UNIVERSITY OF LUSAKA

SCHOOL OF POSTGRADUATE STUDIES

INVESTIGATING THE EXTENT TO WHICH MOBILE MONEY FRAUD CONTRIBUTES TO THE PERFORMANCE OF SMALL MEDIUM ENTERPRISES IN LUSAKA, ZAMBIA.

BY

ESNART MBEWE

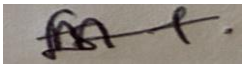
MBAFIN22113367

A dissertation submitted to the School of Post Graduate Studies, University of Lusaka in Partial fulfilment for the award of the Master of Business Administration in Finance.

DECLARATION

I **Esnart Mbewe**, student number **MBAFIN22113367** do hereby declare that the contents of this dissertation is my original work and has not been plagiarized in any way or submitted by someone else at any other University. Any works by other authors have been referenced accordingly.

DATE: January 20, 2025

NAME: ESNART MBEWE CANDIDATE'S SIGNATURE: 

DATE: January 20, 2025

SUPERVISOR'S NAME: MWATA CHISHA, Ph. D

SIGNATURE: 

DEDICATION

This work is dedicated to my parents, Charles Tambeta Mbewe and Beatrice Lindiwe Mbewe who have shown me nothing but love and support, your wisdom and encouragement are priceless.

ACKNOWLEDGEMENTS

I owe my gratitude to God, for the grace he showed me to overcome all the challenges I faced to finish my dissertation. I would also like to express gratitude to my supervisor, Dr. Mwata Chisha, for the guidance, insight and encouragement. And to my family and friends, thank you for your belief in me. I do not take it for granted.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This study investigated the extent to which mobile money fraud contributes to the performance of SMEs in Lusaka, Zambia. The main objectives of the study were to; assess the prevalence of mobile money fraud among SMEs in Lusaka; investigate the type of mobile money fraud SMEs encounter while using mobile money services for their business operations, analyse how mobile money fraud contributes to SME performance in Lusaka and evaluate the effectiveness of existing fraud prevention measures used by SMEs in Lusaka. A mixed methods approach was adopted for this study and it targeted SMEs from 10 different markets in Lusaka with less than 10 employees, a gross monthly revenue below twenty-five thousand Kwacha and less than 5 years in operation. The main data collection tools for quantitative data were collected using questionnaires and the qualitative data extracted from the open-ended questions in the questionnaires. Descriptive and inferential statistics was adopted to analyze the quantitative data and thematic analysis for the collected qualitative data. In addition, the survey questionnaires were purposely distributed among 191 SMEs.

The major research findings revealed a notable prevalence of mobile money fraud with 60% of SMEs in Lusaka experiencing mobile money fraud. Among the SME employees and owners, 40% reported false transactions as most prevalent mobile money fraud type. These findings suggest a weakness in mobile money systems. SME fraud frequency ranged from 35% being affected by fraud at least once to 25% being affected at least once a month, noting real threats and a call for more preventive strategies. The study further quantified financial losses as the most severe effect of mobile money fraud with 50% respondents experiencing a hindrance in business expansion. Other effects were an increase in operation costs at 30% and decreased customer trust at 20%. Measures suggested were transaction monitoring (60%) and fraud risk education for employees (40%). Regulatory recommendations included setting new measures to implement severe punishment for fraudsters, establishment of central agencies for reporting fraud cases and compulsory checking of mobile money providers because the current fraud prevention and management strategies did not align with the SMEs experiences.

Therefore, the findings of the study underscored that mobile money fraud is a significant issue among SMEs in Lusaka, Zambia, with varying levels of intensity across different SMEs depending on the types of mobile money fraud experienced or

frequency of mobile money fraud. It was found that mobile money fraud had a substantial impact on the performance of businesses and highlights the need for tailored fraud prevention strategies. These strategies should include transaction monitoring and fraud risk training of employees and SME owners. By implementing these recommended strategies, SMEs in Zambia can potentially improve their business performance and profitability which could contribute positively to business success and economic growth. These findings align with the study's general and specific objectives of examining the prevalence, types, impact and management of mobile money fraud in businesses.

Keywords: *Mobile Money Services, Small and Medium Enterprises, SME performance, Fraud, Vishing/ Smishing, Advance fee scams, Reversal requests, False transactions.*

CHAPTER ONE: INTRODUCTION

1.0 Introduction

Mobile money services have become a revolutionary instrument in the financial system of diverse developing and underdeveloped countries, where they have a significant impact on the economy offering ease, convenience and efficiency (Donovan, 2012). However, as mobile money service use grows, so does the risk of mobile money fraud, which threatens the financial stability and overall performance of SMEs. Mobile money fraud ranges from vishing/ smishing, false transactions, advance fee scams to reversal requests causing significant challenges, that lead to either financial losses, operational disruptions and reduced trust in digital payment systems for businesses (Gilman & Joyce, 2012).

Understanding the extent to which mobile money fraud impacts SME performance is vital for developing strategies to mitigate risks and enhance the security of digital financial transactions. Secondly, given that SMEs are essential in driving economic growth, employment, and innovation in Zambia, addressing this problem will improve business sustainability and economic development. Thus, this study aims to investigate the prevalence of mobile money fraud and assess the consequences mobile money fraud has on business performance. The findings will contribute to policymaking, financial security measures for SMEs, and raise awareness to protect SMEs from the setbacks related to mobile money.

1.1 Background

A major technological advancement that has impacted the lives of people is that of mobile money services. Mobile money services have encouraged financial inclusion for people not associated with conventional banking systems due to the ease, accessibility and convenience it offers (Mbiti & Weil, 2011). The term Mobile money means financial solutions accessed through a mobile device. It may encompass several varying payments such as (person-to-person, government to people, business to business), financial products (insurance, credits, saving products) and banking features (such as checking account status) (Donovan, 2012). The rise of mobile money services in Zambia can be traced back to the 2000s, with the introduction of digital financial platforms by major telecommunication companies; MTN Mobile

Money, Airtel Money, and Zoona (Ngambi, 2016). The total number of active mobile cellular subscriptions is at 20.1 million subscriptions at the end of June 2023. Airtel Zambia has 6.3 million subscriptions, followed by MTN Zambia and Zamtel at 4.7 million and 1.9 million subscriptions respectively (ZICTA, 2023). Initially designed to promote financial inclusion, mobile money quickly became a widely used tool for transactions, among individuals and SMEs that lacked access to traditional banking services. Today, mobile money permits businesses to conduct transactions on their mobile devices supporting entrepreneurial activity, guaranteeing sustainability, and encouraging growth (Talom & Tengeh, 2019).

However, as the use of mobile money grew, so did the challenges associated with the security of the platform causing mobile money fraud (Hashim, Ariff and Salleh, 2022). Mobile money fraud is an issue affecting the telecommunication industry, and massive amounts of revenue get lost to fraudsters who have devised various ways to defraud (Daka & Nyirenda, 2022). Arhin (2018), reveals that more than 48% companies globally have succumb to fraud bringing the global cost of fraud to $1.5 trillion per year. While in Africa, Ghana recorded losses amounting to GH₵ 27 million in 2022 and 13 million USD was lost in Uganda in 2021(Bank of Ghana, 2022; Ugandan Communications Commission, 2021).

Incidents of mobile money fraud recorded cases of SIM card swapping, fake transactions, advance fee scams, reversal requests and vishing and phishing scams, directed to both individuals and businesses (Gilman & Joyce, 2012). Vishing/Smishing is where the fraudster uses phone calls or SMS to obtain personal details such as Personal Identification Number (PINs) or account numbers, Advance fee scams is where customers are tricked into sending money under false promises or circumstances, Reversal requests encompass requests to reverse transactions that actually went through and False transactions is where mobile money users receive fake SMS alerts to send money to customers for unsuccessful transactions or mobile money agents transferring customer funds to personal accounts (Provencal, 2017; Akomea-Frimpong, Andoh & Akomea-Frimpong, 2020; Gilman & Joyce, 2012).

Reports from Zambia Information and Communications Technology Authority (ZICTA) and Bank of Zambia (BOZ) indicated a growing trend in fraud-related losses, which prompted concerns among SMEs and financial institutions (ZICTA, 2023; BOZ, 2023). Despite raising these concerns, fraudsters have still continued to develop more

sophisticated tactics, which lead to increased financial losses for businesses. Mobile money fraud has remained a persistent threat, affecting the financial stability of SMEs in Lusaka (Mubita, 2023). While BOZ and ZICTA have continued to make efforts to strengthen cybersecurity frameworks, the effectiveness of these measures remains uncertain as SMEs still face challenges in preventing fraud, raising concerns about the overall impact on business performance and profitability.

The impact of mobile money fraud on the performance of SMEs in Lusaka remains an important and underexplored area of study. Fraud-related financial losses can affect business performance, which can lead to financial losses, lower profits, lower employee retention and business closure (Busuulwa, 2016; Salim, 2022; Akomeaa-Frimpong, 2017). The major objective of this study is to investigate the extent to which mobile money fraud contributes to the performance of SMEs in Lusaka, Zambia. Therefore, given the crucial role SMEs play in Zambia's economic development, the justification for doing a research on the Zambian setting is to lessen the digital literacy gap present. The study will also bridge the current literature gap and build on existing literature on mobile money fraud to generate and contextualize literature that will be utilised and applicable locally and to guard SMEs in Zambia from becoming future victims of mobile money fraud. The study will also increase awareness on the emerging threat of mobile money fraud and safeguard the Zambian economy from deteriorating.

1.2 Statement of the Problem

In any business, mobile money plays a significant role. The problem is the presence of mobile money fraud causes business disruptions and loss of morale and trust in the mobile service platforms (Zainal, Hashim, Arff & Salleh, 2022; Akomeaa-Frimpong, 2017). According to recent research, if left unresolved, some SMEs reduce their moble money use while others stop using mobile money for business operations due to reasons that can be linked to mobile money fraud. Additionally, businesses who experience mobile money fraud may experience a decline in business performance, which can lead to financial losses, lower profits, lower employee retention and business closure (Busuulwa, 2016; Salim, 2022; Akomeaa-Frimpong, 2017).

Mobile money fraud has realised as a growing distress in Ghana, Tanzania and Uganda and is not uncommon in Zambia. For instance, mobile money fraud cases stood at 53 percent in Uganda, 42 percent in Tanzania and 23 percent in Ghana (Busuulwa, 2016; Salim, 2022; Akomeaa-Frimpong, 2017). Some of the factors that contribute to mobile money fraud are paying mobile money agents or employees poor salaries or inadequate awareness and training among employees (Busuulwa, 2016; Salim, 2022; Akomeaa-Frimpong, 2017). Ghana recorded losses amounting to GH₵ 27 million in 2022 compared to GH₵ 14.2 million in 2021 and Uganda 61 billon Ugandan shillings equating to about 13 million United States dollars was lost in 2021(Bank of Ghana, 2022; Ugandan Communications Commission, 2021).

The gap in the body of knowledge is the exact magnitude Zambian SMEs have had mobile money fraud affect their business performance. This study will fill in this gap and extend to a new population. Zainal, Hashim, Arff and Salleh (2022) recommend further studies to explore and broaden literature on SME fraud focusing on the impact and type of control mechanisms suitable for SMEs. Conducting a study in Zambia will help bridge the existing gap in Knowledge and literature. This research is designed to investigate the effect of mobile money fraud on SME operations and sustainability by uncovering the prevalence of mobile money fraud, explaining what makes SMEs vulnerable to fraud, understanding the operational setbacks and devising fraud prevention strategies and security measures applicable to the Zambian population.

1.4. Research Objectives

1.4.1 General Objective

The general objective of the research is to investigate the extent to which mobile money fraud contributes to SMEs performance in Lusaka.

1.4.2 Specific Objectives

The specific research objectives will help us provide a road map with precise details about what the research will investigate and will carry out.

The primary objectives of the study are:

1. Assess the prevalence of mobile money fraud among SMEs in Lusaka.
2. Investigate the type of mobile money fraud SMEs encounter while using mobile money services for their business operations.

3. Analyse how mobile money fraud contributes to SME performance in Lusaka.
4. Evaluate the effectiveness of existing fraud prevention measures used by SMEs in Lusaka.

1.4.3 Research Questions

To accomplish the objectives outlined above, the following research questions will guide this study:

1. What is the prevalence of mobile money fraud among SMEs in Lusaka?
2. What are the types of mobile money fraud SMEs encounter while using mobile money services?
3. How has mobile money fraud contributed to SME performance in Lusaka?
4. How effective are the current fraud prevention measures implemented by SMEs?

1.5 Scope

The scope of the study helps make a research manageable, relevant and easier to produce useful results. This scope of the study will be limited to SMEs in Lusaka operating 10 local markets (North mead, Long acres, Chilenje Chris Corner, Chilenje, Kabwata, Libala, Kamwala, Kalundu, Matero and Chaisa) and are in service provision. In Zambia, SMEs refer to those with a total investment amount less than K10,000, an annual turnover less than K80,000 and has less than 30 employees (Kawimbe, 2024). Thus, the study's eligibility criteria are SMEs with less than 30 employees, a gross revenue not greater than K25,000 per month and have not been operating for not more than five years. Since Zambian SMEs are usually categorised as either; trading, manufacturing and service. The service sector is adopted for this study. This will include businesses focused on either goods and passenger transport, restaurants, hair salons and barbershops or cleaning services (Kambone, 2017).

1.6 Significance of the Study

The popularity mobile money fraud has gained worldwide in recent years has become of great economic concern globally leading to financial losses and leaps in businesses. To help mitigate the rising number of mobile money fraud cases, employee education and awareness in security measures has been considered. The results of this study

will be a meaningful step towards finding solutions to the effects of mobile money fraud. The study will help develop robust risk management strategies and risk management will assist with the success of any business by protecting both the reputation of MNOs and loss of revenue by SMEs. The findings from this study will have significant implications for the growth of SMEs, help SMEs make informed decisions when using mobile money platforms and help both the mobile money operators and regulators to support users of mobile money platforms by creating regulatory frameworks and consumer protection measures that defend them. This will be achieved by the general objective of the study which aims to investigate the extent to which mobile money fraud contributes to SMEs performance in Lusaka, Zambia and understanding how financial loss and sustainability would prompt SMEs to devise effective fraud avoidance and mitigation strategies and lastly to contribute to the body of knowledge for researchers.

1.7 Operational Definitions

Mobile Money Services: Refer to a mobile financial platform that allows an individual with a mobile device to send or receive money, and perform other monetary procedures (Asongu & Asongu, 2018; Donovan, 2012).

Small and Medium Enterprises (SMEs): SMEs usually described based on clearing defining the amount of capital invested, annual sales turnover and the number of employees (Garikai, 2011; Iravonga & Miroga, 2018).

SME Performance: Evaluating how a business evaluates their profits or loss margins, growth or market competition (Tarute & Gatautis, 2014; Cicea, Popa, Marinescu & Catalina Stefan, 2019).

Fraud: Fraud generally refers to wrongful or criminal deception intended to result in financial or personal gain (Arhin, 2018; Subex, 2017).

Vishing/ Smishing: refers to the use of either phone calls or SMS to collect personal details or PIN (Gilman & Joyce, 2012; Mussa-Salim, 2022)

Advance fee scams: is when customers are duped into sending money under fake promises or circumstances (Gilaman & Joyce, 2012; Akomea-Frimpong, Andoh & Akomea-Frimpong, 2020).

Reversal requests: involve a customer requesting an individual to reverse a transaction that was actually successful (Gilman & Joyce, 2012; Akomea-Frimpong, Andoh & Akomea-Frimpong, 2020).

False transactions: represents receiving fake SMS alerts to make customers to believe a transaction was successful (Gilman & Joyce 2012; Provencal, 2017).

1.8 Organisation of the Report

Chapter one provides an introduction of the study and the various sub sections, including the statement of the problem and study objectives. The rationale for the first chapter is to share the information regarding the motivation and relevance of the research. Chapter two focuses on the review of literature on mobile money fraud, which will be followed by the review of relevant theories and after a conceptual framework is outlined. Chapter three describes the research design, the methods used for data collection and the analysis procures used. Chapter four is a presentation of the analysis of data collected and the findings on the role played by mobile money fraud in SMEs performance. The findings of this study are discussed in chapter five along with their implications on SMEs, mobile money providers, and policy formulation. To conclude, in chapter six, the research is concluded, the importance of the study restated and the possibilities for further investigations proposed.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

Mobile money services have changed the conventional structures of financial transactions, especially for Small and Medium Enterprises. The objective of this extensive literature analysis is to examine the diverse effects of mobile money fraud on the SMEs performance in Zambia. The analysis is organized into three key perspectives: the global background, the African narrative, and the local Zambian terrain. Each perspective offers distinct insights into the adoption, impact and issues encountered by SMEs within the framework of mobile money services because of mobile money fraud.

2.1 Empirical Literature Review

2.1.1 Global Perspective on mobile money fraud

There are several perspectives of mobile money fraud and a deep dive into relevant research across diverse geographical settings is crucial to help fully grasp the influence of mobile money fraud. This starts with the global perspective. Zainal, Hashim, Ariff and Salleh (2022) present a review of literature on fraud with a specific focus on SMEs in Malaysia, providing further knowledge on recent developments in fraud research and offering suggestions for future research. Common factors of fraud in majority of SMEs is low morale among employees and weak internal control within organizations. Despite the limit on the research on fraud involving SMEs, SMEs are important and this paper recommends that the criminal justice system should identify more accurately the cost of fraud in SMEs. Greater understanding of fraud in the SMEs allows in identifying the best approach to prevent and detect fraud for SMEs with limited resources. This study is relevant for this study as it shows us the existence of mobile money fraud in Malaysia and identifies the reasons why fraud occurs. We could learn from Malaysia however would same results will be produced in Zambia.

De Arroyabe and de Arroyabe (2021) Investigate cyber breaches and the effect cyber breaches have on SMEs. Cyber breach refers to a violation of the security policy of a system to affect its integrity or availability, leading to unauthorised access or attempted access to a system (Enisa, 2018). This is similar to mobile money fraud. SMEs receive a wide variety of breaches, the degree of severity of breaches in SMEs, based on

disruption time and cost help to understand the economic, financial and management impacts. The results reveal that the attacks received by SMEs were not very severe, combining both recovery time and cost compared to previous that suggested that that 60% of SMEs will disappear after six months. These results reinforce the need to establish appropriate cybersecurity policies, procedures, awareness and training in SMEs, as well as insurance cover for business recovery, and to update security controls. From the results, we note that as use and dependence of online services increases, SME managers increase their interest and concern about cybersecurity, introducing new measures prevent further attacks, loss of time to deal with attack, compensating customers and no work for employees. In conclusion the existence of breaches produces a reaction in SMEs in terms of management to protect themselves against future attacks and cyber breaches related to malware attacks have a greater impact on the economic losses of a company, both in terms of additional staff costs and service interruptions. This research study is relevant to this study as it explains the impact of cyber breaches which are related to mobile money fraud have on SMEs highlighting financial disruptions, losses of a company to training and awareness and service interruption costs.

Wilson, McDonald and McGarry (2022) conducted an online survey in the United Kingdom of 85 SMEs on the threats, coping mechanisms and the five common types of cyber-attacks that the SMEs experienced. The five included, network being hacked, data being stolen, malware infection, compromised mobile phones and phishing email attacks. From the results however, the possibility of an attack was low, particularly that of the possibility of SMEs business network having data stolen or being hacked. Due to the low risks perceived, the impact would be high and difficult to cope with, and measures to prevent such attacks expensive. The conclusion was that self-efficacy was significantly lower for keeping mobile devices safe and avoiding phishing attacks suggesting recommendations for SME engagement. This study is relevant to our study as it shows and proves that different types of cyber- attacks exist and mobile money fraud is a type of cyber-attacks. The effect cyber-attacks have on SMEs varies and in this study, are not only difficult to cope with but also costly to engage security measures.

2.1.2 African Perspective on mobile money fraud

Examining research conducted in Africa can help Zambia gain valuable insights on the potential effect of mobile money fraud on SME performance and assist with informed strategies to support SME development in Zambia. The African studies also provide a smooth transition for examining mobile money fraud and SMEs in Zambia. Raphael (2016) studies to spot and reveal the risks and barriers associated with mobile money transactions in Tanzania. His analysis includes; how often incidences of risk occur, the understanding levels among users and ways to avoid risks and barriers that expose the business environment. Descriptive analysis was utilized and a quantitative interpretation. The findings reveal moderate risk as compared to barriers. Majority of risks experienced include; loss of passwords, fake transaction requests, and fake money. On the other hand, common barriers were; poor network, lack of liquidity by agents, and lack of identity cards. Research noted and suggests that regulatory authorities should make security of mobile money services for users a priority and encourage creating awareness and encouraging proper rules and regulations encouraging participation of mobile money users and improvement of mobile companies. This study is important in this on-going study to help us see the risks of mobile money in Tanzania and identifies the common types of money fraud as fake transactions and fake money.

Wamuyu (2014) conducted a survey in Kenya about mobile money usage. The study utilised survey questionnaire and two focus groups to collect data. The results suggest that previous methods of money transfers did a great job in influencing uptake of mobile money in Kenya but fraud and making a transaction to the wrong number were the major risking factors of mobile money services. In a similar study similar study by (Senso & Venkatakrishnan, 2013) in Tanzania, the qualitative study looked at the dark side of mobile money focusing on challenges of mobile money transfer services. Nearly the same results were achieved as in Kenya. Observed was that fraud, a SIM card swap, fake money, fake text message requests to transfer money, PIN leakage and unfaithful workers are among most common risks associated with the money system in Tanzania by both mobile money agents and users. The study is relevant as it shows the type of mobile money fraud that is common.

Peterson (2019) in his research reported countries where mobile money payments gained momentum as hubs for corrupt practices. Because of the weak law

enforcements that exist against financial crimes, risk assessments and policies to avert fraud within organisations responsible for developing mobile money systems are essential dealing with their transactions. In their study on the dimensions of electronic fraud and governance of trust in Nigeria's economic system (Tade & Adeniyi, 2020) used qualitative methods to collect data and purposely selected 30 participants. The aforementioned found that fraud was being committed exclusively by the bank's staff members who exploited the strategic position they held. This aligned with an earlier news report from Uganda where the anti-corruption court convicted six MTN staff for illegally accessing the company's mobile money system and fraudulently transferring funds to various agents and later sharing the money (Waseka, 2015). This suggests that fraudulent activities are not limited to banks but can also be found among telecommunications and agents. This research is relevant to our study as it shows the existence of mobile money fraud and types specifically from the angle of the agents or telecoms.

Gilman and Joyce (2014) conducted a study to manage the risk of fraud in mobile money outlining the framework to follow when managing risk and fraud and the four key elements of the framework are; determine risk appetite, identify and assess risks, establish effective control and monitor and review the risk management strategy. The findings reveal that mobile money operators are aware of the need to develop a robust risk management strategy for mobile money. The risk identifies that three categories of people that need to be considered are: the customers who face transactional risk; the agent facing channel risk and the employee facing internal risk. The identified potential mobile transactional frauds are; vishing/smishing, advance fee scams, payroll fraud, false transactions, reversal requests, split transactions, registration fraud, internal fraud and identity theft (Gilman & Joyce, 2014).

Arhin (2018) Researches on the impact fraud has on the financial performance of mobile payment companies in Ghana. And also analyses the nature of fraud in payment systems, the direct impact that fraud has especially on fraud victims and management implication behind the financial fraud theories which are being used by mobile payment companies. Secondary data from published financial statements was utilised and both quantitative and qualitative data analysed using descriptive data. Data gathered was analysed using descriptive statistical tools. The results indicate that more than 48% companies globally have succumb to fraud bringing the global

cost of fraud to $1.5 trillion per year. The results of the study suggest theoretical, policy and practical implications for scholars, policy makers and practitioners. This study is relevant for this study as it helps us understand the nature of mobile money systems and frequency of fraud.

2.1.3 Zambian Perspective on mobile money fraud

The above African studies provide a smooth transition for examining mobile money fraud in Zambia. Daka and Nyirenda (2022) study a sim box fraud detection model that helps identify fraud patterns and backs artificial neural networks as an enabling tool to classify calls as either fraudulent or legit based on the attributes of the call. This basically involved using actual call detail records (CDRs) from a Zambian telecommunication company using a sample of 13,398 CDRs and a sampling without replacement technique, where each sample unit only has one chance of being selected. Both fraudulent and legitimate callers were part of the data set. The study established that Artificial Neural Network are a successful technology that can be applied in Sim Box fraud detection since it was able to detect abrupt changes in established calling patterns which may be as a consequence of fraud. The implementation of the fraud detection tool will be a big step towards detection and mitigation of Sim Box fraud for mobile telecommunication companies in Zambia. This study is relevant for this study as it shows that Mobile telecommunication companies in Zambia are trying to come up with methods and strategies to detect mobile money fraud which will be of benefit to SMEs that have adopted mobile money for their transactions.

Nyika (2024) studies the challenges in adoption of mobile money services by mobile phone users in Lusaka and utilizes a mixed methods approach. Recognizing that the challenges surrounding adoption of mobile money are multifaceted, the conclusion is security concerns are prevalent while trust and security are relevant for this ongoing study as the concerns are widespread and confidence levels in mobile money security and awareness of cyber scams vary. The results show that a good number of respondents expressed varying degrees of confidence in mobile money security, leaving a significant minority who harbor concerns or uncertainties. Most respondents showcased an awareness of cyber scams, with over half being very aware. This heightened awareness of cyber scams could be linked to the fact that more than a third admitted to having been victims of such scams. Precautionary behaviors were

widely adopted, with the vast majority refraining from sharing their PINs and many actively taking steps to safeguard their accounts. As respondents' awareness of cyber scams increased their trust in mobile money security showed a tendency to wane indicating that knowledge of potential threats is crucial for confidence in the system. This research is important for this study as it shows the existence of mobile money fraud and suggests for service providers to continue educating mobile money users on the benefits of the system by continuously communicating their efforts to assure users of their commitment to safety.

Mwape (2020) reviewed and shed more light on the current trends in the mobile money business by briefly appraising studies on the small-scale mobile money industry, with special emphasis on Zambia. The results established that mobile money is not only convenient and accessible to most people, but it has also led to economic inclusion for disadvantaged communities. Integration of the banking and mobile money system is associated security risk and challenges of mobile money especially those of fraudsters and other online criminal elements. Mobile money is targeted because a huge amount of funds is channelled through this medium and because most smartphones are prone face security threats to hackers, spam, viruses, and worms compromising the confidence in the integrity of the whole mobile payment system. This study though not in great deal, shows the availability of fraud in mobile money services providing relevance to our study. The study urges the government to incorporate privacy and cyber security mechanisms to counter the threats associated with online transactions.

2.2 Theoretical Framework

To investigate the extent to which mobile money fraud contributes to SMEs performance, employing a robust theoretical framework anchored in the Routine Active Theory and the Fraud Triangle Theory will be relevant. These two theories are relevant for this study as they provide complimentary perspectives between mobile money fraud and SMEs performance. Recognizing that mobile money fraud is a multifaceted nature, these theories offer valuable insights into the complexity of mobile money fraud, highlighting the relationship between individual characteristics and the motivation to commit fraud. The routine active theory focuses on crime as a result of a motivated offender, suitable target and the absence of a capable guardian, whereas

the FTT examines the factors that lead to fraudulent activities. The integration of these two ensures that there is both a comprehensive and well-rounded analysis.

The Fraud Triangle Theory

Overview: The Fraud Triangle Theory (FTT) dates back to 1939 to works of Edwin Sutherland who invented the terminology white-collar crime and Cressey a former student of Sutherland. Cressey in 1950 conducted a study that focused on the factors that led people to engage in unethical and fraudulent activities and is known as the Fraud Triangle Theory today. FTT was developed to offer a way to analyse mobile money fraud. For fraud to occur; perceived pressure, opportunity and rationalization should be present. The rationalization by the person committing the fraud, incentives or pressures to commit fraud and the opportunity must be present and these three factors are what is known as the Fraud Triangle (Van Akkeren, 2023). The FTT is used in this study to help understand how pressure, opportunity and rationalization can help us develop strategies such as better security to prevent mobile money fraud and detection of fraud to prevent mobile fraud losses. And it will also assist explain the implications management has to provide for prevention of future frauds.

Criticism: Critics argue that individuals are not the only causes of fraud as the triangle theory stresses, the triangle disregards organizational or systematic issues that might be present such as ineffective management, a poor working culture or lack of internal controls. For example, other than personal reasons, a system failure can lead to fraud. The FFT also places a lot of emphasis on fraud being committed by one person than the possibility of a collusion between multiple people and parties. The FFT does not address the challenge of collusion when it might affect the control of preventing fraud.

Other critics argue that the FFT does not fully explain the motivation to carry out fraud because it does not go beyond pressure, rationalization and opportunity. The FFT ignores the cultural or organisational dynamics and the factors of the system. For example, peer pressure could also contribute or lead to fraud. External influences such as a country experiencing a global financial crisis may increase fraudulent cases and the theory nevertheless the theory does not include such external factors. The other critique is the fact that the FFT was developed in the 1950s, it is therefore not a perfect representation of technology advancements over the years and cybercrime increase.

In this digital era, technological vulnerabilities are on the rise, and fraud is now more refined making hard for the fraudulent methods to fit in the triangle.

The Routine Active Theory

Overview: The Routine Active Theory is a criminology theory developed by Lawrence Cohen and Marcus Felson in 1979. This theory explains crime as a result of the convergence of three elements in time and space: a motivated offender, a suitable target and the absence of a capable guardian (Mulei, 2023). The routine active theory is relevant to this study because; Motivated offenders and mobile money fraud perpetrators are often motivated by financial gain. Motivation ranges from: the knowledge of how mobile money systems work.; Opportunities to exploit SMEs due to limited technical expertise or security measures and the high rewards with perceived low risk of being caught. Suitable Targets: due to SMEs reliance on digital transactions, SMEs are particularly attractive targets for mobile money fraud. They also usually have limited resources, handle multiple transactions and operate trust-based relations making them vulnerable to deception. Absence of capable guardians; is due to the lack of adequate security measures which also creates opportunities for fraudsters. This ranges from lack of effective verifications, lack of employee training and poor regulatory oversight and limited response mechanisms to mobile money fraud.

Criticisms: Critics argue that the routine active theory neglects the offender's motivation. It fails to account for additional motives behind an offender's motivation to commit crimes in the beginning, such as the socioeconomic, psychological or inequality issues. Critics also suggest that the routine active theory does not adapt to modern contexts and technological advancements and the role they play in digital modern crime since proximity becomes irrelevant. In this digital era, the absence of a capable guardian is irrelevant when exploiting technological vulnerabilities.

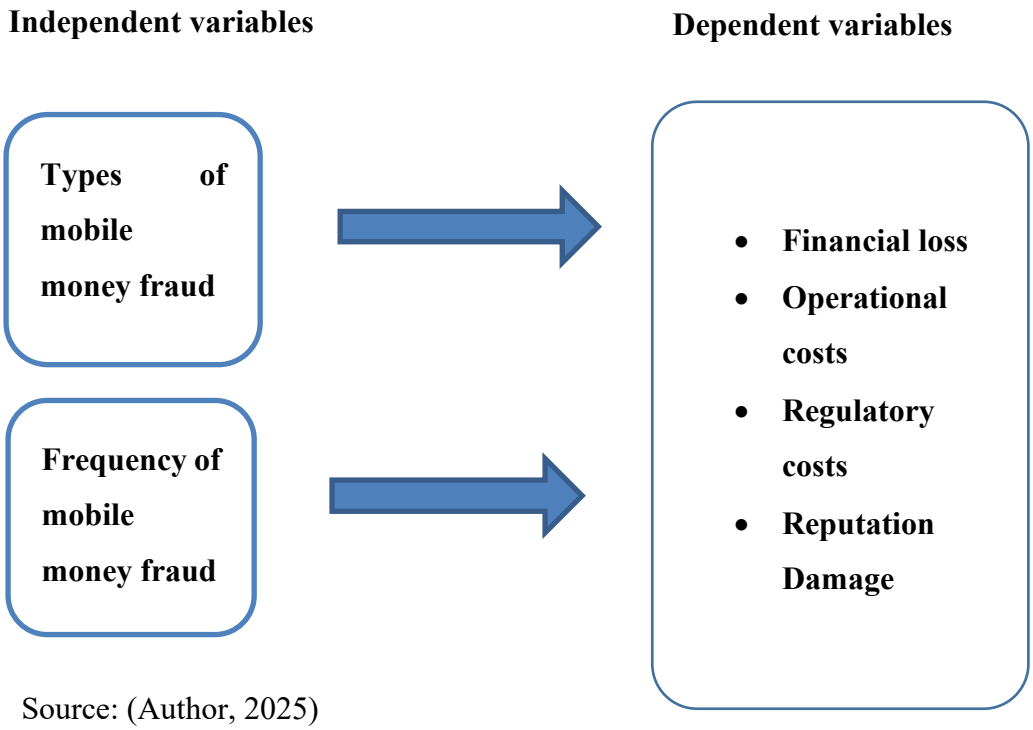
Other critics say that in a world where poverty, lack of education and inequality significantly influence crime, the routine active theory unfortunately deeply relies on situations such as target, guardianship and opportunity ignoring the overemphasis on the situational factors. Critics also suggest that the routine active theory undermines structural and societal factors that also influence crime. The routine active theory assumes an equal play field and fails to recognize systematic inequality and

marginalization and the role the system inadequacies play in creating a suitable atmosphere to conduct crime. For instance, marginalized groups are more likely to face challenges in accessing guardianship or avoiding victimization because they are not capable.

2.3 Conceptual Framework

To comprehensively explore the link between mobile money fraud and the growth of SMEs in Lusaka, a well-defined conceptual framework is imperative. According to Atkinson (2006), the conceptual framework is a visual representation that aims to analyse situations. This framework explains the dependent and independent variables, elucidating their interconnections and hypothesized relationships, thereby furnishing a structured guide for empirical investigation (Bell, Bryman, & Harley, 2022).

This conceptual framework establishes a solid foundation for empirical investigation, providing a structured and systematic approach to dissecting the intricate relationships within the realm of mobile money fraud and SME growth in Lusaka. It serves as a crucial roadmap, guiding the subsequent exploration and analysis in the ensuing sections of the thesis.



Source: (Author, 2025)

Independent variables:

Types of mobile money fraud; represents the independent variable which directly influences the dependent variables. It can be measured by the different types of mobile money fraud that SMEs can be subjected to. Different types of fraud can have varying effects on financial growth and some types are more likely than the others to cause significant damage. Significant financial losses could lead to stunt revenue growth, increased operational costs, loss of customer trust and increased expenses.

Frequency of mobile money fraud; the second independent variable represents the number of times SMEs experience mobile money fraud in their day to day operations. Higher frequency of fraud incidents correlates with greater financial losses and operational cost for most SMEs and could also result in increased expenses for SMEs.

Dependent variables:

The focal point of this study, the dependant variable is SMEs performance- a multifaceted construct encompassing diverse facets of expansion, development and financial performance. SME performance quantifies the expansion and triumph of SMEs. The performance of SMEs in relation to mobile money fraud is operationalized through the following dimensions: The variable ‘direct financial losses’ refers to the straightforward and quantifiable losses in revenue that an SME experience as a result of mobile money fraud in this study. It quantifies SME immediate loss of money results in mobile money fraud. Operational costs: This variable quantifies the increased costs that relate to preventing, responding or detecting mobile money fraud. The money lost as a result to being a victim of mobile money fraud. Damage of reputation: quantifies the loss of customer trust and the impact it will have on business revenue. Regulatory expenses; this represents the costs related to compliance with new government regulations or legal actions taken.

2.3.1 The conceptual framework and research objectives:

Objective one is the prevalence of mobile money fraud among SMEs. The effect of mobile money fraud might vary depending on the type of business or security measures put in place. A high occurrence of mobile money fraud could lead to increased financial loss, operational costs, regulatory costs and a reputation damage

as SMEs are trying to recover. This insight offers valuable lessons on the prevalence of mobile money fraud and the effect of mobile money fraud on SMEs.

The second objective is the types of mobile money fraud SMEs encounter while using mobile money services is connected to the perceived challenges of mobile money services, which can affect SMEs and lead to financial losses, increased operational and security costs and loss of confidence in the system for the sales and profitability of SMEs. Mobile money fraud is intricately connected to the usage of mobile money for selfish gains in crooked ways.

Objective three evaluates how mobile money fraud contributes to SME performance. The correlation between mobile money fraud and SME performance is complex; this can lead to ether increased or decreased sales or profits, operational costs or regulatory costs and a reputation damage. This can might lead to the development of solutions and initiatives to enhance SME satisfaction and promote the mobile money platform, offering useful insights for the development SMEs experience, tackling security issues and fostering the expansion of SMEs.

The fourth objective evaluates the effectiveness of existing fraud prevention measures used by SMEs in Lusaka. This will help user experience of the mobile money platforms. SMEs that have put in place fraud prevention measures have a higher chance of preserving their businesses from the risk of fraud and minimising financial losses, reduced profits and increased operational costs.

2.5 Conclusion

To conclude, this chapter systematically reviewed relevant literature and comprehensively examined mobile money fraud at global, regional and local perspectives. Both the theoretical and conceptual frameworks were precisely detailed focusing on the existence of mobile money fraud and it numerous effects such as financial losses, increased operational costs and loss of confidence in the mobile money system. This study has the potential to make a valuable contribution to the existing pool of knowledge, in the form of providing valued insights that can shape policies, foster innovation, and promote sustainable growth for SMEs operating in the ever-changing realm of mobile money services.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Introduction

This chapter presents the methodology that will be adopted for this research. The research methodology is crucial to ensure a systematic and comprehensive investigation on the extent to which mobile money fraud contributes to the performance of Small and Medium Enterprises (SMEs) in Lusaka, Zambia. Outlined is; the research design, target population, sampling procedure, research instruments, data collection technique, methods of data analysis, and ethical considerations followed in the study.

3.1 Research Design

To achieve practical research objectives on the subject, a mixed-methods approach was adopted for a holistic exploration of the research objectives and an explanatory sequential design to explain the quantitative findings through qualitative exploration. This research design made it easier to comprehend a large amount of data due to the strengths of the quantitative and qualitative approaches. These methods were used in synergy so as to give a rich understanding of the relationship between of mobile money fraud and SMEs performance.

3.1.1 Quantitative Research Approach

Quantitative data analysis referred to the systematic examination of data collected through a structured questionnaire. It helped for analysing the patterns, relationships, associations and other measures of statistical comparison to the research questions. Both Descriptive and inferential statistics of data were analysed using Statistical software called SPSS Statistical Package for the Social Sciences (SPSS).

3.1.2 Qualitative Research Approach

To complement the quantitative data, qualitative insights were gathered from the open ended structured questionnaire. The open ended responses allowed for richer and relatable insights. Responses provided by the study participants for Open ended questions from the study's questionnaire were analysed using the Thematic analysis.

3.2 Target Population

A population is a cluster of individuals, objects or items from which samples are drawn from measurement (Creswell, 2012). According to Lusaka City Council, there are 57 markets in Lusaka. For the purpose of this study, only 10 markets (North mead, Long acres, Chilenje Chris Corner, Chilenje, Kabwata, Libala, Kamwala, Kalundu, Matero and Chaisa) will be sampled and only 20 SME owners or employees from each market, bringing the total study population to 200. The specific sampling unit for this study was SMEs in service sector that have adopted mobile money in Lusaka, Zambia. The criteria for selection of the SMEs were companies employing less than ten people, with gross monthly revenue below twenty-five thousand Kwacha and with a business operation period less than five years.

3.3 Sampling Procedure

3.3.1 Sampling Technique

Purposive sampling was utilized in an attempt to sample only important informant that the researcher was dimmed as relevant to the research questions. Creswell (2012) contends that purposive sampling method involves the identification and selection of individuals or groups of individuals that are proficient and well informed with the phenomenon of interest. Moreover, the remaining participants were recruited by multi-stage sampling technique.

3.3.2 Sample Size

To obtain desired results, it is important to determine a sample size. Sampling is defined as the subsets of the desired population from which a sample is drawn (Creswell, 2012). Because it is rare for a researcher to analyse the entire population of the study, estimating proportions is adopted. The use of the simplified technique by Israel (1992) using the Yamane's (1967) formula was adopted to come up with the sample size.

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

n represents the sample size, N represents the size of the population and e presents the precision level (0.05). Therefore, the sample size is:

n= 200

n= 200/ 1+ 200 (0.05) (0.05)

n= 191

3.4 Research Instruments

3.4.1 Questionnaire

The chosen research instrument was a structured questionnaire that captured quantitative responses from the SME owners and employees. The questionnaire comprised both open and closed-ended questions aimed at establishing both the mobile money fraud and how it contributes SMEs performance. The subsequent questions were aligned with the research objectives and were checked for feasibility and coherence.

3.5 Data Collection Procedure

3.5.1 Model

The research model adopted in this study was an explanatory sequential research method, in which SMEs were administered structured questionnaires. The questionnaires were administered both via e-mail and directly to participating SMEs according to their preferences. The open ended questions in the questionnaire aimed at exploring the qualitative aspects of the study.

3.6 Methods of Data Analysis

To address the research questions, quantitative data was analysed using measures of descriptive and inferential statistics. Descriptive statistics such as mean, percentages and frequency distribution were used to describe the characteristics of the subjects. Demographic data was analysed by descriptive statistics while inferential data by Correlation analysis, regression analysis and chi-square tests to explore the relationship between the variables.

Qualitative information was obtained from the open ended questions and was subjected to a thematic analysis. The obtained responses were also written down and the material analysed in relation with factors such as patterns and trends. The qualitative approach offered richness and context to the assessed quantitative results in a way that clarified the research objectives even further.

3.7 Ethical Considerations

To avoid coming up with a flawed model, issues of ethics were very important when conducting the research. The study followed ethical standards to protect participants' rights and bring privacy into practice. All SME owners and employees who participated in the study signed consent to participate in the study. The following measures were adopted to ensure the collected data was protected.

Voluntary Participation: Voluntary participation means emphasising that participation is voluntary and participants are allowed to withdraw from the study at any time without any consequences or penalties. The research sought to tap positive results from the SME community in Lusaka and participants were enlightened on possible uses of the results in shaping policies and efforts to boost the SME sector.

Informed consent: Informed consent is the process of getting voluntary participation from research participates. Voluntary participation was greatly emphasized and ensured on one is forced to be a part of the study. This means the nature, purpose, objectives and benefits of the study are clearly explained by the researcher before participation (Resnik, 2020).

Confidentiality: The confidentiality of participants was highly maintained to protect them from any sort of harm that might surface from disclosing their personal information. Anonymity was the basis on which confidentiality was founded. This means that the research findings were presented in such a way that the responses could not be linked to the participants, the responses did not show which response came from which SME owners (Beauchamp, 2023).

CHAPTER FOUR: PRESENTATION AND ANALYSIS OF RESULTS

4.0 Introduction

This chapter presents the findings of the study on the extent to which mobile money fraud contributes to the performance of Small and Medium Enterprises (SMEs) in Lusaka, Zambia. The data was gathered through a structured questionnaire distributed to 191 SMEs, with less than 10 employees and less than five years of operation. The results are organised according to the questionnaire sections, beginning with general information about the businesses, followed by an exploration of their experiences with mobile money fraud, the impact of these experiences on business performance, and the preventive measures adopted.

Each question is analysed individually, highlighting trends, variations, and notable insights. The interpretations offer a contextual understanding of how these responses reflect the broader challenges faced by SMEs in Lusaka. The analysis also includes recommendations and insights that could guide policymakers, mobile money providers, and SME owners in developing strategies to mitigate the negative impacts of mobile money fraud.

4.1 General Information

4.1.1 Business Type

Figure 1 presents the distribution of SMEs based on their type of business.

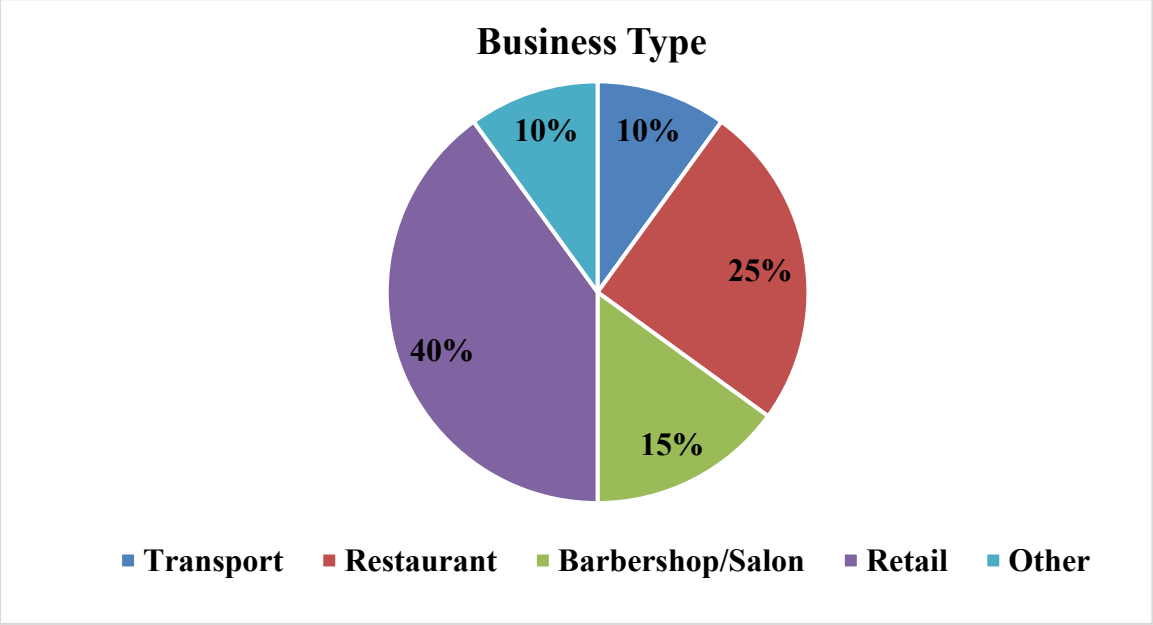


Figure1. Distribution of SMEs by business type

Figure 1 indicates that most of the SMEs are in the retail trade with 40% (n=76) of the total respondents being represented. Restaurants account for 25% (n=48), and barbershops/salons account for 15 % (n= 29). 10% (n=19) are transport businesses and the other 10% are unspecified businesses. This distribution clearly shows the high concentration of selling and eating establishment businesses in Lusaka.

4.1.2 Duration of Business Operation

Table 1 illustrates the length of time the surveyed SMEs have been in operation.

Table 1: Duration of business operation

Duration	Frequency (n)	Percentage (%)
Less than 1 year	10	5
1-3 years	86	45
4-5 years	57	30
More than 5 years	38	20
Total	191	100

The Table 1 indicates that about 45% (n=86) of the SMEs who were the majority have been involved in business operation for 1-3 years. The firms in the sample that have been in business for 4-5 years formed 30% (n=57), whereas those that have been in business for more than 5 years formed 20% (n=38). Interestingly, a meagre 5% (n=10) of the SMEs under study have been in existence for less than one year. Such conclusions indicate a trend towards increased entrepreneurship, as well as the share of rather young companies.

4.1.3 Use of Mobile Money Services

Table 2 presents the usage of mobile money services among the surveyed SMEs.

Table 2: Use of mobile money services by SMEs

Mobile Money Usage	Frequency (n)	Percentage (%)
Yes	162	85
No	29	15
Total	191	100

From Table 2, it can be seen that the majority (85%, 162) of SMEs employ mobile money services for business purposes while a paltry 15% (29) do not. This explains the high-level use of mobile money services in Lusaka as a source of finance for SMEs.

4.1.4 Number of Employees

Figure 2 provides a breakdown of the number of employees employed by the SMEs.

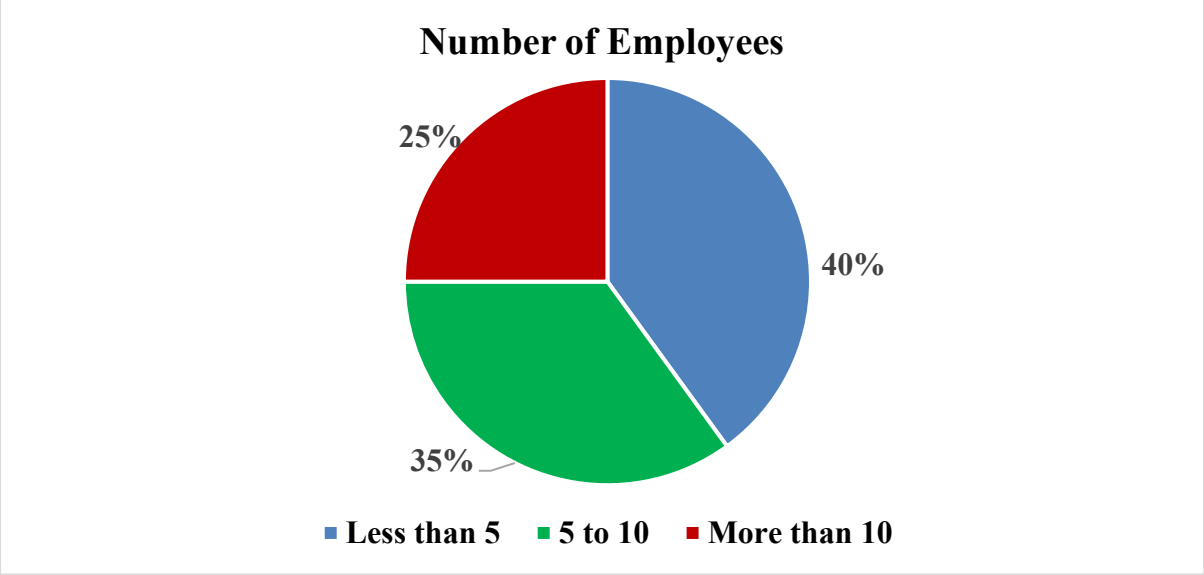


Figure 2: Number of employees in SMEs

Pie chart presented in figure 2 gives the number of SMEs that employ less than five people who made the majority as 40% (n=76), followed by 35% (n=67) employed between five and ten people and 25% (n=48) employed more than ten. These observations corroborate with the limited employment proven in the surveyed SMEs.

4.1.5 Average Monthly Revenue

Figure 3 outlines the average monthly revenue generated by the SMEs.

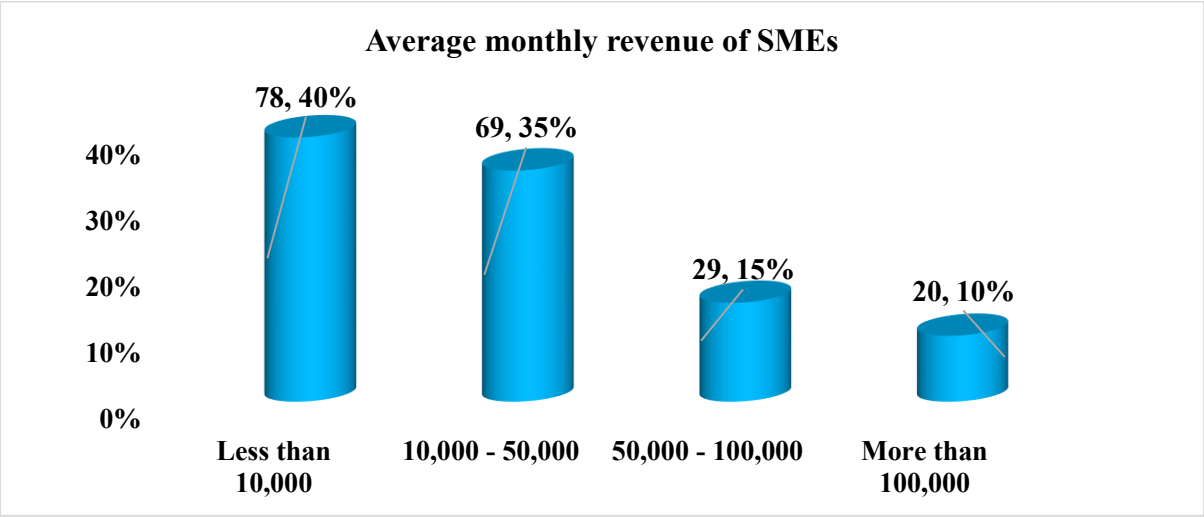


Figure 3: Average monthly revenue of SMEs

The results presented in Figure 3 reveal that 40% (n=76) of the SMEs who were the majority establish monthly sales revenue of less than ZMW 10,000. This is then

succeeded by 35% (n=67) that reported revenues in the ZMW 10,000–50,000 bracket, 15% represented 29 responses from revenues ranging ZMW 50,000-100,000 and only 10% (n=19) who reported revenues greater than ZMW 100,000. These figures show that the majority of SMEs earn within a small income level – a realisation affirming their small-scale business nature.

4.2 Mobile Money Fraud Analysis

This section examines the extent and types of mobile money fraud encountered by SMEs while using mobile money services. The findings align with the study's objective of investigating these challenges, providing a comprehensive view of SMEs' experiences with fraud.

4.2.1 Types of Mobile Money Fraud Encountered

Table 3 presents the various types of fraud that SMEs who have reported Mobile money fraud come across.

Table 3: Types of mobile money fraud encountered by SMEs

Type of Fraud	Frequency (n)	Percentage (%)
Vishing/Smishing	38	20
Advance Fee Scam	38	20
Reversal Request	29	15
False Transaction	76	40
Other	10	5
Total	191	100

The survey results shown in Table 3 indicate that the most common type of mobile money fraud is false transactions, experienced by 40% (n=76) of the responding SMEs. Most of these frauds necessarily entail manipulation of payment confirmations hence direct monetary losses.

Vishing/Smishing and Advance fee scams posed serious challenges in equal measure, with 20% of the (n=38) SMEs reporting on both kinds. Vishing/Smishing relies on untruthful messages to elicit personal details whereas, the advance fee scams involve the tricking the SMEs into paying for something believing it is the genuine deal.

A former type of fraud, reported by 15% (n=29) of SMEs, implies that fraudsters ask for a reversal of transactions on bogus pretexts relying on trust and discrepancies in operations.

The ‘Other’ category that was identified by 5% (n=10) of SMEs indicates other forms of fraud that may not be easily classified but remain as factors of the operations of the SMEs.

4.3 Frequency of Mobile Money Fraud

This section analyses the level of mobile money fraud the SMEs reported to experience in their use of mobile money service. It accumulates respondents’ answers regarding how often their SMEs experience fraud and their first impressions of such occurrences.

4.3.1 Extent of Mobile Money Fraud

Figure 4 indicates whether SMEs have ever fallen victim to mobile money fraud or not.

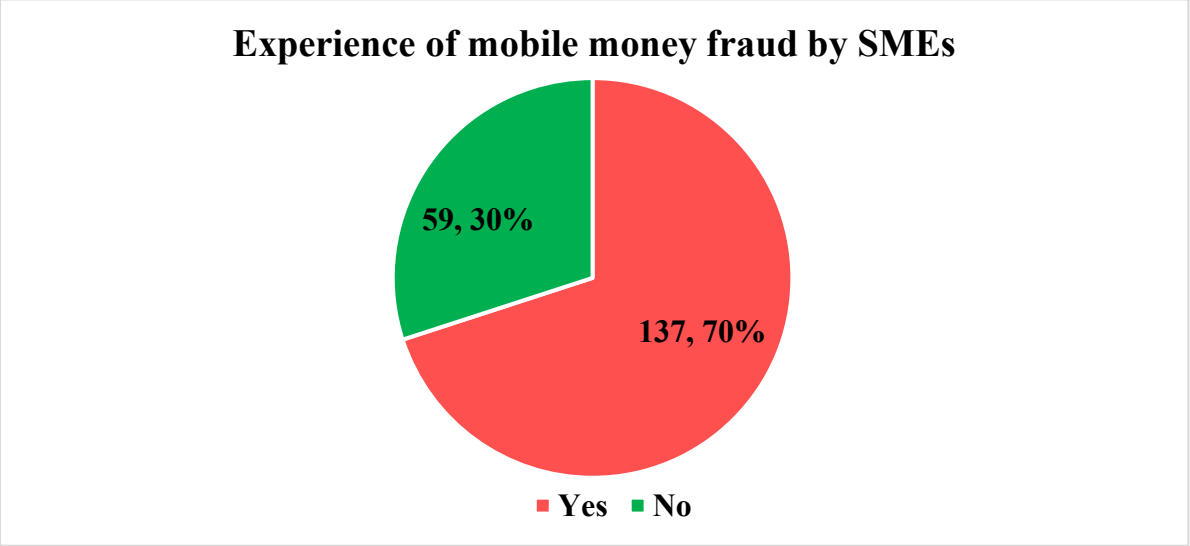


Figure 4: Experience of mobile money fraud by SMEs

The study’s findings depicted in Figure 4 indicate that most of the respondents represented by 70% (n=134) of SMEs responded affirmatively to having at some point been victims of mobile money fraud. This finding confirmed that fraud is an existing problem for SMEs in Lusaka and that most of the businesses are vulnerable to it. On the other hand, 30 % (n=57) SMEs stated they have no experience on fraud indicating that these businesses have perhaps put measures in place to prevent fraud or are located in settings which are not vulnerable to fraud.

4.3.2 Frequency of Mobile Money Fraud Experienced

Table 4 shows the incidence of fraud in the mobile money for the SMEs that responded having encountered mobile money fraud.

Table 4: Frequency of mobile money fraud experienced by SMEs

Frequency	Frequency (n)	Percentage (%)
Very frequently (once a month or more)	48	25
Occasionally (every few months)	67	35
Rarely (once or twice a year)	57	30
Never	19	10
Total	191	100

Table 4 reveals that **35% (n=67)** of SMEs encounter fraud occasionally, every few months. **25% (n=48)** of SMEs report very frequent encounters, occurring at least once a month or more. Fraud is experienced rarely, once or twice a year, by **30% (n=57)** of SMEs. Interestingly, **10% (n=19)** of SMEs indicate that they never encounter fraud, despite previously acknowledging its existence. The findings suggest that mobile money fraud is a recurring issue for most SMEs, with **60% (n=115)** experiencing it either frequently or occasionally.

4.3.3 Initial Responses to Mobile Money Fraud

Some of the actions taken by SMEs immediately they realize that they have been a victim of mobile money fraud are highlighted below in Table 5.

Table 5: Initial responses to mobile money fraud

Response	**Frequency (n)**	**Percentage (%)**
Reported it to mobile money provider	95	50
Stopped using mobile money temporarily	38	20
Tightened security measures	38	20
Took no action	10	5
Other	10	5
Total	191	100

Some of the actions taken by SMEs immediately they realize that they have been a victim of mobile money fraud are highlighted below in Table 5.

From the Table 5, it is evident that the most common response regarding fraudulent activities was reported by 50% (n=95) of the affected SMEs to mobile money providers and 20% (n=38) of the SMEs adapted enhanced security measures in order to avoid similar incidences of fraud in the future. Similarly, another 20% (n=38) temporarily discontinued using the mobile money services which could be attributed to loss of confidence in the platforms. 5% (n=10) of the SMEs shockingly to did not take any action at all after being victims to fraud, meaning these SMEs were open to prey to

fraud again. The study underscore how knowledge has to be provided to SMEs to be able have effective mechanisms of handling fraud.

4.3.4 Financial Losses Due to Fraud

The results of the analysis of the financial consequences of fraud on SMEs in the past year are presented in table 6.

Table 6: Average financial losses due to mobile money fraud

Loss Range (ZMK)	Frequency (n)	Percentage (%)
Less than 1,000	76	40
1,000 - 5,000	67	35
5,000 - 10,000	29	15
More than 10,000	19	10
Total	191	100

From table 6, 40 % (n=78) of the SMEs affirmed that they lost less than ZMK 1000 to mobile money fraud. Slightly more than a third, 35% (n=69) of the SMEs incurred losses between ZMK 1,000 and ZMK 5,000; while 15% (n=29) lost between ZMK 5,000 and ZMK 10,000. More serious losses, amounting to ZMK 10,000 or more, were indicated by 10% (n=19) of these firms. As the findings above depict, although most losses are small in value, they have a substantial effect on the profit and performance of SMEs particularly for firms with a thin profit margin.

4.4 Contribution of Mobile Money Fraud to SME Performance

This section assesses the effects of mobile money fraud on the performance of the SMEs operating in Lusaka on the basis of factors such as; Financial cost, Operations, Customer relations, and Viability. The analysis is made on the basis of the answers received regarding the influence of fraud on the SME processes.

4.4.1 Effects of Mobile Money Fraud on Business Operations

The impact of mobile money fraud on SME performance is depicted in Table 7 below.

Preventive Measure	Frequency (n)	Percentage (%)
Reputational Damage	8	4
Decreased Profitability	19	10
Loss of business opportunities	32	17
Increased operational costs	32	17
Reduced customer trust	24	12
Financial Loss	77	40
Total	**191**	**100**

Table 7: Effects of Mobile Money Fraud on Business Operations

As shown in Table 7, the most prevalent effect of Mobile Money fraud for SMEs is in the form of Financial loss as seen from the 40 % (n=77) of the responses received. They have a direct impact on the actual cash flow reducing the capital that is available for investment on business growth and profitability of operations.

Another important issue is the rise of operating costs which has been reported by 17% (n=32) of firms. It also reflects other costs that firms bear in putting up security mechanisms and in healing from fraud cases.

Decreased customer trust claimed by 12 % (n = 24) of the surveyed SMEs also worsens the situation because it influences clients' loyalty and satisfaction level. This is especially very unhelpful for those businesses employing the repeat business or the relational model.

Other symptoms are reduced profit margin (10%, n=19), potential loss of business (10%, n=20), tarnished image (4%, n=8) showing that fraud cuts across all aspects of operation – financial, operational and strategic.

4.4.2 Changes in Business Practices Due to Fraud

The adjustments made by SMEs with regards to their response to fraud have been addressed in table 8.

Table 8: Changes in business practices due to fraud

Response	Frequency (n)	Percentage (%)
Yes	115	60
No	76	40
Total	191	100

From table 8, it is evident that, out of all the SMEs 60% (115) have had to shift their business practises due to mobile money fraud. Such transformations may consist of raising the level of security, increasing the awareness of employees, or changing transactions in order to minimize fraud. Yet, 40%, (n=76) SMEs said that no business practices were changed as a result of fraud risk and this may perhaps be due to lack of resources, awareness or confidence in the efficacy of such measures

4.4.3 Interruption of Business Operations

Table 9 displays information on whether fraud affected routine business operations.

Table 9: Operational interruptions caused by fraud

Response	Frequency (n)	Percentage (%)
Yes	86	45
No	105	55
Total	191	100

Table 9 also shows that 45% (n=86), of the SMEs reported having been a victim of mobile money fraud that led to operational disruptions. Such disruptions may be the time spent to solve fraud cases, inability to access financial platforms or loss of productivity.

However, 55 % (n= 105) of the SMEs responded that there was no significant operational disruption due to fraud which may mean that fraud was well contained or did not impact the key operations of the organization.

4.4.4 Long-Term Sustainability

Table 10 determines whether SMEs think that fraud has negatively impacted on the future viability of the companies.

Table 10: Perceived impact of fraud on long-term sustainability

Response	Frequency (n)	Percentage (%)
Yes	67	35
No	76	40
Not Sure	48	25
Total	191	100

Table 10 has revealed that 35% (n=67) of the SMEs stated that mobile money fraud has affected their long-term sustainability in business. Fraud enables the depletion of organisational reserves, sullying of a company's image, and loss of customer confidence, all of which are fundamental to the sustainable growth of an organisation.

40% (n=76) of SMEs responded that they cannot see long-term effects which may be due to strong antifraud measures or awareness of long-term implications of fraud are still unknown to them as 25% (n=48) expressed uncertainty.

4.4.5 Spearman's Rank Correlation Analysis Table

This section focuses on the relationship between mobile money fraud incidence and SMEs' performance in Lusaka. Therefore, Spearman's Rank Correlation was used to test the strength and direction of this relationship. Table 4.6.1 contains the findings of the study.

Table 11: Spearman's Rank Correlation Between Fraud Frequency and SME Performance

Variable	Correlation Coefficient (r)	p-value	Significance
Fraud Frequency vs. SME Performance	-0.45	< 0.01	Significant Negative Correlation

The findings shown in Table 11 reveal that the frequency of mobile money fraud has a statistically significant inverse relationship with SME performance ($r=-0.45$, $p<0.01$). This shows how many fraud incidences can bring negative performance in SMEs' operations, therefore justifying the importance of strong anti-fraud mechanisms to protect SME performance.

4.5 Preventive Measures Against Mobile Money Fraud

This section outlines the preventive measures implemented by SMEs in Lusaka to combat mobile money fraud. It also explores their effectiveness and highlights additional recommendations to enhance protection against fraud.

4.5.1 Preventive Measures Implemented by SMEs

The preventive measures that the SMEs have put in place to protect themselves against mobile money fraud are highlighted in table 11.

Table 12: Preventive measures implemented by SMEs

Preventive Measure	**Frequency (n)**	**Percentage (%)**
Educated employees and customers about fraud risks	48	25
Implemented additional security measures	38	20
Regularly monitored transactions	75	40
Changed mobile money service providers	10	5
Used a more secure payment platform	10	5
Other	10	5
Total	**191**	**100**

Table 12 shows that the most common prevention measure employed by SMEs is monitoring of transactions as implemented by 40 percent (n=75) of the respondents. This measure captures what can be described as surveillance of events that may well be illicit in quiet discrete timeframes.

Another popular method stated by 25 % (n=48) of the SMEs is providing the employees and customers with information on fraud risks. Some of the measures include awareness campaigns and training sessions which assists the stakeholders understand these fraud indicators not to incur it.

As for the steps taken to address fraud risks, it was found out that 20% (n=38) of the respondents implemented two-factor authentication, 5% (n=10) for shifting to more secured payment platforms and 5% (n=10) for changing the mobile money service provider. The last response option was Other, in which 5% (n=10) of the respondents proposed non-traditional or context-specific approaches to changing the targets.

4.5.2 Effectiveness of Preventive Measures

Table 13 assesses the level of the effectiveness as perceived by SMEs of the measures that have been put in place.

Table 13: Effectiveness of preventive measures

Effectiveness	Frequency (n)	Percentage (%)
Very effective	38	20
Moderately effective	95	50
Slightly effective	48	25
Not effective	10	5
Total	**191**	**100**

According to the data presented in Table 12, 50 % (95) of the SMEs rated their preventive measures as moderately effective whereas 20% (38) considered they are very effective. This means that though the majority of SMEs have instituted measures with some levels of success, there is still potential for increasing their efficiency.

Another 25% (n = 48) of SMEs said their measures are slightly effective, while 5% (n=10) said they are not, indicating that some organizations continue to struggle to contain fraud risks.

4.5.3 Challenges in Implementing Preventive Measures

Using data gathered from the survey, Table 14 below shows the difficulties encountered by SMEs in the prevention of fraud.

Table 14: Challenges in implementing preventive measures

Challenge	Frequency (n)	Percentage (%)
High costs	86	45
Lack of access to secure technology	38	20
Employee resistance	19	10
Insufficient fraud prevention knowledge	38	20

Other	10	5
Total	**191**	**100**

Table 14 shows that 45% of the SMEs (n=86) identified high costs as the major impediment to the implementation of preventive measures. This includes, expenses that have to do with enhancing the security system as well as trainings that are offered by security. Other barriers that were reported include no or limited access to secure technology by 20% (n=38) of SMEs and inadequate fraud prevention knowledge among 20% (n=38) of the participants. A 10% (n = 19) rate of employee resistance to fraud prevention initiatives underlines the need for tackling the organizational culture issue more proactively.

4.6 Thematic Analysis of Open-Ended Questions

This section provides a detailed thematic analysis of the open-ended questions from the survey. By grouping responses into themes, the analysis reveals underlying patterns and actionable insights into SMEs' perspectives on mobile money fraud and preventive measures.

4.6.1 Suggestions for Mobile Money Service Providers

Responses from 48 SMEs (n=25%) suggested an improvement in the verification process to ensure secure transactions. 50% representing 96 respondents suggested providing more education and awareness campaigns for small business owners. A 10% (n=19) responses said introducing real-time fraud monitoring systems. another 10% (n=19) responses also recommended ensuring regular communication about potential fraud risks and scams. Lastly, 5% (n=10) respondents suggested offering user-friendly security features for SMEs.

Themes Identified:

Enhanced Security Measures: Many respondents emphasized the need for advanced verification processes, such as biometric authentication or two-factor verification. This highlights a demand for robust systems that reduce the likelihood of unauthorized access and fraudulent transactions.

Education and Awareness: A significant proportion of respondents called for regular education campaigns targeting both SMEs and their customers. Topics could include recognizing phishing scams, managing secure passwords, and responding to suspicious activities.

Technology Integration: SMEs frequently suggested real-time fraud monitoring systems as a critical requirement. These systems could provide instant alerts for suspicious activities, enabling businesses to act swiftly and mitigate risks.

User-Focused Design: Some respondents recommended that mobile money service providers focus on designing user-friendly interfaces that make security features easy to access and use, particularly for SMEs with limited technical expertise.

These responses underline the pivotal role of mobile money service providers in fraud prevention. By investing in security technologies, conducting awareness campaigns, and improving user experience, providers can foster trust and reduce vulnerabilities in their platforms. This also reflects SMEs' reliance on service providers for safeguarding financial transactions, indicating an opportunity for collaborative initiatives.

4.6.2 Suggestions for Regulatory Institutions

40% (n=76) of respondents suggested an introducing stricter penalties for mobile money fraud. 20% (n=38) respondents recommended creating a centralized fraud reporting system accessible for SMEs. Another 20% (n=38) represent making it a mandate to conduct regular audits of mobile money service providers. Only 5% (n=10) recommended to enforce standardized security protocols across all providers and 15% (n=29) recommended promoting transparency in fraud investigations and resolutions.

Themes Identified:

Stricter Regulations and Penalties: Many respondents expressed the need for tougher penalties for fraudsters to act as a deterrent. This includes legal consequences and financial penalties for individuals or entities involved in fraudulent activities.

Centralized Fraud Reporting: SMEs highlighted the importance of a centralized reporting system that allows businesses to easily log and track fraud cases. Such a system would provide data for regulators to monitor trends and address systemic issues.

Provider Accountability: Calls for mandatory audits and compliance checks point to SMEs' concerns about the transparency and reliability of mobile money providers. Ensuring adherence to standardized security protocols could enhance trust in the system.

Transparency and Communication: Respondents emphasized the need for transparent investigations and regular updates on resolved cases to boost confidence in regulatory bodies' efforts to mitigate fraud.

The responses reflect SMEs' reliance on regulatory institutions to create an enabling environment that ensures fairness and security. Stricter oversight, combined with user-friendly reporting mechanisms, would help address existing vulnerabilities in the system.

4.6.3 Additional Preventive Measures Recommended

35% (n=67) suggest to provide low-cost fraud prevention tools for small businesses. A total of 25% (n=48) responses encourage collaboration between SMEs and mobile money providers. 15% (n=29) recommended a launch community-based fraud awareness programs and another 15% (n=29). 5% (n=10) responses encourage establishing affordable insurance options for SMEs affected by fraud and another 5% (n=10) recommend developing a simple fraud prevention guidelines tailored for SMEs.

Themes Identified:

Cost-Effective Solutions: Many SMEs expressed concern about the high costs of implementing preventive measures, suggesting a need for affordable, scalable tools such as low-cost fraud detection software or subsidized security upgrades.

Collaboration and Partnerships: Responses frequently highlighted the importance of stronger partnerships between SMEs, mobile money providers, and regulators. Collaborative efforts could include shared databases of known fraudsters, joint awareness campaigns, and co-developed solutions.

Community-Based Interventions: Several respondents suggested community-level initiatives, such as workshops and training sessions, to build collective awareness and resilience against fraud.

Insurance Options for Fraud: Some SMEs recommended introducing affordable insurance plans to help businesses recover from financial losses caused by fraud. This would act as a safety net and encourage greater adoption of preventive measures.

Guidelines and Resources: Respondents emphasized the need for simple, clear guidelines tailored to SMEs, including practical steps to avoid common fraud risks and manage incidents effectively.

These responses highlight the critical need for inclusive and practical solutions that cater to the unique challenges faced by SMEs. By addressing cost barriers, fostering collaboration, and providing accessible resources, stakeholders can create a supportive ecosystem to combat fraud effectively.

Thematic analysis of open-ended questions reveals that SMEs in Lusaka face multifaceted challenges in addressing mobile money fraud. Key themes—such as enhanced security, regulatory oversight, cost-effective solutions, and community collaboration—underscore the importance of a multi-stakeholder approach to tackling fraud.

This section reflects the necessity of targeted, actionable measures to empower SMEs, improve system security, and foster trust in mobile money platforms. These insights inform both practical recommendations and future research directions.

CHAPTER FIVE: DISCUSSION OF FINDINGS

5.1 Overview

Based on the study results, findings on the type of mobile money fraud encountered by SMEs in Lusaka are discussed in this chapter. The study findings are discussed in conjunction with relevant literature to provide an in depth understanding of the fraud landscape. In this chapter, the findings are contextualized and are shown as part of the larger body of research, thus indicating the implications for SMEs and possible strategies for grappling with the mobile money fraud challenges without bias.

5.2 The prevalence of mobile money fraud among by SMEs

The study found that mobile money fraud is a recurrent problem for SMEs in Lusaka, 35% (n=68) of businesses reported that it presented itself once in a while, every few months, while 25% (n=48) stated they encountered it very often, at least once a month or more. The high rate of recurrence of fraudulent activities in the mobile money environment serves as a reminder of how persistent a threat fraudulent activity could be. However, 30% (n=57) of SMEs reported fraud rarely, once or twice a year, and 10% (n=19), did not encounter fraud, indicating difference in the level of exposure, potentially the result of SMEs different business practices, security measures and business environment.

Mobile money fraud frequency experienced by SMEs follows a similar trend in other regions. Salim (2022) mentions that there is a high prevalence of phishing and spoofing in Zanzibar that frequently hamper businesses by compromising user accounts and transactions. Also, Lambongang (2023) reported frequent reoccurrence of fraud incidents in Kumasi, Ghana through the utilization of security vulnerability and users' fear of being violated with their personal information. The implication is that the same challenges SMEs in Lusaka are experiencing, are applicable to SMEs in other developing markets as smacks of consistency of fraud persistence in developing markets.

The frequency with which fraud can occur calls for strong mitigation practices. According to Franco (2023), Africa's mobile money fraud frequency is fueled by fast technological progress and the ongoing creation of fraud methods. Frequent and Passive fraud encounters are high when frequent fraud is encountered in Lusaka due to lack of proactive interventions including better fraud detection systems, better

transaction monitoring, and heightened awareness among users to reduce the susceptibility.

Finally, the prevention of mobile money fraud that SMEs experience in Lusaka is an issue that needs vital solutions. Findings include that most SMEs are recurrently affected by fraud that has operational efficiency and financial stability implications. These risks need to be mitigated and steps have to be taken to ensure sustainable business practices, and effective strategies needed include technology driven solutions and awareness campaigns.

5.3 The Types of Mobile Money Fraud Experienced by SMEs

The findings of the study established that False transactions were the most predominant type of fraud experienced by SMEs, with 40% of respondents (n=76) reporting that is a problem for them. False transaction is characterized by payment confirmations manipulation, which in turn leads to financial losses for businesses. The findings are similar with Salim's (2022), who also pointed out the problems of fraudulent transactions in Zanzibar. The higher prevalence of false transactions shows that payment authentication processes are plagued with systemic weaknesses which call for more advanced verification processes to secure SMEs' businesses.

Also, vishing and smishing are just a couple of other fraud types established by the study, with 20% (n=38) of SMEs reporting that they have been victims of these schemes, as well as advance fee scams. Advance fee scams are fraudulent calls and texts that prey on SMEs by asking them to make upfront payments to receive services, while vishing and smishing recruit victims by sending out deceptive text messages or making immune phone calls with the hopes of getting sensitive information from the target. This correlates to fraud patterns observed in Pakistan that Razaq et al. (2021), reported in similar social engineering tactics leveraging mobile money users.

Reversal requests, which were experienced by 15% (n=29) of SMEs is another form of fraud established by the study. When using this tactic, fraudsters leverage operational gaps and user trust to claim that transactions need to be reversed. Similar approaches have been reported in Ghana by Akomea-Frimpong et al. (2019), where they indicated that weak internal controls facilitated such manipulations. However, reversal requests remain a risk for SMEs in spite of it being a less common fraud tactic as compared to the ones discussed above.

5% (n=10) of the respondents reported fraud related to the “Others” category, which can be considered as likely representing more emerging, or less defined, fraud methods involving variations of phishing and spoofing techniques. However, fraud schemes have become more sophisticated and Njoya et al. (2023) suggest technology driven solutions, such as reinforcement learning, may be able to keep pace with the changing fraud landscape.

Adedoyin (2018) stated that the anonymity and speed of mobile money transactions are enablers of fraud which the findings agree with the global trends. Finally, consistent with the patterns in Lusaka, Annan (2017) finds general fraud is highly prevalent in Ghana, primarily in large transaction values. Trust in mobile money systems, too, is of vital importance: Fianu et al. (2023) specified trust as an important factor as decreasing levels of trust increased vulnerability to fraud.

Mobile Money Fraud poses significant challenges to SMEs and this study’s findings highlight this challenge. The landscape overflows with false transactions, showing that system reliability is weak. Vishing and smishing which are communication-based frauds also indicate the need for increase awareness and education about this to SMEs. The request for reversal as a new fraud technique indicates a continuously moving fraud front and underlines the need for acting pre-emptively to combat the Vise. Addressing these challenges, especially in mobile money, will increase security protocols for the SMEs and awareness for the customers, reducing risks of fraud and enhancing SMEs operational resilience.

5.4 Contribution of Mobile Money Fraud to SME Performance

The findings show that the operation of mobile money frauds significantly affects SME performance in Lusaka. The most critical impact was financial losses which affected 50% (n=98) of SMEs. These losses reduce the available financial resources to grow business and conduct operational activities, adversely impacting profitability. These observations consistent with Mvogo et al. (2022), who detected that the financial loss from fraud raises operational risks thus constraining SMEs from effectively availing themselves of the advantages of mobile money services.

Another major issue was increased operational costs reported by 30% (n=57) of SMEs. Fraud incidents as well as the implementing preventive measures, also create considerable new expenses for businesses. The power of these findings is further

realized as they support observations made by Rahayu (2015) showing that mobile money fraud causes businesses to allocate more resources to security, thus straining the budget of the business to such an extent that growth is stifled.

The study also showed that reduced customer trust (n=38; 20%) has a significant impact in client retention and satisfaction. This is also the view as emphasized by Tengeh and Talom (2020) that trust constitutes a crucial requirement for the continual usage of mobile money services. Let's face it — When customers lack trust in these systems and continuously fall victim to fraud, the cycle becomes a discouraging one for the customers as well as the SMEs depending on generating repeat transactions.

Reduced profitability (15%, n=29), loss of business opportunities (10%, n=19), and reputational damage (5%, n=10) are additional impacts of the mobile money fraud other than the cost of customer acquisition and loss of revenue. These findings corroborate Simate (2013) who pointed out that SMEs are prone to operational discontinuities caused by fraudulent activities in areas with minimal fraud precautionary measures.

Surprisingly, 60% (n = 115) of the SMEs indicated how they are utilizing new business rules following fraud, for example, reinforcing security measures, and providing employee training. The proactive changes these SMEs have taken show resilience and willingness to adapt in order to reduce fraud risks. However, 40% (n=76) stated there were no changes (no resources or confidence in the effectiveness of such measures). The same is noted by Ngaruiya (2014) who highlighted the importance of having robust training and support systems to enable SMEs to adopt strategies to effectively prevent fraud.

In addition, operational interruptions due to fraud were reported by 45%, or n = 86, of SMEs. These disruptions result from investing time in resolving fraud cases or recovering access to financial platforms and cause an impact on productivity. On the other hand, those who say they haven't dealt with fraud, perhaps because they managed it well or had little exposure, numbered 55% (n=105). The findings of these match those of Chale and Mbamba (2014), that effective fraud management practices can significantly cut down on disruptions and operational continuity issues.

With respect to long term sustainability, 35% (n=67) perceived that fraud had a negative impact, 40% (n=76) felt it had no long-term impact and 25% (n=48) were not

sure. This variability in uncovers different levels of SME resilience and effectiveness of countermeasures. Talom and Tengeh (2019) indicated that mobile money services can improve financial performance, but the fear of fraud can discourage SME use of these benefits to the full.

Spearman's Rank Correlation shows further that there is a significant negative relationship ($r = -0.45$, $p < 0.01$) between frequency of mobile money fraud and SME performance. This means frequent fraud incidents are directly impacting the business operating and profitability metrics, compelling the need for robust preventive strategies. According to Botchey et al. (2020) advanced machine learning algorithms like gradient boosted decision trees could assist SMEs in addressing these hurdles by aiding in fraud detection and prevention.

Finally, the study shows that mobile money fraud is a threat to SME Performance in Lusaka, hampering access to financial resources, operational efficiency and customer trust. Addressing these challenges through security training and technological innovations such as blockchain and bitcoin could help SMEs overcome fraud and make them more resilient and sustainable.

5.5 Preventive Measures for Mobile Money Fraud

From the study's findings, it can be noted that SMEs in Lusaka have developed different measures to counter mobile money fraud risk factors. Frequent monitoring of transactions revealed itself as the most implemented control mechanism as stated by 60 % (n=115) of the SMEs. This supports calls for a robust monitoring mechanism that can efficiently identify risky transactions as they unfold since Adeboye, (2024), established that periodic reviews and assessments are indispensable in combating fraud. Also, employee and customer fraud risks education awareness were also suggested by the SMEs, with 55% (n= 105) clearly indicating that awareness and knowledge is very important factor in identification of fraudulent risk. The finding in line with the arguments advanced by Sumbwanyambe (2023) who has also recommended a detailed awareness education on risk issues in the financial transactions.

Additionally, 45% (n=86) of SMEs employed further security precautions including using two factor authentication, a clear indication that technology must be used to increase security. Furthermore, a small number (20%, n=38) of SMEs made changes to improve the security of their mobile money transactions by shifting to secure

payment platforms and 10% (n=19) moved to new mobile money service providers. The lower adoption rates of more sophisticated technology which prevents fraud, of course, suggest possible threats, like higher costs than in the developed world, or insufficient access to sophisticated systems. Interestingly, Franco (2023) noted that other advances such as machine learning algorithms to estimate and guard against fraud could successfully overcome these shortcomings.

The impact of these preventive measures was therefore not viewed in a similar manner by all SMEs. 50% (n=95) of participants described the impact of their measures as moderately effective while the other 20% (n=38) responded as having adopted very effective measures. The compared expenditure for each strategy and the results indicated a possible scope for enhancing the actualization of the two strategies. On the other hand, 25. % (n=48) regarded their measures as moderately effective while 5% (n=10) considered them as ineffective measures. These ideas coincide with Lokanan (2023), suggested that a lot of potential to apply practical tools for instance predictive analysis to increase fraud prevention rates exist.

Furthermore, difficulties in implementing measures of prevention were revealed as the main issue, highlighting the high cost that comes with procuring technology that can assist with preventive measures as cited by 45% (n=86) SMEs. The cost that comes with upgrading the security system for the organizations run by SMEs and training of employee denoted notable limitations; especially for organizations with access to limited funding. A 35% (n=67) of participants further listed lack of access to technology that is safe as another obstacle, and 30% (n=57) reported do not have sufficient knowledge on fraud prevention. Resistance by employees; 20% (n=38); also points to the need for the organization to adopt a culture that encourages positive attitude towards fraud prevention.

Conducting and analyzing responses regarding specific mobile money fraud experiences with Thematic analysis elicited practical knowledge for both the mobile money service provider and the regulatory authorities. The majority of the SMEs proposed improving the security features within their accounts like biometric login options and fraud check in real-time. Further, enhanced awareness programs and clear conceptual fraud prevention measures pointing for SMEs were mentioned often. It also called on regulatory institutions to increase federal sentences for fraud, include

audit requirements for mobile money providers, and establish individual centralized fraud complaint facilities.

These findings align with previous works, for instance, Zimba et al. (2022) who called for policy measures to prevent the main weaknesses of GSM networks, and therefore cut short the many risks that mobile money fraud poses. In the same regard, Simate (2013) highlighted the criticality of responding to immanent security threats in the antiquated framework of mobile networks for SMEs in Zambia.

Therefore, this research points to need for more tangible and coherent measures that will help protect the SMEs against mobile money fraud. Currently, there are many barriers like high costs and limited access to security technologies, as well as lack of cooperation between SMEs, service providers, and regulators – which can be eliminated in order to come up with a more secure ecosystem.

5.6 Limitations of the Study

There are some limitations that may have affected the study which ultimately affects the understanding as the generalisation of results on the extent to which mobile money fraud affects the performance of SMEs in Lusaka. Each limitation is discussed below, along with the mitigation strategies employed:

Self-Reported Data: Respondents might have overestimated or underestimated incidences of fraud in the mobile money sector and the effects it has on the performance of the SMEs. Some respondents might have given only the answers that they felt were appropriate in the society rather than the reality. To deal with this limitation, the study ensured that the respondents remain anonymous and confidentiality was observed. To check for reliability of the responses the cross-validation questions were provided in the questionnaire. Further, a pilot study was used to improve the formulated questions and eliminate instances of misunderstanding to ensure improved reliability of obtained information.

Recall Bias: Participants' reports of prior use of the mobile money services for fraud may have been subject to recall bias because it might have been difficult for participants to recall some of their past experiences. This was done in the development of the questionnaire to make it cover the last one year in the incidents of fraud and to have it well described of what was required in terms of time recall. Such

an approach stemmed auto-recall of information and made the reportage more accurate.

In recognizing these limitations, the study forms a sound starting point in establishing the phenomenon of mobile money fraud and its impact on the performance of SMEs, together with the need for further study and prevention.

5.7 Chapter Conclusion

This chapter summarized the study results on the types, frequency and effects of mobile money fraud on SMEs in Lusaka with key issues like money loss, raised operating expenses and reduced customer confidence. Preventive measures discussed included transaction monitoring, and employee training measures. However, the study brings out useful information on the threats that SMEs are likely to encounter and the counteractions against fraud. Mobile money tenancy innovations highlight the need for collective action by SMEs, Mobile Money Service Providers, and regulators to build resilience to fraud. The implications of this research are useful to the policymakers and other stakeholders, who seek to encourage and safeguard SMEs with central relevance to Zambia’s economy.

CHAPTER SIX: CONCLUSION AND RECOMMENDATIONS

6.1 Chapter Overview

In this chapter, the results of the study are summarized in two areas: the effects of mobile money fraud on the performance of SMEs in Lusaka and the measures used to address these problems. The research goals aligned the different types of mobile money fraud and how often it occurs, and on investigating the impact and countermeasures in the context of SMEs. And lastly, chapter 6 recommends to SMEs techniques which can be used for SMEs to become resilient against fraud and future directions for enlarging the research scope.

6.2 Conclusion of the Study

The research established that mobile money fraud is a vice that affects SMEs in Lusaka as 60% (n=115) of the SME participants interviewed had experienced fraud incidences. Regarding the nature of fraud carried out against their businesses, 40% (n = 76) of the respondents reported false transactions to be the most prevalent type of frauds followed by vishing/smishing and advance fee scams qualifying 20% (n=38) of SMEs. These findings point to inherent weaknesses in mobile money systems at the system level, mainly in payment confirmation procedures and threats arising from social engineering strategies.

SME fraud frequency shows that 35% (67) reported that they are affected by fraud at least sometimes, while 25% (47) said that they are affected by fraud very often, within a month. The above percentages show that fraud remains a very real threat and must always remain a topical issue and call for more preventive strategies. Consequently, fraud frequency was negatively and significantly associated with SME performance, ($r = - 0.45$, $p < 0.01$), which signified that frequent fraud compromised the SMEs' operational efficiency, profitability, and customer credibility.

The study further elaborated that 50% (n=96) of the total sample size, quantified financial losses as the most severe consequence of fraud that hinders funds that can be used to expand business or operation. Other effects were increased operation costs, this impacted 30% (n=57) of the respondents and decreased customer trust in the SMEs, this impacted 20% (n=38) of the firms, thus further illustrating the diverse effects of fraud to SMEs. Measures that were in place are transaction monitoring (60%, n=115) and fraud risk education for employees (105, 55%); although the following are

some of the problems - high cost that organizations faced during implementation (86,45%) and lack of access to secure technologies (67, 35%).

It was observed that underserved SMEs require a higher level of security, including biometric authentication and live fraud detection and called for a promotional crusade to raise the level of awareness on the subject. Regulatory recommendations were setting new measures to implement severe punishment for fraudsters, establishment of central agencies for reporting fraud cases and compulsory checking of mobile money providers.

Therefore, the findings of the study emphasize the high prevalence of mobile money frauds and how they impact the performance of the SME in Lusaka. In general, the SMEs have implemented several preventive measures but the gaps in the resource, technology and awareness remain evident. All these challenges require collaboration between the SME's, service providers, and the regulators. Thus, it is possible to help SMEs and develop the Zambian economy using a secure and less vulnerable mobile money platform supported by stakeholders.

6.3 Recommendations and Application

The following recommendations are suggested for consideration in tackling the problem of mobile money fraud as well as its consequences to SME performance Practical applications of the recommendations are also brought to enhance their implementation.

1. There is need for mobile money service providers to improve the security aspects in their systems through integrating complex aspects like finger print scanning, passwords, and comprehensive fraud detection mechanisms in real times. These would give SMEs more protection against fraud, which at present is a significant weak point in many payment systems. It is importance for providers to make these tools easily understandable and take necessary training sessions for SMEs to get optimal benefits from them and these protocols must be changed frequently due to increased sophistication of fraud tricks.
2. There should be more keenness on corporate ablaze and enlightening crusades in order to ensure that SMEs and their employees have a clue into the way fraud can be looked out for. Larger scope providers, legislative bodies,

and SME associations should work together to produce appropriate content of training materials suitable especially to the small business enterprises like video clips, seminars, and internet platforms. Sharing of such information would be most effective through other special events within the community or through the Internet.

3. There is need for an enhancement of the level of regulation to reduce fraud by enhancing the regulations through the improvement of standards of compliance, involving stricter penalties for the fraudsters, and developing a single central reporting system for the fraudsters. That is why such a system would enable SMEs to report incidents and track the case resolutions with ease and contribute to the analysis of trends to enhance policy formulation. Periodic assessment of the providers would help in the creation of awareness on compliance to the set security measures because users would be confident in the service providers.
4. Specific measures to reduce fraud and computers with related technologies which should be low priced and adapted for SMEs should be created and offered. This could comprise of affordable security software, inexpensive detection mechanisms and even monetary incentives for the acquisition of the same. The technology firms in collaboration with donor organizations can be used to develop fraud solutions that can be implemented by all SMEs regardless of the level of resource constrain.
5. Industry stakeholders, particularly the SMEs, the mobile money providers, and the regulators need to work together in a bid to fight fraud. Formation of working groups which will address the most frequently reported fraud types, establishment of databases containing information on the frequently observed fraud types, and the organization of joint awareness raising activities would allow for a concerted approach towards combating the challenges occasioned by mobile money fraud.
6. Last but not least, insurance solutions applicable for SMEs should be promoted in order to protect from the financial damage that may result from fraud. The SMEs should be provided with cheap insurance policies that best suit their exposures to risks, so that upon being insured they would take precautions

without fear of loss. Insurers and both major and SME associations ought to work together to develop and advertise these policies, as well as review the policies on a regular basis to hone them.

However, to make the above recommendations effective it was established that regular monitoring, stakeholder feedback and the use of adaptive strategies must also form part of the implementation process. Such a combined strategy would help SMEs to be equipped and fight fraud and, as a result, become sustainable, thus making their impact on Lusaka's economy positive.

6.4 Future Research

Future research should aim to deepen the understanding of mobile money fraud and its impact on SMEs, focusing on the following areas to complement and extend the findings of this study:

1. Subsequent studies should employ a longitudinal study using a panel data design to assess the changes that mobile money fraud has on SME performance in the long-run. They might contain information on a continuous occurrence of fraud affects vision of complete business sustainability, organizational changes, and the development of countermeasures.
2. Successive study can examine the social and economic impact that advances in fraud of mobile money services has on SMEs and stakeholders and the effects it has on employment and local economies. This analysis would promote for better appreciation of the effects of mobile money fraud has on economic growth.

Hence, closing these gaps, the future research will make a significant contribution to delineating the specific types of mobile money fraud and designing evidence-informed LT-Fintech interventions for SMEs and the public, with an aim at increasing the level of trust in digital financial systems and fostering the economic development.

References

AFI. (2017). *Mobile Financial Services Basic Terminology.* doi:https://doi.org/10.3403/30281584u

African Development Bank. (2023). *Supporting Small and Medium Enterprises in Africa.* doi:https://doi.org/10.18356/9789213586228c007

Agboh, Y. P. (2021). Small business owners' strategies for accessing capital and improving financial performance. *(Doctoral dissertation, Walden University)*.

Aker, J., & Fafchamps, M. (2010). Mobile phone penetration and economic growth in Africa. *Journal of Economic Perspectives, 24*(3), 21-38. doi:https://doi.org/10.1257/jep.24.3.207

Amponsah , E. O. (2018). The Advantages and Disadvantages of Mobile Money on the Profitability of Ghanian Banking Industry. *Texila International Journal of Management*, 4, 1-8.

Aremu, M. A., & Adeyemi, S. L. (2011). Small and medium scale enterprises as a survival strategy for employment generation in Nigeria. *Journal of sustainable development*, 4(1), 200.

Aron, J. (2018). Mobile money and the economy: A review of the evidence. . *The World Bank Research Observer*, 33(2), 135-188.

Atkinson, H. (2006). *Strategy for implementation: a role for the balance scorecard? Management Decision.(pp. 1441-1460)..* University of Brighton. doi:https://doi.org/10.1108/00251740610715740

Awa, H., & Ojilabo, O. (2015). Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. *Journal of Science & Technology Policy Management, 6*(1), 76-94. doi:https://doi.org/10.1108/jstpm-04-2014-0012

Bell, E., Bryman, A., & Harley, B. (2022). *Mixed methods research: Combing quantitive and qualitative research methods.* doi:https://doi.org/10.1093/hebz/9780198869443.003.0040

Blackwood, D., & Smith, J. (2021). Cybersecurity concerns of SMEs using mobile money services in Lusaka, Zambia. *Journal of Business Ethics, 182*(3), 457-472.

BOZ. (2018). *Mobile Money and Small and Medium-Sized Enterprises in Zambia.* Lusaka: Bank of Zambia.

Brown, S., Green, K., & Blackwood, D. (2020). Mobile money and SME growth in urban Africa: The case of Lusaka, Zambia. *Journal of African Business*, 365-382.

Bruh, M. (2019). *The impact of mobile mony on poor rural housholds: Experimental evidnece from Uganda. In AEA randomized controlled trials.* American Economic Association. doi:https://doi.org/10.1257/rct.4605-1.0

Carlos, M., & Soares, A. (2011). Examining the technology acceptance model in the adoption of social networks. *Journal of research in Interactive Marketing, 5*(2/3), 116-129. doi:https://doi.org/10.1108/17505931111187767

CGAP. (2016). *Small and Medium Enterprise Finance and Mobile Banking in Zambia. CGAP.* CGAP.

Chen, H., & Zhang, M. (2018). Early growth states of small business in China: The business model perspective. *International Journal of Entrepreneurship and Small Business, 35*(2), 220. doi:https://doi.org/10.1504/ijesb.2018.10016269

Chipa, N., & Mwanza, B. G. (2021). Factors Impeding Mobile Money Expansion in Zambia. *International Journal of Engineering and Management Research*, 11(1), 178–186. https://doi.org/10.31033/ijemr.

Chishala, M., & Tembo, L. (2022). The long-term impact of mobile money services on the financial inclusion of small and medium-sized enterprises (SMEs) in Zambia. *Journal of Financial Services Research, 111*(2), 363-384.

Chundu, A., & Mutisunge, J. (2022). Factors affecting the adoption of mobile money services by small and medium-sized enterprises (SMEs) in Zambia: A case study of Lusaka District. *Journal of African Business Research, 3*(1), 1-16.

Cole, H. (2019). Money. *Finance and Finacial Intermediation*, 115-125. doi:https://doi.org/10.1093/oso/9780190941697.003.0009

Demirguc-Kunt, A., & Klapper, L. (2015). The global findex database 2014: Measuring finacial inclusion around the world. In policy research working papers. *The World Bank*. doi:https://doi.org/10.1596/1813-9450-7255

Donou-Adonsou, F., & Amekudzi, A. (2019). Mobile banking and financial inclusion in Sub-Saharan Africa: Evidence from panel data. *Journal of African Business Research, 10*(4), 463-481.

Fafchamps, M., & Aker, P. (2014). Mobile phone coverage and producer markets: Evidence from West Africa. *American Economic Journal: Applied Economics, 6*(1), 1-33. doi:https://doi.org/10.1111/joes.12372

Fowowe, B. (2008). Financial Liberalization Policies and Economic Growth: Panel Data Evidence from Sub-Saharan Africa. *African Development Review*, 549-574. doi:https://doi.org/10.1111/j.1467-8268.2008.00198.x

Frempong, G. (2009). *Mobile telephone opportunities: the case of micro‐and small enterprises in Ghana, info, Vol. 11 No. 2, pp. 79-94.* Emerald Group Publishing Limited. doi:https://doi.org/10.1108/14636690910941902

Global Findex. (2021). *Global Financial Inclusion (Global Findex) Database. Financial Inclusion. Pakistan Wave 4 Report FII Tracker Survey.* Pakistan: InterMedia: Washington, DC, USA.

Green, K., & Brown, S. (2018). Mobile money and SME financial growth: Evidence from Lusaka, Zambia. *International Journal of Finance, 15*(2), 312-341.

Hasnain, S., Komu, A., & Black , C. (2016). Mobile money in the Philippines: market conditions drive innovation with Smart Money and GCash.

IFC. (2020). *Regulatory and Policy Issues for Mobile Financial Services in Developing Countries.* IFC.

John, K. E., Gwahula, R., & Msemwa, F. M. (2018). The Influence of Perceived Risk on the uptake of Mobile Money Services by SMEs Operations in Karagwe District, Tanzania. *International Journal of Advanced Engineering, Management and Science, vol. 4, no. 9*, 4, 703-712.

Johnson, L., & Brown, T. (2022). Mobile money and SME growth in Africa: A cross-country analysis. *African Development Review, 34*(4), 412-433.

Jones, P., & Blackwood, D. (2019). Mobile money and digital literacy among SMEs in Lusaka, Zambia. . *Journal of Information Technology*, 467-472.

Kawimbe, S. (2022). Factors affceting listing of small and meduim enterprises on LuSE alternative investment market in Zambia: A case of Lusaka Business DIstrict. *International Journal of Current Science Research and Review, 5*(10). doi:https://doi.org/10.47191/ijcsrr/v5-i10-14

Kendall, J., Machoka, P., Veniard, C., & Maurer, B. (2011). An emerging platform: From money transfer system to mobile money ecosystem. *UC Irvine School of Law Research Paper*, 2011-14.

Long, E. (2022). *Mobile money and financial inclusion in Kenya and Tanzania. .*

Lwonga, E., & Mwaura, J. (2017). The role of mobile money services in financial inclusion: The case of Tanzania. *The Electronic Journal of Information Systems Evaluation, 14*(1), 1-6. doi:https://doi.org/10.1596/26393

Makhandia, C. S., Miroga, Dr. J, Otinga, & Dr. C.H.N. (2022). (MAKHANDIA, C. S., MIROGA (PhD), DR. J., & OTMobile Money Services and Financial Growth Of Small and Medium Enterprises In Kakamega Town, Kenya. *Strategic Journal of Business & Change Management*, 9(2).https://doi.org/1.

Mas, I., & Morawczynski, O. (2009). *Designing mobile money services: Lessons from M-Pesa. .* MIT Press.

Mas. (2010). *Mobile money: The economics of financial inclusion.* World Bank Publications. doi:https://doi.org/10.2139/ssrn.1801742

Masaka. (2022). *Addressing challenges in accessing finance by small and medium enterprises (SMES) in Zambia: a pragmatic approach.* Lusaka: The University of Zambia. doi:https://doi.org/10.37945/cbr.2022.05.06

Mazambani, L., & Juliet Rushwaya, T. (2018). Financial inclusion: Disrupted liquidity and redundancy of mobile money agents in Zimbabwe. *Investment Management and Financial Innovations*, 131-142. doi:https://doi.org/10.21511/imfi.15(3).2018.11

Mazzarol, T. (2014). Research review: A review of the latest research in the field of small business and entrepreneurship: Financial management in SMEs. *Small Enterprise Research*, , 21(1), 2-13.

Mbewe, L. (2022). The impact of mobile money services on the growth of small and medium-sized enterprises (SMEs) in Zambia: A longitudinal study. *Journal of African Business, 23*(1), 67-91.

Mbiti, I., & Weil, D. (2011). *Mobile Banking: The Impact of M-PESA in Kenya. National Bureau.* National Bureau of Economic Research. doi:https://doi.org/10.3386/w17129

Mbiti, I., & Weil, P. (2014). *Mobile banking: The impact of M-Pesa in Kenya.* FinTech Africa.

Morawczynski, O. (2009). Designing mobile money services: Lessions from M-PESA. doi:https://doi.org/10.2139/ssrn.1552753

Morina, D., & Gashi, P. (2016). The role of SMEs on the economic development: Kosova's case. Available at SSRN 2820980. Available at SSRN 2820980.

Motta, V. (2018). *Mobile money use and financial inlusion for SME entrepreneurs in East Africa.* Egepe. doi:https://doi.org/10.17648/egepe-2018-83545

Mugenda, M. (2003). *Quantitative & Qualitative approaches. s.l.:.* Nairobi: Nairobi Acts Press. .

Muiruri, S. M. (2017). African small and medium enterprises (SMEs): Contributions, challenges and solutions. *Eur. J. Res. Reflect. Management Science*, 5, 36–48.

Mulenga, S. (2022). The impact of mobile money services on the productivity of small and medium-sized enterprises (SMEs) in Zambia: A longitudinal study. *International Journal of Productivity and Performance Management, 71*(1), 17-36.

Musonda, G. (2022). The challenges and opportunities of mobile money services for small and medium-sized enterprises (SMEs) in Zambia. *Journal of Small Business and Enterprise Development, 29*(1), 20-35.

Must, B., & Ludewig, K. (2010). *Mobile Money: Cellphone banking in Developing countries*, 7, 27-33.

Must, B., & Ludewig, K. (2010). Mobile money: Cell Phone Banking in Developing countries. 7, 27-33.

Mutsonziwa, K., & Maposa, O. (2016). Mobile money-A catalyst for financial inclusion in developing economies: A case study of Zimbabwe using FinScope survey data. *International Journal of Financial Management, 6*(3), 45-56. doi:https://doi.org/10.21511/imfi.15(3).2018.11

Mwaba, M. (2019). *Unpublished Study on the Impact of Mobile Money Services on SMEs in Lusaka, Zambia.* doi:https://doi.org/10.47941/ijf.1400

Mwale, M., & Daka, P. (2015). The adoption and impact of mobile money services on small and medium-sized enterprises (SMEs) in Zambia. *International Journal of Business and Information Management, 4*(2), 55-64.

Mwape, C. (2022). The impact of mobile money services on the financial performance of small and medium-sized enterprises (SMEs) in Zambia. *International Journal of Entrepreneurial Behavior & Research, 28*(7), 1530-1552.

Mwila, K. A. (2020). An assessment of cyber attacks preparedness strategy for public and private sectors in Zambia . *Doctoral dissertation, The University of Zambia*.

Mwila, M., & Ngoyi, L. (2019). The use of ICT by SME's in Zambia rto access business information services and investment: barriers and drivers. *Journal of Global enterpreneurship research, 9*(1). doi:https://doi.org/10.1186/s40497-019-0145-7

Ndekwa, A. (2017). *Factors influencing adoption of mobile money services among small and medium enterprises (SMEs) in Tanzania: a case study of tourism sector (Doctoral dissertation, The Open University of Tanzania).* The Open University of Tanzania. doi:https://doi.org/10.22161/ijaems.4.3.3

Ngaruiya, B., Bosire, M., & Kamau, S. M. (2014). Effect of Mobile Money transactions on the financial performance of small and medium enterprises in Nakuru central business district. *Res. J. Finance. Account*, 5, 53–58.

Ngwenya, V., & Mutambara, T. (2020). Mobile money services and financial inclusion: A case study of Zambia. *Journal of African Business, 21*(1), 77-97.

Njele, C., & Phiri, J. (2021). Factors Affecting Usage of Mobile Money Services and Their Impact on Financial Inclusion: Case of Lusaka Province. *International Journal of Business and Management, 16*(7), 104-118. doi:doi.org/10.5539/ijbm.v16n7p104

Nyika, A. (2023). A role cryptocurrencies in shaping the future of mobile money services in Lusaka, Zambia. *International Journal of Finance, 8*(4), 19-49. doi:https://doi.org/10.47941/ijf.1400

Reddy, K., & Upadhyay, A. (2021). DIgital financial inclusion demand side vs supply side approach. *Interantional JOurnal of electronic finance, 10*(3), 191. doi:https://doi.org/10.1504/ijef.2021.10038668

Rogerson, C. (1990). Manageing urban growth in Lusaka, Zambia. *Development Southern Africa, 7*(2), 179-194. doi:https://doi.org/10.1080/03768359008439511

Sakala, N. (2021). *Mobile-money-transaction-volumes-swell-to-k105-6bn/. Lusaka: diggers.news/business/.* Lusaka: Diggers.

Shukla, S., Bisht, K., Tiwari, K., & Bashir, S. (2023). Comparative Study of the Global Data Economy. In Data Economy in the Digital Age. *Springer Nature Singapore.*, Shukla, S., Bisht, K., Tiwari, K., & Bashir, S. (2023). Comparative

Study of the Global Data Economy. In Data Economy in the Digital Age (pp. 63-86). Singapore: Springer Nature Singapore.

Silva. (2015). *Technology acceptance model: TAM. . Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behavior and Technology Adoption.* doi:https://doi.org/10.4018/978-1-4666-8156-9.ch013

Sinkala, N. N. (2023). Mobile Money and SME Growth: A Zambian Perspective. *Journal of Business and Strategic Management*, 8(7), 1–18. https://doi.org/10.47941/jbsm.1589.

SIwale, J., & Hapompwe, C. (2021). Analysis of the impact of financial illiteracy on SMEs growth in Lusaka's Centrak Business District, Zambia. *International Journal of Scientific and Research Publications (IJSRP), 11*(6), 124-130. doi:https://doi.org/10.29322/ijsrp.11.06.2021.p11417

Smith, J., & Jones, P. (2021). Mobile money and SME growth: A global perspective. *Journal of International Business Studies, 52*(1), 1-28.

Sthembiso, M. (2023). The effects of interest rates on the credit access for SMEs: A South African perspective. *Banks and Bank Systems., 18*(4), 140-148. doi:https://doi.org/10.21511/bbs.18(4).2023.13

Talom, F. S., & Tenge, R. K. (2019). The Impact of Mobile Money on the Financial Perfomance of SMEs in Douala, Cameroon. *Department of Entrepreneurship and Business Management, Faculty of Business and Management Sciences,*, 2-6.

Thabani, M., & Richard, E. (2020). Factors that affect tax compliance among small and meduim enterprises in Lusaka, Zambia. *Journal of Accounting, 3*(1), 1-14. doi:https://doi.org/10.47941/jacc.415

Tsokota, T., Chipfumbu, C., & Maseko, M. (2023). The dark side of Mobile Money Transfer: A case study of Zimbabwe.

Upadhyay, R. a. (2021). *DIgital financial inclusion demand side vs supply side approach. Interantional JOurnal of electronic finance, 10(3), 191.* Edward Elgar Publishing.

Waweru, E. W. (2017). Challenges of financial management affecting performance of small and medium enterprises in Nairobi. *Doctoral dissertation*.

White, A., & Smith, J. (2019). The impact of mobile money on SME growth: A regulatory perspective. . *Journal of Financial Intermediation.*

World Bank. (2014). *Global Findex Database 2014: Measuring Financial Inclusion around the World.* The World Bank.

World Bank. (2016). (2015). Consultative Group to Assist the Poorest. The World Bank Group A to Z 2016,. *https://doi.org/10.1596/978-1-4648-0484-7_consultative_group_to*, 24c–24c.

Zhang, Q., Li, Y., & Lim, W. (2016). Mobile payment and the growth of small businesses: Evidence from China. *Journal of International Business Studies, 47*(6), 1080-1096.

Zhang, W., Li, Y., & Zhou, Y. (2013). The impact of mobile money on the financial behavior of rural households in China: Evidence from a mobile money program. *Journal of Banking and Finance, 3*7(10), 1827-1839.

Zureck, A. (2015). Financial communicatoon in SMEs. *Financial communication in SMEs*, 23-35. doi:https://doi.org/10.1007/978-3-658-07487-6_3

Additional References

Adeboye, E.O. (2024). Strengthening fraud prevention in small businesses: An analysis of effective accounting and auditing practices. *International Journal of Science and Research Archive*. doi: 10.30574/ijsra.2024.13.2.2160

Adedoyin, A. (2018). *Predicting fraud in mobile money transfer* (Doctoral dissertation, University of Brighton).

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., & Dwomoh-Okudzeto, Y. (2019). Control of fraud on mobile money services in Ghana: An exploratory study. *Journal of Money Laundering Control*, 22(2), 300-317.

Annan, F. (2017). Fraud on mobile financial markets: Evidence from a pilot audit study. *Available at SSRN 3049376*.

Botchey, F. E., Qin, Z., & Hughes-Lartey, K. (2020). Mobile money fraud prediction—a cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and naïve Bayes algorithms. *Information*, 11(8), 383.

Chale, P. R., & Mbamba, U. O. (2014). The Role of Mobile Money Services on Growth of Small and Medium Enterprises in Tanzania.

Fianu, E., Arku, Z., & Boateng, S. (2023). Determinants of Mobile Money Fraud on C2C E-Commerce: A Trust Perspective. In *Exploring the Dark Side of FinTech and Implications of Monetary Policy* (pp. 93-117). IGI Global.

Franco, G.S. (2023). Mobile Money Frauds in the African Continent. *Advances in Finance, Accounting, and Economics Book Series*, 344-360. doi: 10.4018/978-1-6684-5007-9.ch01

Lambongang, J.M. (2023). Investigating Challenges of Mobile Money Usage in the Central Business District of the Kumasi Metropolitan Assembly, Adum-Ghana. *South American Journal of Management*. doi: 10.21522/tijmg.2015.09.01.art004

Lokanan, M. E. (2023). Predicting mobile money transaction fraud using machine learning algorithms. *Applied AI Letters*, 4(2), e85. doi: 10.22541/au.168172408.81196220/v1

Mvogo, G., Ndzana, M., & Bidiasse, H. (2023). The determinants of the adoption of mobile money by small enterprises (SEs) in Douala, Cameroon. *African Journal of Science, Technology, Innovation and Development*, 15(3), 287-299.

Ngaruiya, B. (2014). Effects of mobile money transactions on financial performance of small and medium enterprises in Nakuru central business district. *Doctoral dissertation, Egerton University*.

Njoya, A. N., Ngongag, V. L. T., Tchakounté, F., Atemkeng, M., & Fachkha, C. (2023). Characterizing Mobile Money Phishfing Using Reinforcement Learning. *IEEE Access.*

Rahayu, S. (2015). The influence of mobile banking transaction used on cost reduction of SMEs employers. In *International Conference on Economics and Banking (ICEB-15)* (pp. 88-92). Atlantis Press.

Razaq, L., Ahmad, T., Ibtasam, S., Ramzan, U., & Mare, S. (2021). "We Even Borrowed Money From Our Neighbor": Understanding Mobile-based Frauds Through Victims' Experiences. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1), 1-30.

Salim, A. M. (2022). Assessment of Mobile Money Transaction Frauds and Consequences Confronting Zanzibar Telecom Service Providers. *Asian Journal of Economics, Business and Accounting.* doi:10.9734/ajeba/2022/v22i2030671

Simate, Z. (2013). Evaluation of mobile network security. In *2013 Pan African International Conference on Information Science, Computing and Telecommunications (PACT)* (pp. 170-175). IEEE.

Sumbwanyambe, M. (2023). A Review of the Role of Risk Management in Online Transactions: The Growing Issues of Network and System Security among Zambia's Financial Institutions. *American Journal of Finance*. doi: 10.47672/ajf.1510

Talom, F. S. G., & Tengeh, R. K. (2019). The impact of mobile money on the financial performance of the SMEs in Douala, Cameroon. *Sustainability*, 12(1), 183.

Tengeh, R. K., & Gahapa Talom, F. S. (2020). Mobile money as a sustainable alternative for SMEs in less developed financial markets. *Journal of Open Innovation: Technology, Market, and Complexity*, 6(4), 163. doi: 10.3390/JOITMC6040163

Viviers, S., & Venter, D. (2008). Fraud: An SMME perspective. *The Southern African Journal of Entrepreneurship and Small Business Management*, 1(1), 51-65.

Zimba, A., Mukupa, G., & Chama, V. (2022). Emerging Mobile Phone-based Social Engineering Cyberattacks in the Zambian ICT Sector. doi: 10.48550/arxiv.2212.13721

APPENDICES

Research Questionnaire on "Investigating the extent to which Mobile Money Fraud Contributes to the Performance of MSEs in Lusaka, Zambia."

This research is only for academic purposes in partial fulfilment of the requirements for the award of a Master of Business in Finance. You are encouraged to give your views freely and accurately. The information/ responses provided by you in this questionnaire will only be for academic purposes and will be kept confidential; no names of forms or individuals will be mentioned in any report to ensure no one is harmed. Your cooperation will be appreciated. Please direct any queries to Email: essymbewe@gmail.com

Instruction: Please indicate your responses by ticking (√) the appropriate box. Provide brief and concise comments where required.

Section 1: General Information

1. **Business Name:** _____
2. **Business Type (**Select One**):**
    - Transport
    - Restaurant
    - Barbershop/Salon
    - Retail
    - Other (please specify): _____
3. **How long has your business been operating?**
    - Less than 1 year
    - 1-3 years
    - 4-5 years
    - More than 5 years
4. **Do you use mobile money services for your business transactions?**
    - Yes

- No

5. **How many employees does your business have?**
    - Less than 5
    - 5- 10
    - More than 10
6. **What is your average monthly revenue?**
    - Less than ZMW 10, 000 Less than ZMK 10,000
    - ZMW 10,000 – ZMW 50,000
    - ZMW 50,000 – ZMW 100,000
    - More than ZMW 100,000

Section2: Experience with Mobile Money Fraud

7. **Have you or your business ever encountered mobile money fraud**
    - Yes
    - No (If no, skip to Section3)
8. **What types of mobile money fraud have you encountered? (Select all that apply)**
    - Vishing/Smishing (fraudulent messages to steal login credentials)
    - Advance fee scam
    - Reversal request
    - False transaction
    - Other (please specify)
9. **How frequently have you encountered mobile money fraud in the past year?**
    - Very frequently (once a month or more)
    - Occasionally (every few months))

- Rarely (once or twice a year)
- Never

10. **What was your initial response when you first sicovered mobile money fraud? (Select all that apply)**
    - Reported t to mobile money service provider Reported it to mobile money service provider
    - Stopped using mobile money for a period
    - Tightened security measure
    - Too no action
    - Other (please specify): _____

11. **On average, how much money has your business lost due to mobile money fraud in the past year?**

- Less than ZMW 1,000
- ZMW 1000- ZMW 5,000
- ZMW 5000 – ZMW 10,000
- More than ZMW 10, 000

Section3: Impact on Business Performance

12. **How has mobile money fraud affected your business operations? (Select all that apply)**

- Financial loss
- Reduced customer trust
- Increased operational costs
- Loss of business opportunities
- Decreased profitability
- Reputational Damage

- Other (please specify): _____

13. **Has mobile money fraud caused you to change your business practices? Has mobile money fraud caused you to change your business practices?**

- Yes (please specify changes made): _____
- No

14. **Has mobile money fraud caused interruptions in daily business operations?**

- Yes
- No

15. **Do you think mobile money fraud has affected the long-term sustainability of your business? Do you think mobile money fraud has affected the long-term sustainability of your business?**

- Yes
- No
- Not sure

Section 4: Preventive Measures

16. **What steps have you taken to prevent mobile money fraud in your business? (Select all that apply)**

- Educated employees and customers about fraud risks
- Implemented additional security measures (E.g. two-factor authentication)
- Regularly monitor transactions for unusual activity
- Changed mobile money service providers
- Used a more secure payment platform
- Other (please specify): _____

17. **How effective do you find the preventive measures you have taken?**

- Very effective

- Moderately effective
- Slightly effective
- Not effective

18. **What challenges have you encountered in implanting preventive measures? (Select all that apply)**

- High costs
- Lack of access to secure technology
- Employees resistance
- Insufficient fraud prevention knowledge
- Other (please specify): _____

19. **Do you provide any training for employees on digital literacy and fraud prevention?**

- Yes
- No

20. **What do you believe money mobile service providers can do to reduce fraud? (select all that apply)**

- Improve customer education and awareness
- Strengthen verification procedures (E.g two-factor authentication)
- Monitor and flag suspicious transactions
- Offer more secure payment methods
- Other (please specify): _____

21. **What should regulatory institutions do to ensure mobile money fraud is mitigated?**

- _____
- _____

- _____

22. **What additional preventive measure would you recommend to safeguard SMEs against mobile money fraud?**

- _____
- _____
- _____

Section 5: Conclusion

23. **Rank the following types of mobile money fraud based on perceived risk or impact (1= Highest risk; 5= Lowest risk):**

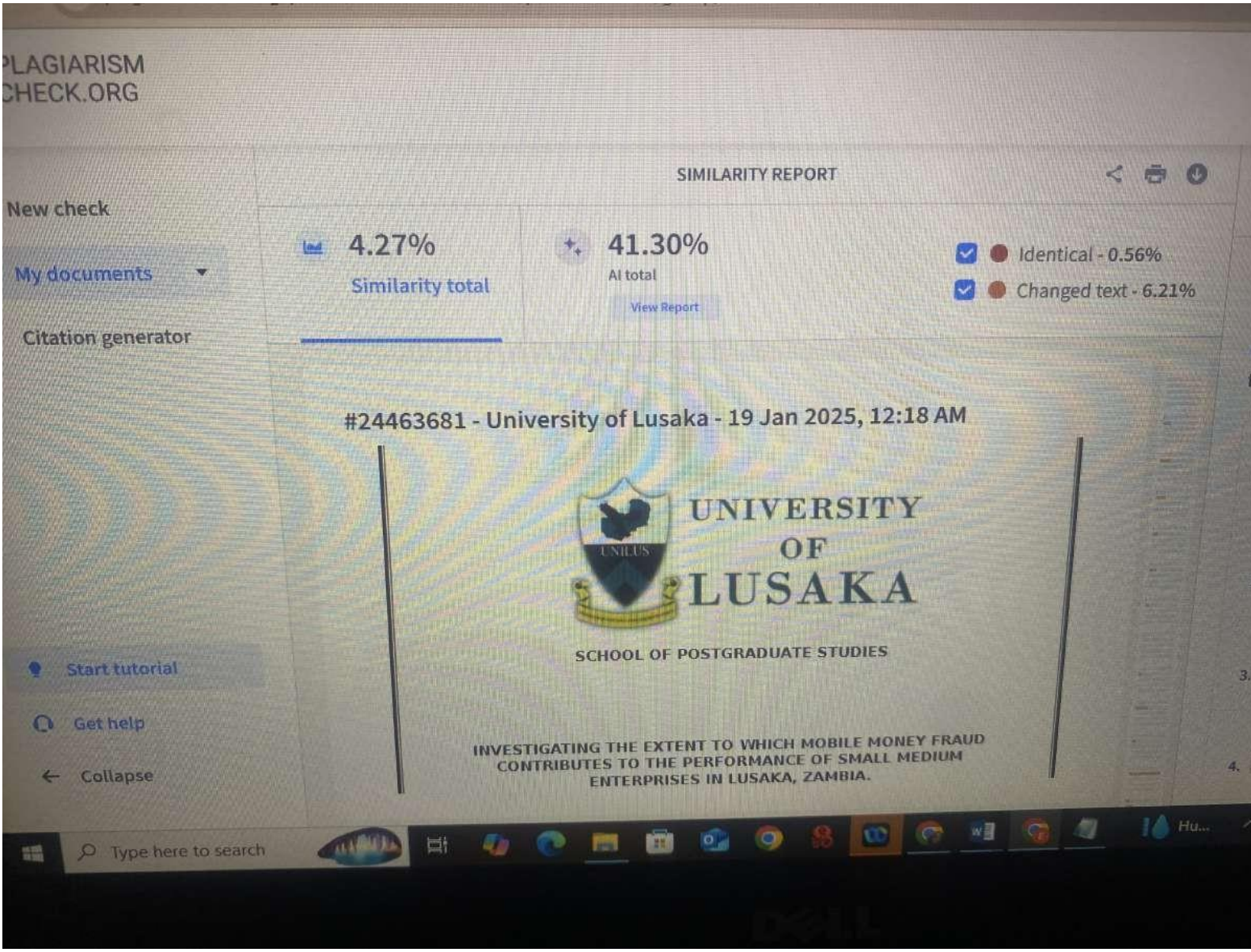
- Vising? Smishing
- Advance fee scam
- Reversal request
- False transactions
- Other (please specify): _____

24. **Do you believe mobile money fraud is a significant challenge for SMEs in Lusaka??**

- Yes
- No

25. **Any additional comments or suggestions on how to address mobile money fraud for SMEs?**

- _____
- _____
- _____


PLAGIARISM CHECK.ORG
SIMILARITY REPORT
New check
My documents
Citation generator
4.27%
Similarity total
41.30%
AI total
View Report
Identical - 0.56%
Changed text - 6.21%
#24463681 - University of Lusaka - 19 Jan 2025, 12:18 AM
UNIVERSITY OF LUSAKA
SCHOOL OF POSTGRADUATE STUDIES
INVESTIGATING THE EXTENT TO WHICH MOBILE MONEY FRAUD CONTRIBUTES TO THE PERFORMANCE OF SMALL MEDIUM ENTERPRISES IN LUSAKA, ZAMBIA.
Start tutorial
Get help
Collapse
Type here to search