chichester: Wiley.
95. Saunders, M., Lewis, P., and Thornhill, A., 2019. Research methods for business students. 8th ed. Harlow: Pearson Education.
96. Shiloh, J., Amzath, F., n.d. Cybercrime in Africa: Facts and figures [www document]. SciDev.Net Sub-Saharan Africa. url:http://www.scidev.net/index.cfm?originalUrl=/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html& (accessed 3.19.20).
97. Signé, L.S. and K., 2018. Global cybercrimes and weak cybersecurity threaten businesses in Africa. Brookings. url:https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/ (accessed 3.19.20).
98. Silimina, D., n.d. financial inclusion by phone [www document]. Development and Corporation. url:https://www.dandc.eu/en/article/zambians-are-increasingly-using-mobile-phones-move-money-online-platforms (accessed 10.10.22).
99. SIM swap fraud explained and how to help protect yourself [www document], n.d. url:https://us.norton.com/internetsecurity-mobile-sim-swap-fraud.html (accessed 4.1.22).
100. Skaleet, n.d. Mobile Money: definitions and benefits [www document]. Skaleet. url:https://skaleet.com/en/blog/mobile-money-definitions-and-benefits (accessed 12.9.24).
101. Susanto, A., & Aljoza, M. (2015). "Individual Acceptance of Mobile Money Applications: A Case Study in Indonesia Using the Diffusion of Innovation Model." Procedia Computer Science.
102. Suspected Digital Fraud Attempts from Zambia the Highest in Financial Services and Telecommunications [www document], n.d. url: https://newsroom.transunionafrica.com/suspected-digital-fraud-attempts-from-zambia-the-highest-in-financial-services-and-telecommunications/ (accessed 11.25.24).

103. Tasca, P., Aste, T., Pelizzon, L., Perony, N. (Eds.), 2016. Banking Beyond Banks and Money, New Economic Windows. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-42448-4
104. TechTrends, 2024. Navigating Zambia’s Mobile Money and Remittance Surge with FinTech Solutions - [www document]. url:https://www.techtrends.co.zm/navigating-zambias-mobile-money-and-remittance-surge-with-fintech-solutions/ (accessed 12.13.24).
105. The Latest Cyber Crime Statistics (updated October 2024) | AAG IT Support [www document], n.d. url:https://aag-it.com/the-latest-cyber-crime-statistics/ (accessed 12.16.24).
106. The Normalisation of Mobile Money in Sub-Saharan Africa [www document], 2023. Euromonitor. url:https://www.euromonitor.com/article/the-normalisation-of-mobile-money-in-sub-saharan-africa (accessed 12.10.24).
107. The Outlier [www document], n.d. url:https://theoutlier.co.za/business/2024-07-29/88653/mobile-money-sub-saharan-africa-dominates-gsma-report (accessed 11.25.24).
108. The State of the Industry Report on Mobile Money 2024 | Publication | FinDev Gateway [www document], n.d. url:https://www.findevgateway.org/paper/2024/03/state-of-industry-report-on-mobile-money-2024 (accessed 12.10.24).
109. The Vital Role of Agent Networks in Scaling Mobile Money Profits, 2023. Papersoft. url:https://papersoft-dms.com/blog/the-vital-role-of-agent-networks-in-scaling-mobile-money-profitability/ (accessed 12.9.24).
110. Timeline of Cyber Incidents Involving Financial Institutions [www document], n.d. Carnegie Endowment for International Peace. url:https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline (accessed 3.19.20).
111. Trist, E. L. (1981). "The Evolution of Socio-Technical Systems." Tavistock Institute.
112. Tavistock Institute (1981). "The Socio-Technical Systems Approach."
113. Vasudevan, S., 2021. Mobile Money is Rewriting the Fraud Landscape in Africa [www document]. SUBEX. url:https://www.subex.com/blog/mobile-money-is-rewriting-the-fraud-landscape-in-africa/

114. Walliman, N., 2021. Research Methods: The Basics, 3rd ed. Routledge, London. https://doi.org/10.4324/9781003141693
115. Winterfeld, S., Andress, J., 2013. The basics of cyber warfare: understanding the fundamentals of cyber warfare in theory and practice.
116. Writer, S., 2023. Zambia Mobile Money balloon as fintech adoption increase [www document]. ITWeb Africa. url:https://itweb.africa/content/KzQenqjyNnXMZd2r (accessed 2.1.24).
117. Yin, R.K., 2018. Case study research and applications: Design and methods. 6th ed. Thousand Oaks, CA: SAGE Publications.
118. Your guide to sampling techniques and best practices [www document], n.d. Qualtrics. url:https://www.qualtrics.com/experience-management/research/sampling-methods/ (accessed 11.24.24).
119. Zambia Information and Communications Technology Authority [www document], n.d. url:https://www.zicta.zm/ (accessed 12.4.24).
120. Zambia Police Release Annual Crime Statistics for 2023 – Efficacy News, 2024. url:https://efficacynews.africa/2024/02/26/zambia-police-release-annual-crime-statistics-for-2023/ (accessed 12.2.24).
121. Zambia population (2022) live - Countrymeters [www document], n.d. url:https://countrymeters.info/en/Zambia (accessed 6.30.22).
122. Zambia: Time is Money: The mobile money revolution in Zambia, 2018. url:https://www.lusakatimes.com/2018/01/04/time-money-mobile-money-revolution-zambia/ (accessed 11.25.24).
123. Zambia : Zambia Police Service records an increase in Cyber related financial crimes, n.d. url:https://www.lusakatimes.com/2020/04/07/zambia-police-service-records-an-increase-in-cyber-related-financial-crimes/ (accessed 6.5.22).
124. Zambians are increasingly using mobile phones to move money via online platforms [www document],n.d.url:https://www.dandc.eu/en/article/zambians-are-increasingly-using-mobile-phones-move-money-online-platforms (accessed 6.28.22).
125. ZICTA demands subscriber protection against mobile money fraud, 2019. Zambia: News Diggers! url:https://diggers.news/local/2019/05/14/zicta-demands-subscriber-protection-against-mobile-money-fraud/ (accessed 11.4.24).

126.ZICTA warns of rising mobile money fraud amid increased internet penetration, Zambia Monitor, 2024.url:https://www.zambiamonitor.com/zicta-warns-of-rising-mobile-money-fraud-amid-increased-internet-penetration-video/ (accessed 11.25.24).

127.Zimba, A., Mukupa, G., Chama, V., 2022. Emerging Mobile Phone-based Social Engineering Cyberattacks in the Zambian ICT Sector [www document]. arXiv.org. url:https://arxiv.org/abs/2212.13721v1 (accessed 12.26.24).

APPENDICES

Appendix 1: Literature Review Matrix

Author	Study	Findings
Kitime, E (2020)	A framework of cybersecurity risks on mobile money users in Tanzania: A case study of Dodoma city.	The findings of this study show that the mobile money users are at risk due to the use of the internet on their mobile phones.
Ali et al (2020)	Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda.	The study proposed 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.
Interpol (2020)	Mobile Money and Organized Crime in Africa.	The report demonstrated how weaknesses in mobile money security and regulation implementation have offered criminals the opportunity to commit fraud and enable other offences.
Chikoo, I (2020)	Perceived influence of Cybersecurity on the intention to use Mobile Banking Applications.	The research found that cybersecurity awareness was found as a salient significant factor that influences the intention to use mobile banking applications.
Raphael (2016)	Risks and Barriers Associated with Mobile Money Transactions in Tanzania.	The research found that incidents of risk were mainly caused by factors such as mobile money users being exposed to risky environments, illiteracy and lack of awareness.
Ambore et al (2017)	A resilient cybersecurity framework for Mobile Financial Services.	The study found that lack of trust has slowed down the adoption of MFS (Mobile Financial Services) products despite the inherent benefits.

Aron (2018)	Mobile Money and the Economy: A Review of the Evidence.	The study found that mobile money has a direct impact on the economy of developing countries.
Gaber et al (2022)	Security challenges of mobile money transfer services.	The study found security challenges associated with mobile money transfer services.
Gombiro et al (2015)	A conceptual framework for detecting financial crime in mobile money transactions.	The study proposed a framework for detecting financial crime in mobile money transactions.
Giandomenico (2019)	Cybercrime Trends and Financial Services	The study proposed strategies to mitigate cybercrime trends affecting financial services.
Berdibayev and Kwon (2022)	Improving digital financial services inclusion: A panel data analysis	The study proposed ways of improving digital financial services in developing countries as part of the sustainability development goals (SDGs).
Mbunji and Kaira (2024)	An Investigation of the Impact of Mobile Money Services on the Profitability of Commercial Banks in Zambia	The study found that there is a high level of use of MMS in Zambia due to the reliability, accessibility and convenience of the services.
Mkalipa (2022)	The Effect of Mobile Network Operators on Financial Inclusion in Zambia	The researcher was able to come with some recommendations for mobile network operators and key stakeholders of the mobile financial services industry.
Chipa and Mwaanza (2021)	Factors Impeding Mobile Money Expansion in Zambia	The study identified strategies that can be used to accelerate the development of mobile money services in Zambia.
Sakala and Phiri (2019)	Factors Affecting Adoption and Use of Mobile Banking Services in Zambia Based on TAM Model	According to the report, commercial banks and mobile banking service providers should enhance external features, perceived usefulness, and simplicity of use. They should also encourage favourable user attitudes and intentions.

Appendix 2: Questionnaire

The University of Zambia

Graduate School of Business

A FRAMEWORK FOR ADDRESSING SECURITY VULNERABILITIES EXPERIENCED BY REGISTERED MOBILE MONEY CLIENTS IN LUSAKA, ZAMBIA.

Tanje David Sakala, MBA-General

For more information or any queries, kindly get in touch on Cell: 0976766143 or
Email: tstanje64@gmail.com

Dear Respondent,

I am a Postgraduate student at the University of Zambia in my final stage pursuing a Master of Business Administration (MBA General). As partial fulfilment for the award of a Master's degree, I am conducting a baseline study on:

"A Framework for Addressing Security Vulnerabilities Experienced by Registered Mobile Money Clients in Lusaka, Zambia"

You have been purposefully sampled to provide information for the topic indicated above. The information being collected is purely for academic purposes, as such it will be treated with maximum confidentiality. Subsequently, you are not supposed to indicate your name or any personal information that can lead to revealing of your identity. Your co-operation will be greatly appreciated.

For more information or any queries, kindly get in touch with the following:

Project Supervisor: Dr. Jackson Phiri (Jackson.phiri@cs.unza.zm) or

Coordinator: Dr. Bupe M. Mwanza (directorgsb@unza.zm)

SURVEY QUESTIONNAIRE

PART ONE: DEMOGRAPHIC INFORMATION (PLEASE TICK [√])

1. Gender: Male [ ] Female [ ]
2. Marital Status: Single [ ] Married [ ] Divorced [ ] Other [ ]
3. Age: 20 or under [ ] 21-30 [ ] 31-40 [ ] 41-50 [ ] 51-60 [ ] 61+ [ ]
4. Highest level of Education: Secondary School or Below [ ] Diploma [ ] First degree [ ] Masters [ ] Ph.D. [ ]
5. Type of Employment: Not Employed [ ] Employed [ ] Self-Employed [ ] Pensioner [ ]

PART TWO: MOBILE PHONE KNOWLEDGE AND EXPERIENCE (PLEASE TICK [√])

1. How would you describe your general knowledge and use of mobile phones?
   Very poor [ ] Poor [ ] Moderate [ ] Good [ ] Very good [ ]
2. How long have you been using a mobile phone?
   Don't use [ ] Less than 1yr [ ] 1- 2 yrs. [ ] More than 2 yrs. [ ]
3. How often do you use a mobile phone per day?
   Less than 1hr [ ] 1-2 hrs. [ ] 3- 4 hrs. [ ] More than 4 hrs. [ ]

PART THREE: MOBILE MONEY OPERATORS (PLEASE TICK [√])

Using a rating scale from the lowest point of 1 to the highest point of 5, please tick the number that indicates your use of the following Mobile Money Operators (*MMO*)

Never = 1 | Rarely = 2 | Sometimes = 3 | Often = 4 | Always = 5

Mobile Money Operator (MMO)	Never	Rarely	Sometimes	Often	Always
Airtel Zambia	1	2	3	4	5
MTN Zambia	1	2	3	4	5

Zamtel	1	2	3	4	5
Other	1	2	3	4	5

PART FOUR: USE OF MOBILE MONEY SERVICES (PLEASE TICK [√])

1. How long have you been using Mobile Money Services? Under 1 year [ ] 1-2 years [ ] 3- 4 years [ ] more than 4 years [ ]

2. On a weekly basis, how many times do you use Mobile Money Services? Not at all [ ] Once a week [ ] 2- 3 times [ ] More than 3 times [ ]

PART FIVE: MOBILE MONEY SECURITY VULNERABILITIES

Using a rating scale from the lowest point of 1 to the highest point of 5, please circle the number that indicates your level of agreement or disagreement with the following statements.

SD = Strongly Disagree | D = Disagree | N = Neutral | A = Agree | SA = Strongly Agree

MOBILE MONEY SECURITY VULNERABILITIES						
Unauthorized SIM Swap		SD	D	N	A	SA
1	How much do you agree or disagree that you are aware of the threats that an unauthorized SIM swap poses on the security of mobile money transactions?	1	2	3	4	5
2	How much do you agree or disagree that your SIM card has ever been replaced without your knowledge?	1	2	3	4	5
3	How much do you agree or disagree that you immediately block your cell phone number after an unauthorized SIM swap?	1	2	3	4	5
4	How much do you agree or disagree that when you encounter an unauthorized SIM swap, you immediately notify the police and/or the mobile money operators(s)?	1	2	3	4	5
SMishing (Suspicious text messages soliciting funds or mobile money account credentials)		SD	D	N	A	SA
1	How much do you agree or disagree that you are aware of the threats that SMishing poses on the security of mobile money transactions?	1	2	3	4	5
2	How likely is it that you've ever received a suspicious text message asking you to start a transaction from an unknown number?	1	2	3	4	5
3	How likely is it that you have ever received a suspicious text message from an unknown number asking for your mobile money account details?	1	2	3	4	5
4	How much do you agree or disagree that you immediately block an unknown mobile number that asks you to start a transaction or for the details of your mobile money account?	1	2	3	4	5
5	How much do you agree or disagree that when you encounter SMishing, you immediately notify the police and/or the mobile money operators(s)?	1	2	3	4	5
Vishing (Suspicious phone calls soliciting funds or mobile money account credentials)		SD	D	N	A	SA
1	How much do you agree or disagree that you are aware of the threats that Vishing poses on the security of mobile money transactions?	1	2	3	4	5
2	How likely is it that you have ever received a questionable phone call asking for money or your mobile money account information?	1	2	3	4	5
3	How much do you agree or disagree that you immediately block an unknown cell phone number that asks you to start a transaction or for account details for your mobile money?	1	2	3	4	5
4	How much do you agree or disagree that when you encounter Vishing, you immediately notify the police and/or the mobile money operators(s)?	1	2	3	4	5
Stolen/Lost Mobile Phone		SD	D	N	A	SA
1	How much do you agree or disagree that you are aware of the threats that a lost/stolen phone poses on the security of mobile money transactions?	1	2	3	4	5
2	How much do you agree or disagree that when your mobile phone gets lost/stolen, you immediately notify the police?	1	2	3	4	5
3	How much do you agree or disagree that you immediately replace your mobile phone and renew your mobile number without contacting the police?	1	2	3	4	5
PIN Sharing		SD	D	N	A	SA
1	How much do you agree or disagree that you are aware of the threats that PIN sharing poses on the security of mobile money transactions?	1	2	3	4	5
2	How much do you agree or disagree that you have ever shared your mobile money PIN with close friends, family members, or another person who is well-known?	1	2	3	4	5
3	How much do you agree or disagree with the statement that you have ever given your mobile money PIN to an unauthorized person?	1	2	3	4	5
Agent Driven Fraud (Fraud resulting from trusting Mobile Money Agents to conduct transactions on your behalf)		SD	D	N	A	SA

1	How much do you agree or disagree that you are aware of the threats that Agent Driven Fraud poses on the security of mobile money transactions?	1	2	3	4	5
2	How much do you agree or disagree that you have ever shared your mobile money login details with a mobile money agent?	1	2	3	4	5
3	How much do you agree or disagree that you have ever trusted a mobile money agent to manage your mobile money transaction?	1	2	3	4	5

PART SIX: MOBILE MONEY TRANSACTIONS

Using a rating scale from the lowest point of 1 to the highest point of 5, please circle the number that indicates your level of agreement or disagreement with the following statements.

Never = 1 | Rarely = 2 | Sometimes = 3 | Often = 4 | Always = 5

MOBILE MONEY TRANSCTIONs (MMT)						
Mobile Money Transactions (MMT): Facing Security Vulnerabilities						
1	Have you ever experienced any of the previously listed security vulnerabilities and were able to conduct a successful mobile money transaction?	1	2	3	4	5
2	Have you ever experienced any of the previously listed security vulnerabilities that resulted in an unreliable mobile money transaction?	1	2	3	4	5
3	Have you ever experienced any of the previously listed security vulnerabilities that resulted in a failed mobile money transaction?	1	2	3	4	5
Mobile Money Transactions (MMT): Frequency of Facing Security Risks & Vulnerabilities						
1	How often have you experienced any of the previously listed security vulnerabilities and were able to conduct a successful mobile money transaction?	1	2	3	4	5
2	How often have you experienced any of the previously listed security vulnerabilities that resulted in an unreliable mobile money transaction?	1	2	3	4	5
3	How often have you experienced any of the previously listed security vulnerabilities that resulted in a failed mobile money transaction?	1	2	3	4	5

PART SEVEN: MOBILE MONEY AWARENESS AND TRAINING

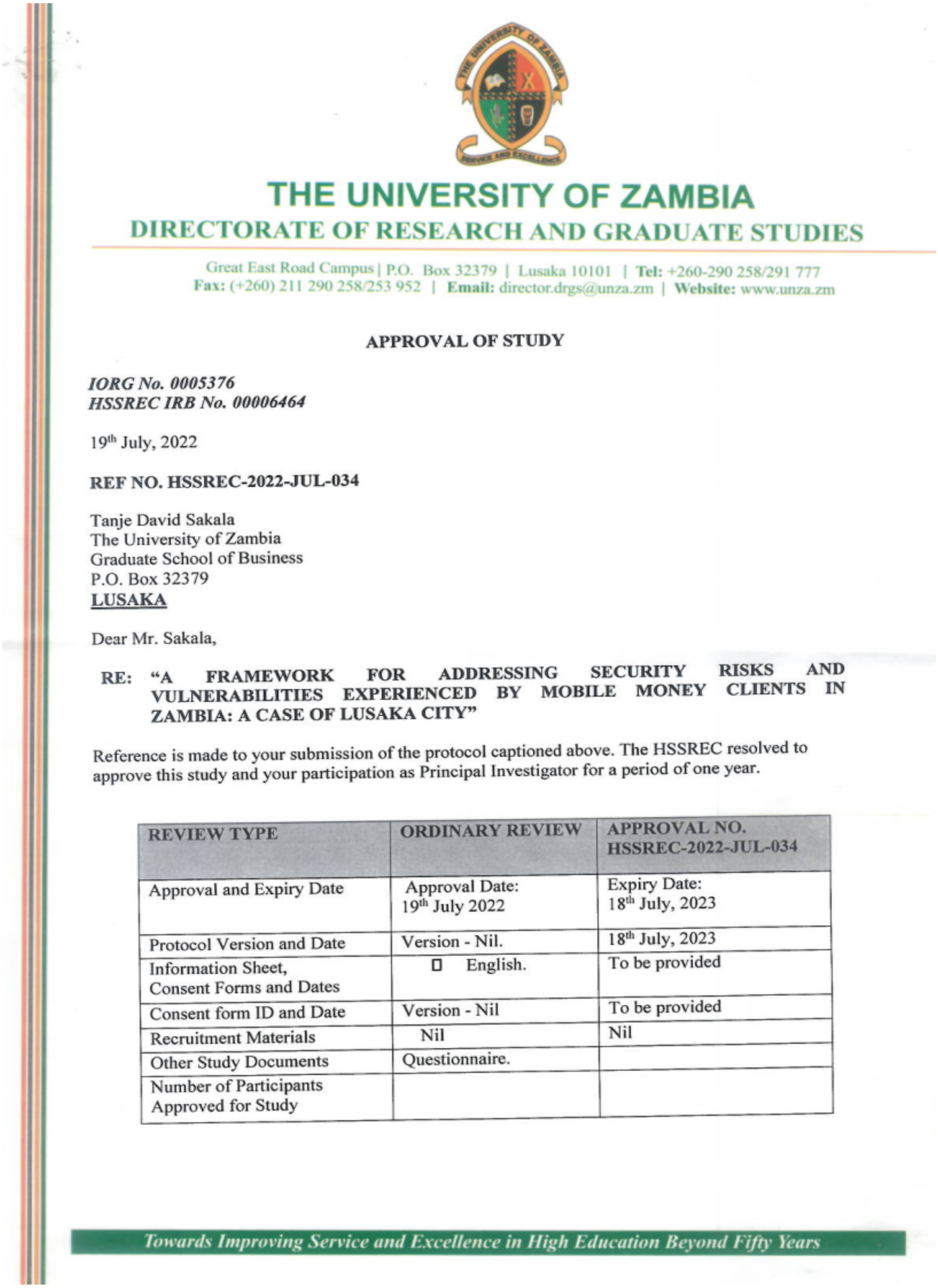
Using a rating scale from the lowest point of 1 to the highest point of 5, please circle the number that indicates your level of agreement or disagreement with the following statements.

SD = Strongly Disagree | D = Disagree | N = Neutral | A = Agree | SA = Strongly Agree

Mobile Money Awareness & Training		SD	D	N	A	SA
1	Do mobile money operators provide adequate awareness on the security vulnerabilities associated with mobile money transactions through TV, radio, magazine, flyers and brochures, or other media?	1	2	3	4	5
2	Do mobile money operators provide adequate training on the security vulnerabilities associated with mobile money transactions through TV, radio, magazine, flyers, brochures, or other media?	1	2	3	4	5
3	Would you require further training on the security vulnerabilities associated with mobile money transactions?	1	2	3	4	5
4	Would you be more aware on the security vulnerabilities associated with mobile money transactions if you received more training?	1	2	3	4	5
5	Are you happy with the current levels of security, training and awareness offered by Mobile Money Operators (MMO)	1	2	3	4	5

Thank you for your participation!!

Appendix 3: Approval Letter



THE UNIVERSITY OF ZAMBIA
DIRECTORATE OF RESEARCH AND GRADUATE STUDIES
Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | **Tel:** +260-290 258/291 777
Fax: (+260) 211 290 258/253 952 | **Email:** director.drgs@unza.zm | **Website:** www.unza.zm

APPROVAL OF STUDY

IORG No. 0005376
HSSREC IRB No. 00006464

19th July, 2022

REF NO. HSSREC-2022-JUL-034

Tanje David Sakala
The University of Zambia
Graduate School of Business
P.O. Box 32379
LUSAKA

Dear Mr. Sakala,

RE: "A FRAMEWORK FOR ADDRESSING SECURITY RISKS AND VULNERABILITIES EXPERIENCED BY MOBILE MONEY CLIENTS IN ZAMBIA: A CASE OF LUSAKA CITY"

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.

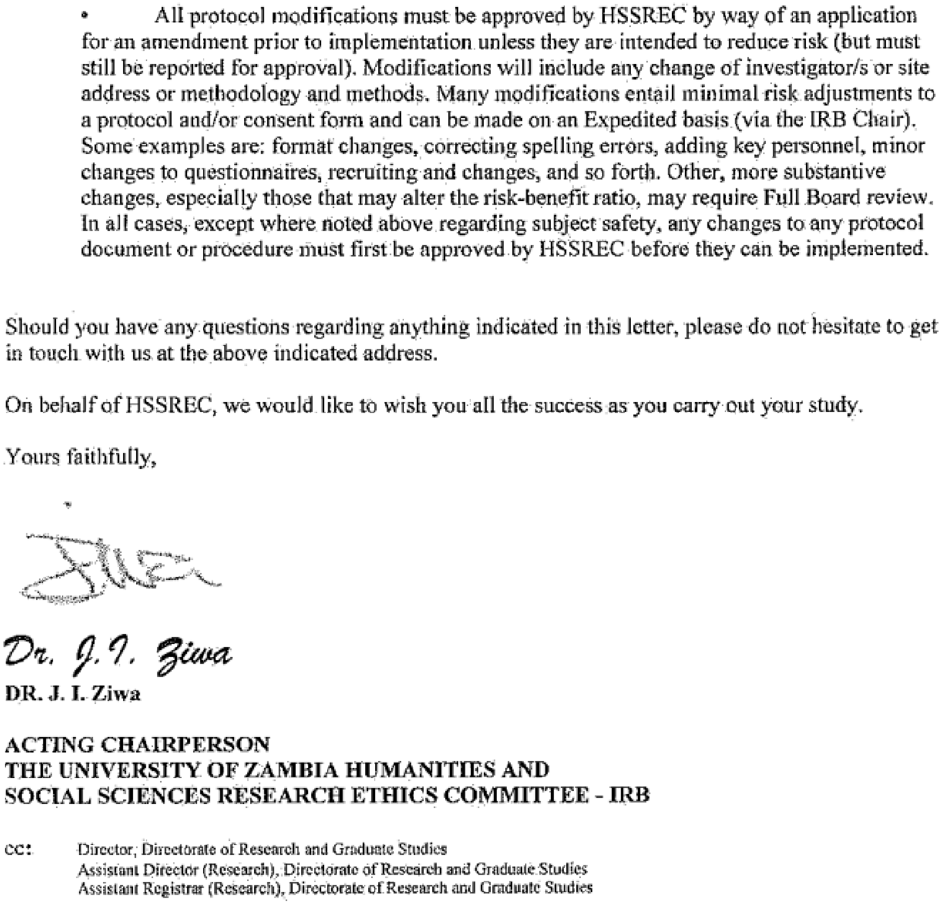
REVIEW TYPE	ORDINARY REVIEW	APPROVAL NO. HSSREC-2022-JUL-034
Approval and Expiry Date	Approval Date: 19th July 2022	Expiry Date: 18th July, 2023
Protocol Version and Date	Version - Nil.	18th July, 2023
Information Sheet, Consent Forms and Dates	☐ English.	To be provided
Consent form ID and Date	Version - Nil	To be provided
Recruitment Materials	Nil	Nil
Other Study Documents	Questionnaire.	
Number of Participants Approved for Study		

Towards Improving Service and Excellence in High Education Beyond Fifty Years

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,

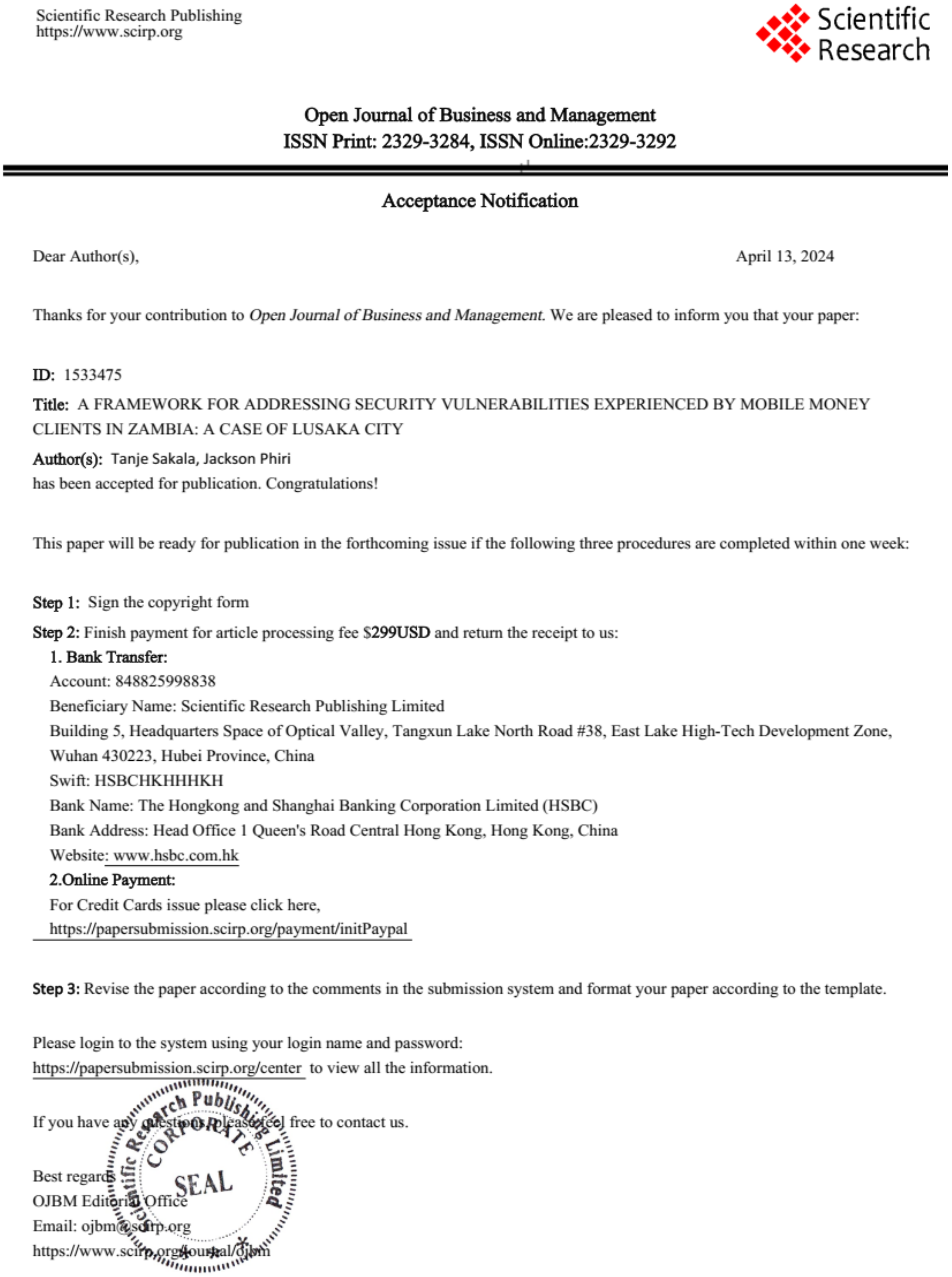
Dr. J. I. Ziwa

DR. J. I. Ziwa

ACTING 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

Appendix 4: Publication



Scientific Research Publishing
https://www.scirp.org

Scientific Research

Open Journal of Business and Management
ISSN Print: 2329-3284, ISSN Online:2329-3292

Acceptance Notification

Dear Author(s),

April 13, 2024

Thanks for your contribution to *Open Journal of Business and Management*. We are pleased to inform you that your paper:

ID: 1533475

Title: A FRAMEWORK FOR ADDRESSING SECURITY VULNERABILITIES EXPERIENCED BY MOBILE MONEY CLIENTS IN ZAMBIA: A CASE OF LUSAKA CITY

Author(s): Tanje Sakala, Jackson Phiri
has been accepted for publication. Congratulations!

This paper will be ready for publication in the forthcoming issue if the following three procedures are completed within one week:

Step 1: Sign the copyright form

Step 2: Finish payment for article processing fee $**299USD** and return the receipt to us:

1. Bank Transfer:
Account: 848825998838
Beneficiary Name: Scientific Research Publishing Limited
Building 5, Headquarters Space of Optical Valley, Tangxun Lake North Road #38, East Lake High-Tech Development Zone, Wuhan 430223, Hubei Province, China
Swift: HSBCHKHHHKH
Bank Name: The Hongkong and Shanghai Banking Corporation Limited (HSBC)
Bank Address: Head Office 1 Queen's Road Central Hong Kong, Hong Kong, China
Website: www.hsbc.com.hk

2.Online Payment:
For Credit Cards issue please click here,
https://papersubmission.scirp.org/payment/initPaypal

Step 3: Revise the paper according to the comments in the submission system and format your paper according to the template.

Please login to the system using your login name and password:
https://papersubmission.scirp.org/center to view all the information.

If you have any questions, please feel free to contact us.

Best regards
OJBM Editorial Office
Email: ojbm@scirp.org
https://www.scirp.org/journal/ojbm