

**The risk management and fraud control in mobile money services post COVID-19 in
Uganda: A case study on Kampala District**

Rosemary Marion Ndyemanya

S20B33/028

**A DISSERTATION SUBMITTED TO THE SCHOOL OF BUSINESS IN PARTIAL
FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF A BACHELORS
DEGREE IN SCIENCE OF ACCOUNTING AND FINANCE OF UGANDA CHRISTIAN
UNIVERSITY MUKONO.**

September, 2023




**UGANDA CHRISTIAN
UNIVERSITY**

A Centre of Excellence in the Heart of Africa

DECLARATION

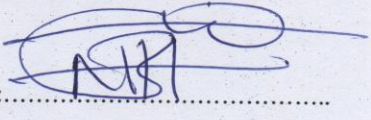
I, Ndyemanya Rosemary Marion, declare that this research report is entirely my own original work, except where acknowledged and that this work has never been submitted before to any University or Institution of higher learning for the award of a degree or certificate or for other academic purposes.

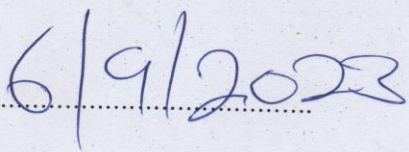
Signature:.......... Date:.....6/9/2023.....

NDYEMANYA ROSEMARY MARION

APPROVAL

This research report was conducted under my supervision and has been submitted for examination with my approval.

Signature: .....

Date: .....

MR. KATSME NICSON
(Supervisor)

DEDICATION

With deep respect and heartfelt gratitude, I dedicate this research dissertation to my cherished parents. Their love, care, invaluable advice, fervent prayers, and steadfast support have been my foundation since the day I came into this world. May their lives be abundantly blessed.

I also extend my profound thanks to my siblings and friends, as well as my esteemed lecturers, whose support, courage, and constant motivation have been a driving force throughout my academic journey.

Furthermore, I dedicate this report to my dedicated research supervisor, Mr. Katsme Nicson. His sage guidance, invaluable advice, and unwavering attention have been instrumental in helping me reach this pivotal milestone.

ACKNOWLEDGEMENT

I would like to extend my heartfelt gratitude to several individuals whose invaluable assistance and contributions were instrumental in making this study a reality.

First and foremost, I am deeply appreciative of my dedicated supervisor, whose unwavering encouragement and guidance were instrumental throughout the duration of this study. His expertise and support were truly indispensable.

I am equally indebted to my esteemed lecturers for the wealth of knowledge they imparted during my time at the institution. Their teachings have enriched my understanding, and I feel significantly more informed than when I first joined.

I would also like to express my profound appreciation to my friends, the diligent library staff, and my colleagues at the University. Your unwavering support, both in terms of moral encouragement and material assistance, has been nothing short of remarkable. May this spirit of camaraderie continue to flourish, and may you all be blessed abundantly.

Once again, my sincere thanks go out to all who played a part in this journey. Your contributions have left an indelible mark on this study, and I am deeply grateful for your involvement.

TABLE OF CONTENTS

DECLARATION	i
APPROVAL	ii
DEDICATION	iii
ACKNOWLEDGEMENT	iv
LIST OF TABLES	viii
LIST OF FIGURES	ix
ABSTRACT.....	x
CHAPTER ONE	1
1.1. Background.....	1
1.2. Statement of the Problem.....	2
1.3. Main Objective of the Study	3
1.4. Specific Objective of the Study	3
1.5. Research Questions	4
1.6 Scope of the Study.	4
1.6.1 Time Scope	4
1.6.2 Geographical Scope	4
1.6.3 Subject Scope.....	5
1.7 Justification of the study	5
1.8. Conceptual Framework.....	7
CHAPTER TWO: LITERATURE REVIEW	8
2.0 Introduction.....	8
2.1 Definitions of the Key Terms.....	8
2.1.1 Mobile Financial Services.....	8
2.1.2 Risk management.....	8
2.1.3 Fraud	8
2.1.4 Fraud Control	8
2.2 The relationship between customer verification and fraud control in the study context.	9
2.3. The relationship between password strength and fraud control in the study context.....	11
2.4 The relationship between audit checks of mobile money accounts and fraud control in the study context.....	13
2.5 Conclusion of Literature.	15
CHAPTER THREE: METHODOLOGY	16
3.0 Introduction.....	16

3.1 Research design	16
3.2 Study Area	16
3.3 Study Population.....	16
3.4 Sample Size.....	17
3.5 Sampling Technique	18
3.6 Sources of Data.....	18
3.6.1 Primary Data.....	18
3.6.2 Secondary Data.....	18
3.7 Data Collection methods.....	18
3.7.1 Questionnaire method.....	18
3.8 Data Collection Instruments.....	19
3.8.1 Questionnaire	19
3.9 Data quality control.....	19
3.9.1 Validity	19
3.9.2 Reliability.....	20
3.10 Ethical considerations	20
3.11 Limitations of the study.	20
CHAPTER FOUR.....	21
PRESENTATIONS, ANALYSIS AND INTERPRETATION OF FINDINGS.....	21
4.1 Findings of the study.....	21
4.1.1 Response rate	21
4.2 Demographic findings of the study.....	22
4.2.1 Gender of respondents	22
4.2.2 Marital status of respondents	22
4.2.3 Age group of respondents	23
4.2.4 Education level of respondents	23
4.2.5 Time spent by respondents in Mobile money services usage.	24
4.3 Findings on the relationship between customer verification and fraud control	25
4.5 Findings on the relationship between Audit Checks and fraud control	29
4.6 Correlation between risk management and fraud control in Mobile Money Services.....	31
CHAPTER FIVE	32
DISCUSSION OF FINDINGS, CONCLUSION AND RECOMMENDATIONS	32
5.1 Introduction.....	32

5.2 Discussion of findings.....	32
5.2.1 The relationship between customer verification and fraud control.....	32
5.2.2 The relationship between password strength and fraud control.....	32
5.2.3 The relationship between audit checks and fraud control.....	33
5.3 Conclusion	33
5.4 Recommendations.....	34
5.5 Areas of further research.....	34
References.....	35
APPENDIX I: QUESTIONNAIRE	40
APPENDIX II: INTRODUCTORY LETTER FOR DATA COLLECTION.....	43

LIST OF TABLES

Table 1: Response Rate.....	21
Table 2: Gender of respondents.	22
Table 3: Respondents' marital status	22
Table 4: Respondents' age group.....	23
Table 5: Respondents education level.....	23
Table 6: Time spent using mobile Money services	24
Table 7: Table showing findings on the relationship between customer verification and fraud control.	25
Table 8: Table showing findings on the relationship between password strength and fraud control.	27
Table 9: Table showing findings on the relationship between Audit checks and fraud control. ..	29
Table 10: Correlation table of Risk management and Fraud control.....	31

LIST OF FIGURES

Figure 1: Krejcie and Morgan table 17

ABSTRACT

The research delved into a comprehensive exploration of risk management and fraud control within the context of post-Covid-19 mobile money services, focusing its investigation on Kampala District as a representative case study. This inquiry was guided by three core objectives: firstly, to examine the relationship between customer verification and fraud control in the study context; secondly, to examine the relationship between password strength and fraud control in the study context; and thirdly, to examine the relationship between audit checks of mobile money accounts and fraud control in the study context; Employing a case study design and adopting a purely quantitative methodology, data was collected from 40 respondents through structured questionnaires. The collected data underwent meticulous analysis using descriptive statistics.

The study uncovered a noteworthy discovery, a substantial weakness in the connection between mobile money services and robust risk management. This discovery underscores a critical issue: a substantial number of customers remain dissatisfied with the existing security measures, emphasizing the pressing demand for a more secure money transfer and payment platform. To address these concerns effectively, the study puts forward a series of recommendations. Firstly, it advocates for a tailored approach to customer verification processes that align with specific user demographics and transaction volumes. Secondly, it emphasizes the imperative for all mobile money service providers to fully comply with international regulatory frameworks governing fraud control and risk management. Finally, the study underscores the significance of conducting regular audits, a practice beneficial to both service providers and users alike. Such audits help in continually assessing the effectiveness of fraud prevention strategies and allow for necessary adjustments to maintain a consistently high level of security and risk management practices.

In summation, this research provides valuable insights into the challenges faced by mobile money services in the post-Covid-19 landscape, specifically concerning fraud control and risk management. The study's findings highlight the imperative of proactive measures, personalized solutions, regulatory compliance, and regular audits as essential components in enhancing the security and reliability of mobile money platforms. By implementing these measures, the industry can meet the evolving demands of users while assuring their financial security throughout all transactional activities.

CHAPTER ONE

1.0 Introduction

This chapter begins by introducing the research topic and its significance in the context of the mobile money industry's growth and impact in Uganda. It outlines the specific objectives of the study and establishes the structure of the proposal.

1.1. Background

Mobile Financial Service (MFS) is a service that allows users to transfer money using their mobile phones, and it has become an increasingly popular financial service in many developing countries. Mobile Financial Service offers a convenient and secure way of conducting financial transactions, especially in areas where traditional banking services are limited. Through increased accessibility and decreased transaction costs, they provide tremendous prospects for enhancing the effectiveness of financial services. The quick adoption of these services by the general population in several nations, including the Philippines, Brazil, India, Uganda, and Kenya, has shown that the technology is advanced and provides genuine benefits to those who previously did not have access to financial goods or services. (Lake, 2013). In November 2012, International Financial Corporations formally accepted MFS as a key component of its Access to Finance activities after seeing the potential of leveraging it as a tool to promote financial inclusion. (Lake, 2013)

An article published by Petroc Taylor, affirmed that with the general increase from the first quarter of 2017 to the first quarter of 2022, Uganda's mobile financial service subscriptions increased to just over 33 million in the first quarter of 2022, which is the highest number of registered mobile money subscriptions ever recorded in Uganda. (Taylor, 2023). However, the growth of mobile money has also led to an increase in fraudulent activities, which pose a significant risk to both mobile money businesses and their customers.

According to Mobile Worldwide News, The Uganda Communication Commission urged consumers to be cautious of criminals who were attempting to scam people out of funds using mobile money platforms. They had recorded an increase in such cases during the Covid-19 (corona virus) outbreak. The regulator outlined security advice for subscribers after noticing the

circulation of fake promotions and instances where fraudsters pretended to be employees of mobile operators to obtain account details. (Donkin, 2020)

Various fraudulent schemes were being circulated, including efforts to convince users to disclose or enter their PIN numbers, which were then used for fraudulent transactions. "These scams had resulted in significant financial losses for unsuspecting subscribers, especially during the COVID-19 lockdown when subscribers increasingly relied on digital financial platforms due to limited mobility and their desperation to maintain connectivity," they had added. Uganda, like other countries, had supported reductions in operator fees to encourage the use of mobile financial services during the ongoing global public health crisis. This move aimed to reduce the need for in-person transactions and the exchange of physical cash. (Donkin, 2020)

Several studies have investigated mobile money fraud and risk management in different countries, including Uganda. For example, Mugume and Turyakira (2020) investigated the relationship between mobile financial service fraud and financial inclusion in Uganda. However, since Mobile financial service transfer is a technology-based advancement that has brought about beneficial effects on the inclusion of financially disadvantaged individuals while also aiding central banks in terms of regulation, it is unclear on why the current available risk management strategies on fraud have been barely effective post Covid.

Therefore, due to the lack of clarity regarding the limited success of the existing risk management and fraud control measures in handling fraudulent activities in mobile money businesses, this research aims to enhance the knowledge in the field of mobile money by investigating the current strategies employed to combat fraud in mobile money services after the Covid pandemic in the study context.

1.2. Statement of the Problem

Mobile financial services (MFS) have the potential to contribute to poverty reduction by enhancing individuals' income-earning capabilities. Over the past years, these services have emerged as the primary means of financial inclusion for millions of individuals, particularly in low-income countries like Uganda. In 2019, the number of registered mobile money accounts surpassed one billion, with digital transactions surpassing traditional cash transactions for the first time. (Matthew Bird, n.d.)

With the global spread of the corona virus, businesses and governments faced the challenge of limiting cash exchanges, which were identified as potential sources of virus transmission by the World Health Organization. (Berger, 2020) This circumstance fueled a significant surge in the adoption of mobile money services within the economy. However, alongside this growth, mobile financial services have also become vulnerable to fraudulent activities, particularly those targeting consumers. Such fraudulent incidents pose a considerable risk to the usage of mobile money services by vulnerable segments of the population and have resulted in substantial economic losses for service providers. (Matthew Bird, n.d.)

Although companies have implemented certain measures like user verification to combat fraud and related crimes, there is a pressing need for more comprehensive data and evidence to investigate, develop and implement effective strategies against financial criminal activities in the mobile financial service sector.

1.3. Main Objective of the Study

The main objective of the study is to enhance the understanding of mobile financial services by examining the current strategies associated with fraud control in the post-Covid era of the study context. By conducting a comprehensive analysis, the study aims to contribute to the existing literature on mobile financial services and provide valuable insights into effective measures that can be implemented to combat risk and fraud in the mobile service sector. Ultimately, the research seeks to promote the development and implementation of robust and efficient strategies that safeguard users and service providers against fraudulent activities in the evolving landscape of mobile financial services.

1.4. Specific Objective of the Study

The specific objectives of this study are:

- i. To examine the relationship between customer verification and fraud control in the study context.
- ii. To examine the relationship between the password strength and fraud control in the study context.

- iii. To examine the relationship between audits checks of mobile money accounts and fraud control in the study context.

1.5. Research Questions

The research questions for this study are:

- i. What is the relationship between customer verification and fraud control in the study context?
- ii. What is the relationship between the password strength and fraud control in the study context?
- iii. What is the relationship between audits checks of mobile money accounts and fraud control in the study context?

1.6 Scope of the Study.

1.6.1 Time Scope

This study aims to analyze fraud control strategies in mobile money services over an extended period beyond the immediate post-Covid era. It seeks to understand how the mobile money sector has adapted and responded to the challenges posed by the pandemic and its aftermath (Berger, 2020). By considering a broader timeframe, the study aims to capture the long-term effects, trends, and evolving nature of fraud control practices in this sector. It also aims to identify variations in fraud patterns, emerging trends, and assess the effectiveness of different strategies over time. This research contributes to the development of more robust and adaptable fraud control measures in the evolving landscape of mobile money services.

1.6.2 Geographical Scope

This study concentrates on Kampala district, the capital city of Uganda, due to its significant concentration of mobile financial services. This geographical area serves as a crucial hub for mobile money activities, hosting numerous service providers. (News, 2016). By focusing on Kampala district, the research delves deeply into the dynamics, challenges, and opportunities surrounding fraud control in mobile money services. This targeted approach allows for a comprehensive analysis of strategies used by providers, the prevalence of fraud incidents, and

user experiences in a context where mobile financial services are highly accessible and widely utilized.

Narrowing down the scope to Kampala district facilitates a more profound understanding of the local regulatory framework, market conditions, and socioeconomic factors influencing the effectiveness of fraud control measures in mobile money services. The localized perspective gained from this study offers valuable insights that can inform policy recommendations, industry best practices, and customized approaches to combat fraud not only in Kampala but also in other similar urban areas or regions with a high concentration of mobile money activities. (Berger, 2020)

1.6.3 Subject Scope

This study focuses on mobile financial services and specifically centers on the control of fraud within this domain. Mobile money services involve using mobile phones or digital devices for financial transactions like money transfers and payments (Mobile Financial Services, 2019). The research delves into the strategies employed by service providers, regulatory bodies, and other stakeholders to detect, prevent, and mitigate fraudulent activities in the mobile money sector. It aims to identify vulnerabilities, particularly consumer-oriented frauds, and assess the economic impact of fraud on different user segments and mobile money service providers.

Moreover, the study encompasses an examination of regulatory frameworks, industry guidelines, and technological advancements that contribute to fraud control efforts in mobile money services. By exploring these aspects, the research sheds light on the dynamic landscape of mobile financial services and emphasizes the importance of effective measures to ensure the security and trustworthiness of these services for both users and providers.

1.7 Justification of the study

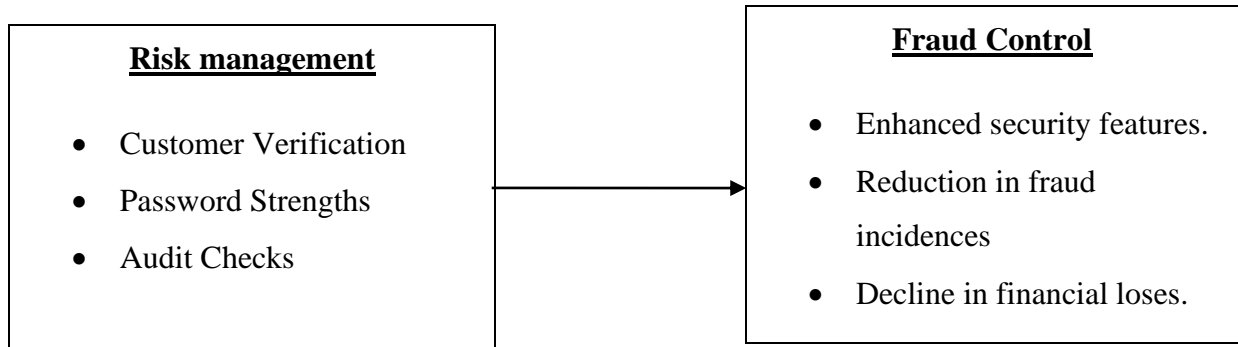
The justification for the research study lies in the need to address the significant issue of fraud in mobile financial services, particularly in the post-Covid era. Mobile financial services have become vital for financial inclusion, especially in low-income countries like Uganda. However, the rapid growth of mobile money has also led to an increase in fraud and criminal activities, posing risks to both service providers and users. (PYMNTS, 2020)

Fraud in mobile money services has severe consequences, including economic losses for providers and a decline in consumer confidence and trust. Vulnerable populations, who heavily rely on mobile money, are disproportionately affected. (Berger, 2020). The study aims to mitigate these risks and protect users by understanding the current strategies employed for fraud control.

While measures have been implemented to combat fraud, there is still a lack of comprehensive understanding regarding their effectiveness. The study seeks to fill this knowledge gap by providing empirical evidence, data, and insights into the effectiveness of fraud control strategies in the mobile money sector. This will inform the development of targeted and evidence-based measures to combat fraud and enhance the security of mobile money services.

The Covid-19 pandemic has presented unique challenges and opportunities for the mobile money sector. As businesses and governments limited cash exchanges, mobile money services experienced significant growth. (Berger, 2020). However, this growth also brought new risks and vulnerabilities. Understanding how fraud control strategies have evolved in response to the pandemic and its aftermath is crucial for adapting to the changing landscape and ensuring the security of mobile money services. By addressing these justifications, the research study aims to contribute to the mobile money literature, provide valuable insights, inform policy recommendations, and assist service providers and regulators in developing robust fraud control measures.

1.8. Conceptual Framework



Source: Adopted and Modified from Mobile Financial Services. (2019). In H. K. Aijaz A. Shaikh, Marketing and Mobile Financial Service

The conceptual framework centers around the independent variable of risk management, specifically examining customer verification, password strength, and audit checks as factors that contribute to fraud control in mobile money businesses. The dependent variable is fraud control, which refers to the effectiveness of measures implemented to prevent, detect, and mitigate fraudulent activities.(Times, 2023). The indicators used to assess the control of fraud include enhanced security features, reduction in fraud incidences, and financial losses.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter aims to provide clear and concise definitions of the key terms, namely risk management and fraud control, ensuring a shared understanding of their meanings within the study. Additionally, it explains the specific objectives of the research, which involve exploring the strategies and measures associated with fraud control in mobile financial services in the aftermath of the Covid-19 pandemic.

2.1 Definitions of the Key Terms

2.1.1 Mobile Financial Services

Mobile financial services (MFS) refer to a broad range of digital devices, channels, and financial transactions that consumers execute on their mobile phones or tablets. (Mobile Financial Services, 2019)

2.1.2 Risk management

Risk management is the process of identifying, analyzing, evaluating, and managing potential risks to minimize their negative impact on a business or service. It includes the conduct of a risk assessment, implementation of a risk mitigation strategy, and continuous monitoring of the security state of an information system. (N-ABLE, n.d.)

2.1.3 Fraud

Fraud is a misleading conduct done by someone, with the objective to get an illegal advantage or to harm someone else's (victim's) rights (Times, 2023)

2.1.4 Fraud Control

Fraud control refers to the measures and strategies implemented to detect, prevent, and mitigate fraudulent activities. It encompasses the processes, policies, and technologies put in place to safeguard individuals, organizations, and systems from deceptive practices aimed at gaining unlawful benefits or causing harm to others' rights and interests. (Times, 2023)

2.2 The relationship between customer verification and fraud control in the study context.

Customer verification is a process that is used by businesses with online products, services, or content to ensure that the information provided by their customers is correct and that the customers are who they say they are. (Konfirmi, n.d.).It is a critical aspect of risk and fraud control in mobile money businesses that involves the process of confirming the identity and legitimacy of customers who use mobile money services. By verifying the identity of users, mobile money providers can significantly reduce the risk of fraudulent activities, protect customers from unauthorized access to their accounts, and enhance the overall security of the system.

Hadijah, et al. (2018) provides an extensive overview of the risks faced by mobile money businesses and emphasizes the pivotal role of customer verification in mitigating fraud. Their research highlights the importance of a robust customer on boarding process, incorporating identity verification, and Know Your Customer (KYC) procedures. The authors argue that comprehensive verification measures can establish a strong foundation for fraud control and risk management in the mobile money sector. Among these measures include Biometric authentication as it has emerged as a promising method to enhance customer verification and combat fraud. Singh and Gupta (2019) investigate the implementation of biometric verification in mobile money systems and its impact on fraud prevention. Their findings reveal that biometric-based customer authentication significantly reduces the occurrence of identity theft and fraudulent transactions, offering mobile money businesses a secure and efficient means of verifying their customers.

It is crucial to ensure a smooth user experience while maintaining robust security in mobile money businesses. Liang and Lu (2020) delve into the importance of striking this equilibrium by analyzing different customer verification methods. Their study sheds light on how user-friendly verification processes, such as two-factor authentication (2FA) and device recognition, positively influence customer satisfaction while concurrently fortifying fraud control mechanisms. Additionally, Machine learning and artificial intelligence (AI) technologies have demonstrated immense potential in fraud detection. Chen and Wang (2019) explore the integration of AI-based algorithms in mobile money platforms to enhance customer verification and fraud control. Their research suggests that these intelligent systems can efficiently analyze vast amounts of data, enabling real-time fraud detection and proactive risk management in mobile money businesses.

Also, Machine learning and artificial intelligence (AI) technologies have demonstrated immense potential in fraud detection. Chen and Wang (2019) explore the integration of AI-based algorithms in mobile money platforms to enhance customer verification and fraud control. Their research suggests that these intelligent systems can efficiently analyze vast amounts of data, enabling real-time fraud detection and proactive risk management in mobile money businesses. Correspondingly, Chen et al. (2018) investigates the effectiveness of transaction monitoring systems in detecting fraudulent patterns and how it complements customer verification efforts. Their research underscores that real-time transaction monitoring, coupled with robust customer verification, can proactively identify and mitigate fraud risks, thus safeguarding the integrity of mobile money operations.

Nevertheless, effective fraud control and risk management in mobile money businesses often depend on compliance with regulatory frameworks. Samuels and Jenkins (2021) assess the regulatory landscape surrounding customer verification in the mobile money sector. Their study emphasizes the need for mobile money businesses to stay updated with evolving regulations to ensure the adequacy and legality of their customer verification procedures, consequently minimizing potential fraud risks.

In order to determine the most effective customer verification approach, Chen et al. (2022) conduct a comparative analysis of various verification methods, including biometrics, SMS-based authentication, and knowledge-based questions. Their study evaluates the strengths and weaknesses of each method in terms of fraud control and user experience. The research sheds light on the significance of tailoring verification processes to suit specific user demographics and transaction volumes, contributing to better risk management outcomes. As the landscape of mobile money businesses continues to evolve, new challenges and opportunities in customer verification and fraud control emerge. Ahmed et al. (2022) presents an analysis of current challenges faced by mobile money operators and propose potential future directions in the field of risk management. The paper discusses emerging technologies, regulatory developments, and the need for collaboration among stakeholders to stay ahead in the battle against fraud.

2.3. The relationship between password strength and fraud control in the study context.

Password strength is a critical aspect of cyber security and data protection that refers to the measure of how resilient a password is against various attempts to guess or crack it. A strong password is essential for securing online accounts, including those used in mobile money services, as it significantly reduces the risk of unauthorized access and potential fraud. (PassCamp, 2022)

A study conducted by Smith et al. (2018) investigates the significance of password strength in mobile money platforms. The research reveals that weak passwords are a common entry point for fraudsters attempting to gain unauthorized access to user accounts. By analyzing real-world data breaches, the study emphasizes that enforcing strong password policies, including complexity requirements and regular password updates, can significantly reduce the risk of fraudulent activities. Inclusively, Lee and Park (2019) delve into the effectiveness of two-factor authentication (2FA) in bolstering password security and controlling fraud. The research demonstrates that integrating 2FA, which requires users to provide an additional verification factor beyond their password (such as a one-time code sent to their mobile device), significantly reduces the likelihood of unauthorized access. By mitigating the risk of password-related fraud, 2FA emerges as a powerful tool for mobile money businesses in enhancing security.

Correspondingly, understanding user behavior and their password management practices is vital in comprehending password vulnerabilities. A study by Wang and Zhang (2020) explores user attitudes towards password security in the context of mobile money applications. The research uncovers that many users exhibit risky behaviors, such as reusing passwords across multiple platforms and employing easily guessable passwords. The findings highlight the importance of educating users on secure password practices as part of a comprehensive fraud control strategy. Also; Password managers have gained popularity as tools for simplifying password management while maintaining security. Guo and Li (2021) investigate the adoption of password managers among mobile money users and its impact on fraud control. The research showcases that password managers facilitate the use of unique and complex passwords, reducing the risk of

password-related fraud. Integrating password manager features into mobile money applications can prove beneficial in promoting secure password practices.

The usability of password systems in mobile money applications can influence users' willingness to adhere to secure password practices. Zhu and Wang (2021) investigate the trade-off between usability and password security in the context of mobile money services. Their research reveals that overly complex password requirements may lead to user frustration and result in the adoption of weaker passwords. The study suggests that mobile money businesses should strike a balance between usability and security, providing guidance and incentives for users to create strong passwords without compromising their overall experience. With biometric authentication, such as fingerprint or facial recognition, an alternative to traditional password-based systems is presented. Chang and Kim (2022) analyze the effectiveness of biometric authentication in mobile money businesses and its potential role in fraud control. The study highlights that biometric authentication offers a secure and convenient means of user verification, reducing the reliance on passwords and consequently minimizing password-related fraud risks.

Additionally, Password recovery mechanisms can inadvertently create potential entry points for fraudsters. A study by Li et al. (2019) examines password recovery practices in mobile money platforms and their susceptibility to social engineering attacks. The research highlights that weak password recovery processes, such as using easily accessible personal information, can lead to unauthorized account access. Mobile money businesses must implement secure and robust password recovery mechanisms to prevent fraudulent activities while providing legitimate access to users who have forgotten their passwords.

Nevertheless, understanding human factors in password management is crucial for developing effective fraud prevention strategies. Brown and Taylor (2021) conduct a comprehensive review of human behavior and its impact on password security. The research identifies cognitive biases, such as optimism bias and password fatigue, which can influence user decisions in password creation and management. By incorporating behavioral insights into password policies and education programs, mobile money businesses can empower users to make more secure choices, reducing the risk of fraudulent activities.

2.4 The relationship between audit checks of mobile money accounts and fraud control in the study context.

According to Francis Annan, Audit checks in the context of mobile money services refer to systematic and periodic reviews conducted to assess the security, compliance, and overall operational effectiveness of the mobile money platform. These audits are essential to identify potential vulnerabilities, gaps in security protocols, and compliance with industry standards and regulations. (Annan, 2017)

Parker et al. (2019) examines the role of audit checks in detecting and preventing fraud within mobile money businesses. The study emphasizes that periodic and rigorous audits play a crucial role in identifying unusual transactions, patterns, and discrepancies. By conducting regular audits, mobile money operators can quickly respond to emerging fraud threats and implement necessary preventive measures, bolstering their overall fraud control efforts. With the advancement of technology, auditing tools have evolved to meet the dynamic needs of mobile money businesses. Nguyen and Chen (2020) investigate the effectiveness of auditing technology in detecting fraudulent activities. Their research highlights that data analytics and AI-powered auditing tools can effectively analyze large volumes of transactional data, facilitating the early detection of potential frauds. The study suggests that integrating modern auditing technologies enhances the efficiency and accuracy of fraud control measures in mobile money platforms.

Mobile money businesses operate within a complex regulatory environment. Wang and Li (2022) explore the relationship between auditing regulatory compliance and fraud control in the mobile money sector. The study highlights that auditing compliance with regulatory standards ensures that fraud control measures align with industry best practices and legal requirements. By incorporating regulatory compliance audits into their risk management practices, mobile money operators can strengthen their fraud control mechanisms. Therefore, it is important to note that Internal and external audit checks offer complementary perspectives on fraud control in mobile money businesses. Chang and Park (2021) compare the effectiveness of internal audits, conducted by the organization's internal audit department, and external audits, performed by independent third-party auditors. Their research finds that combining both internal and external

audits provide a robust and independent assessment of fraud risks, leading to improved risk management strategies in mobile money services.

Mobile money businesses are also encouraged to adapt Real-time auditing. This is a proactive approach that involves continuous monitoring of transactions and activities to detect fraud in real-time. Wang et al. (2021) examine the impact of real-time auditing on fraud control in mobile money businesses. Their research highlights that real-time auditing enables immediate detection and response to fraudulent activities, reducing the potential losses associated with fraud incidents. By implementing real-time auditing systems, mobile money operators can significantly enhance their fraud control capabilities and swiftly mitigate risks.

Correspondingly, Mobile money agents play a crucial role in facilitating transactions on behalf of mobile money businesses. Zhang and Liu (2022) explore the relationship between audit checks and fraudulent activities among mobile money agents. The research reveals that regular audits of agent operations can identify internal collusion and fraudulent schemes. By conducting comprehensive agent audits, mobile money operators can deter potentially fraudulent activities and ensure the integrity of their agent networks. Also, unauthorized access to sensitive data and functionalities can lead to fraudulent activities. Chen et al. (2022) investigates the importance of auditing user access and privileges in mobile money platforms. Their research demonstrates that regular audits of user permissions help prevent unauthorized access and insider threats. By implementing effective access controls and conducting periodic audits, mobile money businesses can minimize the risk of internal fraud and unauthorized use of their systems.

It is critical to note that Fraud control frameworks provide a structured approach to managing fraud risks. Lin and Wu (2020) analyze the role of audit checks within fraud control frameworks adopted by mobile money businesses. The study highlights that audit checks serve as a critical component for evaluating the effectiveness of fraud control measures outlined in these frameworks. Regular audits help mobile money businesses assess the performance of their fraud prevention strategies and make necessary adjustments to maintain robust risk management practices.

2.5 Conclusion of Literature.

In conclusion, customer verification, password strength, and audit checks play a crucial role in the robust risk management and fraud control of mobile money businesses. Customer verification processes, such as biometric authentication and two-factor authentication (2FA), provide a strong foundation for mitigating fraud risks and ensuring the legitimacy of user identities. Moreover, enforcing secure password policies and encouraging the use of password managers support the security of user accounts, mitigating potential vulnerabilities exploited by fraudsters. Additionally, the implementation of regular and comprehensive audit checks, including real-time auditing and external audit expertise, enables mobile money operators to proactively detect and respond to fraudulent activities, safeguarding both their platforms and customers from financial threats. By integrating these three pillars into their risk management strategies, mobile money businesses can significantly enhance their fraud control capabilities and instill user confidence in the safety and integrity of their services.

CHAPTER THREE: METHODOLOGY

3.0 Introduction

This chapter presented the research design, research population and sample size, sampling procedure, research instruments, validity and reliability of research instruments, data gathering procedures, data analysis, ethical considerations, and limitations of the study.

3.1 Research design

Research design is a plan or road map that a researcher follows during research in order to find answers to research questions as validly, objectively, accurately, and economically as possible (Kumar, 2014). A completely quantitative research approach were used in this study. The study also adopted a descriptive survey research design. A descriptive survey research design allows a researcher to gather information, summarize it, present it, and interpret it for the purpose of clarification (Orodho, 2012). Large populations that cannot be studied through direct observation can best be studied through a descriptive survey (Borg & Gall, 2009); therefore, the research design was suitable for the study since it was used to collect data from the study population in a relatively shorter period of time.

3.2 Study Area

According to Acanit (2016), a study area is the area that a researcher focuses on when carrying out a research project or study. The study was carried out in Kampala District.

3.3 Study Population

Study population is a group of individuals selected on the basis of inclusion and exclusion criteria that relate to the variables being studied (Wiktionary, 2019). The study population involved a total number of fifty mobile money users in the urban area of Kampala District.

3.4 Sample Size

According to Hamed (2017), sample size measures the number of individuals, samples measured or observations used in a study. The sample size of the study was 44 determined according to the Krejcie and Morgan table as shown below:

Figure 1:Krejcie and Morgan table

Table 3.1									
<i>Table for Determining Sample Size of a Known Population</i>									
N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	354
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	191	1200	291	6000	361
45	40	170	118	400	196	1300	297	7000	364
50	44	180	123	420	201	1400	302	8000	367
55	48	190	127	440	205	1500	306	9000	368
60	52	200	132	460	210	1600	310	10000	370
65	56	210	136	480	214	1700	313	15000	375
70	59	220	140	500	217	1800	317	20000	377
75	63	230	144	550	226	1900	320	30000	379
80	66	240	148	600	234	2000	322	40000	380
85	70	250	152	650	242	2200	327	50000	381
90	73	260	155	700	248	2400	331	75000	382
95	76	270	159	750	254	2600	335	1000000	384

Note: N is Population Size; S is Sample Size Source: Krejcie & Morgan, 1970

3.5 Sampling Technique

Sampling technique is a research technique which identifies a specific process by which the entities of the sample have been selected (Katamba & Balikuddembe, 2014). The researcher used simple random sampling techniques.

A simple random sampling technique was used to select the remaining the 44 participants to provide information regarding risk management and fraud control in mobile money services Post Covid-19.

3.6 Sources of Data

Collection of data relied on both primary and secondary data.

3.6.1 Primary Data

Primary data is that data which was collected for the first time and it's original in character. Primary data was collected from a sample of respondents by use of well designed, pretested and administered questionnaires to collect the required information for the study

3.6.2 Secondary Data

Secondary Data relies on documentary sources to generate the needed information. Secondary Data involves the review of official documents such as text books and journals.

3.7 Data Collection methods

Data collection methods are methods used in gathering primary and secondary data from a variety of relevant sources to find answers to research problems (Katamba & Balikuddembe, 2014). The researcher used the Questionnaire method.

3.7.1 Questionnaire method

A questionnaire is a form containing a set of questions, especially addressed to a statistically significant number of subjects and is a way of gathering information for a survey (University of Pretoria, 2017). The researcher used this method to get data from the 44 respondents, as it is considered to have no bias.

3.8 Data Collection Instruments

Data collection instruments are questionnaires, survey plans, guides, rating scales, or any other forms which are used to collect information from the respondents (Acanit, 2016). The researcher used Questionnaires in this study to collect data.

3.8.1 Questionnaire

A questionnaire is a research instrument consisting of a series of questions or other types of prompts for the purpose of gathering information from respondents (Robinson, 2018). The Researcher used structured, unstructured and Likert scale questionnaires to get the feelings and opinions of respondents about the topic under study.

Questionnaires were physically delivered by the researcher to the respondents and picked after they were filled. The questionnaires were set basing on the themes as per the objectives of the study.

3.9 Data quality control

Data control is the process of governing and managing data (Graef, 2018). The researcher made sure that the data is of high quality and this was achieved by using the following approaches:

3.9.1 Validity

Validity is the extent to which the research data as well as the methods for finding the data are accurate, honest and on target (Dickinson, 2019). Relevant information requires careful planning to ensure that the information is clearly related to research objectives, and would be collected from the individuals best suited to providing the information. In order to obtain complete and accurate information, the researcher used well planned information collection instruments and survey administration procedures.

3.9.2 Reliability

According to Sekaran (2016), reliability of measurement is established by examining the stability and consistency of the data. In order to ensure the reliability of the research findings, the researcher used design questionnaires in a simple short format, to avoid respondents' confusion.

3.10 Ethical considerations

Ethical issues or principles are codes of ethics and oversight of research provided guidance (University of Pretoria, 2017). The researcher observed ethical issues while collecting data by keeping respondent's secrets, keeping time, not revealing respondent identity, getting permission before going to the field, respecting the participants, interpreting issues the way they are and finally the researcher thanked the participants.

3.11 Limitations of the study.

The following are the limitations of this study:

1. **Sample Size:** The study was limited to a specific sample size due to resource constraints. As such, the study's results were not fully a representative of all mobile business in Uganda.
2. **Data Collection:** The study relied on self-reported data from mobile money business managers, staff and regulators. The accuracy and reliability of the data was affected by recall bias, social desirability bias, and other factors.
3. **Time constraints:** The study was conducted within a limited timeframe, which could not allow for an in-depth investigation of all risk management practices of mobile money businesses in Uganda.
4. **Availability of data:** Some mobile money businesses were unwilling to share their risk management practices due to confidentiality concerns, which limited the study's scope and depth.

CHAPTER FOUR

PRESENTATIONS, ANALYSIS AND INTERPRETATION OF FINDINGS

4.1 Findings of the study

The chapter presents findings on “risk management and fraud control in Mobile Money Services in Post Covid-19” a case study on Kampala District. The findings start by showing the response rate, followed by presenting the background information of the respondents and finally descriptive presentation and analysis of the study findings in relation to specific objectives.

4.1.1 Response rate

The response rate for this research was 91% which was high. Amin (2005) suggested that a high response rate also suggests more accurate survey results.

Table 1: Response Rate

Category	Questionnaires issued	Questionnaires returned	Response rate (%)
Mobile branch offices	2	2	5
Mobile business agents	10	8	18
Mobile phone users	28	28	63
Online Bank users	4	2	5
Total	44	40	91

Source: Primary data

According to the table above, the survey response rate showed that out of the 44 questionnaires issued out only 40 were returned accounting to 91% response rate. This section shows the number of respondents who responded to the study based on the target population, but also shows the descriptive explanation of the characteristics of the respondents in relation to gender, age and level of education based on information provided in the questionnaire by the respondents.

4.2 Demographic findings of the study

The demographic characteristics are represented by gender, marital status, age bracket, level of education and time worked in mobile money business.

4.2.1 Gender of respondents

The findings for gender composition are represented in the table below;

Table 2: Gender of respondents.

Gender	Frequency	Percentage (%)
Male	18	45
Female	22	55
Total	40	100

Source: primary data

The findings show that majority of the respondents were female constituting 22(55.0%), while their composition of the male counterpart was 18(45.0%). The demographics imply that there are more females using Mobile Money services in Kampala district.

4.2.2 Marital status of respondents

The findings of the respondents' marital status is represented in the table below;

Table 3: Respondents' marital status

Marital status	Frequency	Percentage (%)
Single	28	70
Married	12	30
Total	40	100

Source: primary data

The findings in table above show that majority of the Mobile service users were single 28(70%) and those who were married constituted 12(30%). The marital composition clearly depicts that

the most of the respondents using Mobile money services are in their youthful years, coupling but not yet formally married.

4.2.3 Age group of respondents

The findings of the respondents' age group is represented in the table below;

Table 4: Respondents' age group

Age group	Frequency	Percentage (%)
18-35years	33	82.5
36-55years	7	17.5
56 and above	0	0.0
Total	40	100.0

Source: primary data

The findings in table above shows that majority of the respondents were in the age group of 18-35years 33(82.5%), followed by 36-55years age group 7(17.5%) and 56yearsand above with 0(0.0%) as age composition. The age group clearly depicts that the most of the respondents using Mobile money services are in their youthful years.

4.2.4 Education level of respondents

The findings of the respondents' education level is represented in the table below;

Table 5: Respondents education level

Education level	Frequency	Percentage (%)
Certificate level	17	42.6
Diploma level	21	52.5
Degree level	2	5.0
Total	40	100.0

Source: primary data

The findings in the table above explains that majority of the respondents had attained the diploma level 21(52.5%), followed by certificate holders 17(42.6%) and then degree level 2(5.0%). The findings imply that at least most of the respondents surveyed had acquired a substantial level of education that can help them use Mobile Phone services or on-line payment services.

4.2.5 Time spent by respondents in Mobile money services usage.

The findings represent the time spent by the respondent using Mobile Money Services is shown in the table below;

Table 6: Time spent using mobile Money services

Time spent at work	Frequency	Percentage (%)
Below 1 year	9	22.5
1-3years	15	37.5
3-5years	10	25.0
Above 5 years	6	15.0
Total	40	100.0

Source: primary data

Findings on the time spent by different respondents using Mobile money services shows that majority 15(37.5%) had been using the services for a period of 1-3years, followed by those who had been using them for 3-5years 10(25%). Those below 1 year had a score of 9(22.5%) and those who had been using the services for 5 years and above had a score of 6(15%). These imply that respondents had a substantial experience on mobile service usage and were in good position to provide the correct responses during the survey.

4.3 Findings on the relationship between customer verification and fraud control

The findings are based on a Likert scale of 1: Strongly Disagree, 2: Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly Agree.

Table 7: Table showing findings on the relationship between customer verification and fraud control.

B	Relationship between customer verification and fraud control	Mean	Std. Deviation
1.	Using finger prints or facial recognition for verification adds strong protection against fraud in mobile money.	4.55	0.714
2.	Strengthening customer verification processes boosts security in mobile money services.	4.23	0.768
3.	Continuous monitoring detects irregularities for timely fraud prevention.	4.15	0.662
4.	Strong customer verification mechanisms reduce occurrence of fraud.	4.13	0.883
5.	Elevated fraud during Covid-19 prompted enhanced customer verification.	3.78	0.832
	Total	20.84	3.859

Source: primary data

The findings on the relationship between customer verification and fraud control showed that majority of the respondents strongly agree that use of finger prints or facial recognition for verification adds strong protection against fraud in mobile money service usage, this was followed by respondents who agree, not sure, disagree and strongly disagreed respectively. The findings recorded an average mean score of 4.55 and the standard deviation of 0.714.

In the same way, the findings on the fact that strengthening customer verification processes boosts security in mobile money services showed that majority agree, followed by those who strongly agree, not sure, disagree and finally strongly disagree. An average mean score was 4.23 and the standard deviation score was 0.768.

Findings on the fact that continuous monitoring detects irregularities for timely fraud prevention showed that majority agree to the statement, strongly agreed, not sure, disagree and strongly disagree. The average mean score was 4.15 while the standard deviation was 0.662.

The survey results on the fact that use of a strong customer verification mechanism reduces occurrence of fraud showed that majority agreed, followed by those who strongly agree, not sure, disagreed and strongly disagree. The average mean score was 4.13 and a standard deviation of 0.883 were recorded.

Findings on the fact that an elevated fraud during Covid-19 prompted enhanced customer verification showed that majority agree, others were not sure, strongly agree, disagreed and strongly disagreed. The average mean score was 3.78 and the standard deviation of 0.832 was recorded.

Conclusively, the results imply that the most effective fraud control technique to Mobile money and service users is securing on line services of the customers by applying verification through use of finger print or facial recognition application use in order to limit fraudulent practices.

4.4 Findings on the relationship between password strength and fraud control

The findings are based on a Likert scale of 1: Strongly Disagree, 2: Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly Agree.

Table 8: Table showing findings on the relationship between password strength and fraud control.

C	Relationship between password strength and fraud control	Mean	Std. Deviation
6.	A mix of upper- and lower-case letters, numbers, and special characters, contributes to creating a strong password.	4.45	0.597
7.	A strong and unique password for your mobile money account reduces the risk and fraud.	4.05	1.037
8.	Updating mobile money account password contributes significantly to reducing the risk of fraud.	3.93	0.917
9.	Enforcing lockouts and monitoring for suspicious activity cuts password attack risks.	3.70	0.911
10.	Regular security updates reduce the risk of unauthorized access.	2.77	1.250
	Total	18.9	4.712

Source: primary data

The findings in the table above show the level of security provided by password strength in fraud control during Mobile money service delivery. According to the survey findings majority of the respondents strongly agree that a mix of upper and lower case letters, numbers and special characters, contributes greatly towards creating a strong password for securing customer mobile money services, followed by those who agree, not sure, disagree and strongly disagreed respectively. The findings recorded an average mean value of 4.45 and the standard deviation of 0.597.

Accordingly, the findings on the fact that a strong and unique password for the mobile money account reduces the risk and fraud when using mobile money services showed that majority

agree, followed by those who strongly agree, disagree, not sure and finally strongly disagree. An average mean value of 4.05 and a standard deviation of 1.037 were registered.

Findings on the fact that updating mobile money account password contributes significantly to reducing the risk of fraud showed that majority agree to the statement, strongly agreed, were not sure, disagreed and strongly disagreed. The average mean value was 3.93 while the standard deviation was 0.917.

Findings on the fact that, enforcing lockouts and monitoring for suspicious activity cuts password attack risks showed that majority agree, others were not sure, strongly agree, disagreed and strongly disagreed. The average mean value was 3.70 and the standard deviation was 0.911.

Finally, the survey on the fact that regular security updates reduce the risk of unauthorized access showed that majority agree, followed by those who strongly agree, not sure, disagreed and strongly disagree to the statement. An average mean value of 2.77 and a standard deviation of 1.250 were recorded.

The results above imply that both the service providers and the users of mobile services need to ensure that they first have a strong password but also have regular updates to increase on the security of their mobile money.

4.5 Findings on the relationship between Audit Checks and fraud control

The findings are based on a Likert scale of 1: Strongly Disagree, 2: Disagree, 3 = Not sure, 4 = Agree and 5 = Strongly Agree.

Table 9: Table showing findings on the relationship between Audit checks and fraud control.

D	Relationship between Audit checks and fraud control	Mean	Std. Deviation
11.	Audit checks promote accountability within mobile money business.	4.65	0.533
12.	Conducting regular audit checks helps in detecting and preventing fraudulent activities.	4.18	0.813
13.	Continuous monitoring of transactions is an effective strategy to identify and respond to fraud.	3.95	0.876
14.	Auditing allows the development and implementation of targeted mitigation plans.	3.60	0.778
15.	External audits provide valuable insights into potential fraud risks and control weaknesses.	3.52	0.716
	Total	19.9	3.716

Source: Primary data

The findings in the table above show the relationship between audit checks and fraud control. Majority of the respondents strongly agree that audit checks promote accountability within mobile money business, followed by those who agree, not sure, disagree and strongly disagree. The findings had a mean value score of 4.65 and the standard deviation of 0.533.

Accordingly, findings on the fact that conducting regular audit checks helps in detecting and preventing fraudulent activities showed that majority agree, followed by those who strongly agree, not sure, disagree and strongly disagree. An average mean value of 4.18 was registered and a standard deviation of 0.813.

Findings as to whether continuous monitoring of transactions is an effective strategy to identify and respond to fraud showed that majority agree, followed with strongly agreed, not sure, disagree and strongly disagree. The average mean value was 3.95 while the standard deviation was 0.876.

A survey on the fact that auditing allows the development and implementation of targeted mitigation plans showed that majority were not sure, followed by those who agree, strongly agree, disagreed and strongly disagree to the statement. An average mean value of 3.60 and a standard deviation of 0.778 were recorded.

Findings on the fact that external audits provide valuable insights into potential fraud risks and control weaknesses showed that majority were not sure, followed with those who agree, strongly agree, disagreed and strongly disagreed. The average mean value was 3.52 and the standard deviation was 0.716.

In conclusion, the results imply that securing Mobile services and payments from fraud requires regular audits so as to promote accountability within mobile money service providers and their customers.

4.6 Correlation between risk management and fraud control in Mobile Money Services

The table below presents the correlation between risk management as the independent and fraud control as the dependent variable in the use of online / Mobile Money Services.

Table 10: Correlation table of Risk management and Fraud control

	Using fingerprints or facial recognition for verification adds strong protection against fraud in mobile money	A mix of upper and lower case letters, numbers, and special characters, contribute to creating a strong password	Audit checks promote accountability within mobile money businesses.	Auditing allows the development and implementation of targeted mitigation plans.
Using fingerprints or facial recognition for verification adds strong protection against fraud in mobile money.	1	.126	.047	-.332*
A mix of upper and lower case letters, numbers, and special characters, contribute to creating a strong password.	.126	1	.105	-.099
Audit checks promote accountability within mobile money businesses.	.047	.105	1	-.037
Auditing allows the development and implementation of targeted mitigation plans.	-.332*	-.099	-.037	1

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

The correlation analysis table above shows the correlation between risk management and fraud controls measures in Mobile Money Services. Generally, the correlation was weak with a 0.126 significant value deemed as a very weak positive relationship. Given that correlation coefficient is significant when ($\alpha = 0.05$). The findings indicate that safeguarding the system from fraudulent activities demands more than just implementing audit control measures. It necessitates a holistic approach, encompassing elements such as infrastructure modernization, user sensitization, and the establishment of an online recovery system for mobile money users, among other critical components. This comprehensive strategy is essential to ensure the absolute security of the entire system.

CHAPTER FIVE

DISCUSSION OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The study investigated the relationship between risk management and fraud control in mobile money services in PostCovid19. The chapter presents the discussion, conclusions and recommendations and areas of further studies.

5.2 Discussion of findings

5.2.1 The relationship between customer verification and fraud control

According to research findings on the relationship between customer verification and fraud control, majority of the respondents strongly agree that use of finger prints or facial recognition for verification adds strong protection against fraud in mobile money service use. However, other risk mitigation measures like strengthening customer verification processes to boosts security in mobile money services also had significant impact.

This finding is supported by Chang and Kim (2022), who acknowledges that with biometric authentication, such as fingerprint or facial recognition, an alternative to traditional password-based systems is presented. This involves analyzing the effectiveness of biometric authentication in mobile money businesses and its potential role in fraud control. His study also highlights that biometric authentication offers a secure and convenient means of user verification, reducing the reliance on passwords and consequently minimizing password-related fraud risks.

5.2.2 The relationship between password strength and fraud control

Research findings on the relationship between password strength and fraud control showed that majority of the respondents strongly agree that a mix of upper and lower case letters, numbers and special characters, contributes greatly towards creating a strong password for securing customer mobile money services.

The above findings were supported by Zhu and Wang (2021) investigations on the trade-off between usability and password security in the context of mobile money services. Their research reveals that overly complex password requirements may lead to user frustration and result in the adoption of weaker passwords. The study suggests that mobile money businesses should strike a

balance between usability and security, providing guidance and incentives for users to create strong passwords without compromising their overall experience.

Additionally, password recovery mechanisms can inadvertently create potential entry points for fraudsters. A study by Li et al. (2019) examines password recovery practices in mobile money platforms and their susceptibility to social engineering attacks. The research highlights that weak password recovery processes, such as using easily accessible personal information, can lead to unauthorized account access. Mobile money businesses must implement secure and robust password recovery mechanisms to prevent fraudulent activities while providing legitimate access to users who have forgotten their passwords.

5.2.3 The relationship between audit checks and fraud control

Research findings on the relationship between audit checks and fraud control showed that majority of the respondents strongly agree that audit checks promote accountability within mobile money business. These findings are supported by Francis Annan (2017), who defined Audit checks in the context of mobile money services to refer to systematic and periodic reviews conducted to assess the security, compliance, and overall operational effectiveness of the mobile money platform. These audits are essential to identify potential vulnerabilities, gaps in security protocols, and compliance with industry standards and regulations.

In the same line Parker et al. (2019) examines the role of audit checks in detecting and preventing fraud within mobile money businesses and emphasized that periodic and rigorous audits play a crucial role in identifying unusual transactions, patterns, and discrepancies. He explains that by conducting regular audits, mobile money operators can quickly respond to emerging fraud threats and implement necessary preventive measures, bolstering their overall fraud control efforts and given the advancement of technology, auditing tools have evolved to meet the dynamic needs of mobile money businesses.

5.3 Conclusion

In as far the relationship between risk management and fraud control in Mobile money services is concerned there is need to employ highly effective and efficient fraud control methods given the circumstances, flexibility in fraud detection and prevention should be the first priority of all mobile service companies if they want to retain their valuable customers. In the same way since the relationship between mobile money services and risk management is very weak it is a strong

indication that many times customers concern about fraud on online payment systems go unresolved therefore the effectiveness of the measures seems not to convince the majority who still demand for a more secure money sending and payment platform so that they do not need to worry about losing their money during any incidence of transaction.

5.4 Recommendations

The mobile money operators should see that they tailor customer verification processes to suit specific user demographics and transaction volumes thus contributing to better risk management outcomes.

All mobile money service providers need to comply with effective fraud control and international risk management regulatory frameworks.

All mobile money service providers and users should carry out regular audits to help mobile money businesses assess the performance of their fraud prevention strategies and make necessary adjustments to maintain a high level of effectiveness in risk management practices.

5.5 Areas of further research

- I. The impact of government intervention in curbing money laundering in Uganda.
- II. The relationship between unemployment and fraudulent practices in the business sector.
- III. The role of an effective on-line security apparatus in limiting financial loss in mobile transactions.

References

- Acanit, M. (2016). Status of information and communication technology in academic libraries in central Uganda. *March*, 58–61.
- Annan, F. (2017, October 11). Fraud on Mobile Financial Markets: Evidence from a Pilot Audit Study. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3049376
- American Psychological Association. (2010). Ethical principles of psychologists and code of conduct. <https://www.apa.org/ethics/code/>
- Babbie, E. (2016). *The basics of social research*. Cengage Learning.
- Banks, J., & Kyobe, M. (2020). Mobile money risks and benefits: Insights from Uganda. *Journal of Financial Regulation and Compliance*, 28(3), 429-447
- Bank of Uganda. (2013). Guidelines on mobile money services in Uganda. Retrieved from https://www.bou.or.ug/bou/rates_statistics/regulations/guidelines_on_mobile_money_services_in_uganda.html
- Bank of Uganda. (2020). Annual Supervision Report: Mobile Money Services. https://www.bou.or.ug/bou/ratetables/supervision/mobile_money_services.html
- Bank of Uganda. (2020). Guidelines for Mobile Money Services in Uganda. <https://www.bou.or.ug/bou/media/regulatedinstitutions/mobile%20money%20guidelines%20-final-2020-02-13.pdf>
- Berger, M. (2020, May 15). The Washington Post. Retrieved from The Washington Post website: <https://www.washingtonpost.com/world/2020/05/15/coronavirus-is-upending-cash-economies-mobile-money-could-emerge-winner/>
- Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 13(3), 319-340.
- Dickinson, G. K., Kimmel, S. C., & Doll, C. A. (2015). *Journal of Librarianship*, 85(3), 225–243.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160.
- Diro. (2021, July 19). Customer Verification: Why Do Online Businesses Need to Know Their Customers? Retrieved from Diro: <https://diro.io/customer-verification/>

- Donkin, C. (2020, April 21). Mobile World Live News. Retrieved from Mobile World Live News Website: <https://www.mobileworldlive.com/money/news-money/uganda-warns-of-increase-in-mobile-money-fraud/>
- Duo. (2022, November 3). Duo. Retrieved from Duo website: <https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa>
- Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Boston: Pitman.
- Fund, I. M. (n.d.). International Monetary Fund. Retrieved from International Monetary Fund: <https://datahelp.imf.org/knowledgebase/articles/1906552-fas-what-is-mobile-money-how-is-it-different-fro>
- Gharad, B. (2019). Financial innovations and the risk of mobile money adoption in Kenya. *World Development*, 123, 104634.
- Graef, I., Husovec, M., & Purtova, N. (2018). Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. *German Law Journal*, 19(6), 1359–1398.
- GSMA. (2021). The state of the mobile money industry 2021. Retrieved from <https://www.gsma.com/mobilefordevelopment/resources/the-state-of-the-mobile-money-industry-2021/>
- Hamed, T. (2017). Determining Sample Size; How to Calculate Survey Sample Size. *International Journal of Economics and Management Systems*, 2(February 2017), 237–239.
- Hussey, J., & Hussey, R. (1997). *Business research: A practical guide for undergraduate and postgraduate students*. Palgrave Macmillan.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360
- Journal of Economics and Behavioral Studies*, 12(2), 13-28. Masika, R., & Karugaba, J. (2020). Mobile Money and Financial Inclusion in Uganda: A Systematic Review. *Journal of African Business*, 21(1), 98-113.
- Kalyango, J. N., & Gasper, K. (2021). Risk Management in Mobile Money Business: A Case Study of Uganda. Unpublished manuscript.

- Kasekende, L. (2018). The Future of Mobile Money in Uganda. Uganda Bankers Association. <https://ugandabankers.org/the-future-of-mobile-money-in-uganda/>
- Katamba, P., & Balikuddembe T.N. (2014). Basic research: Simplified for university students. Kampala: MK Publishers Ltd.
- Katongole, D. (2021). Mobile Money Risk Management Strategies: A Case Study of Uganda. *International Journal of Business and Management*, 16(1), 111-123.
- Kibirige, J., Kiwanuka, D., & Waiswa, R. (2021). Fraud in the Mobile Money Industry in Uganda: A Case of MTN Uganda Limited. *Journal of Advances in Finance and Accounting*.
- Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International.
- Kumar, R. (2014) *Research Methodology: A step by step guide for beginners*. Sage Publication Ltd.
- Lake, A. J. (2013, November). Risk Management in Mobile Money.
- Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). Pearson.
- Lowe, J. (2022, November 02). What is KYC? Financial regulations to reduce fraud. Retrieved from PLAID Website: <https://plaid.com/resources/banking/what-is-kyc/>
- Makate, C., & Nhamo, G. (2020). Determinants of Mobile Money Utilisation in Sub-Saharan Africa.
- Matthew Bird, R. M. (n.d.). *Innovations for Poverty Action*. Retrieved from <https://poverty-action.org/mobile-financial-services-consumer-protection-and-dispute-resolution-uganda>
- Mbabazi, R. (2021). Mobile Money Usage in Uganda: A Survey of the Unbanked Population. *Journal of African Business*, 22(2), 171-186.
- Mobile Financial Services. (2019). In H. K. Aijaz A. Shaikh, *Marketing and Mobile Financial Services* (p. 24).
- Mwesigwa, E. (2021). Operational Risk Management in the Mobile Money Industry: A Case Study of MTN Uganda Limited. *International Journal of Science and Business*.

- Muhumuza, T. (2019). Mobile Money and Financial Inclusion in Uganda: A Review of the Literature. *Journal of African Economies*, 28(2), 131-150
- Muhumuza, W. (2020). Credit Risk Management and Financial Performance of Mobile Money Services in Uganda. *Journal of African Business*, 21(1), 1-19.
- Muteba Mwamba, J. P., & Mabotuane, A. M. (2020). A study of the risk management practices in mobile money businesses: A case of DRC. *Journal of Accounting and Taxation*, 12(1), 1-11.
- Nkundabanyanga, S. K., & Kikonyogo, D. M. (2020). Mobile money, risk management and financial performance of microfinance institutions in Uganda. *Journal of Risk and Financial Management*, 13(6), 129.
- N-ABLE. (n.d.). N-able Risk Intelligence. Retrieved from N-ABLE Website: <https://www.n-able.com/features/risk-management-process-definition>
- News, U. B. (2016, Sept 9). Uganda Business News. Retrieved from Uganda Business News Website: <https://ugbusiness.com/2016/09/companies/airtels-share-of-mobile-money-agents-grows-but-still-behind-mt>
- Odero, J., & Munene, J. C. (2020). Operational risks in mobile money transactions: A case study of Safaricom M-PESA in Kenya. *International Journal of Scientific and Research Publications*,
- Ohia, N. (n.d.). How To Perform Audit of Internet/Mobile Banking and Other Electronic Payment (Fintech) Applications. Retrieved from Oxley: <https://oxleyconsults.com.ng/article/how-to-perform-audit-of-online-banking-and-electronic-payment-applications/>
- Onyango, C. M., & Wang'ombe, J. K. (2021). Mobile Money and Risk Management in Kenya: A Review of Literature. *International Journal of Business and Management Review*, 9(1), 1-12.
- PassCamp. (2022, September 22). PassCamp. Retrieved from PassCamp: <https://www.passcamp.com/blog/what-defines-password-strength/>
- PYMNTS. (2020, October 8). PYMNTS . Retrieved from PYMNTS Website: <https://www.pymnts.com/news/security-and-risk/2020/hackers-hit-mobile-money-payments-processor-uganda>
- RiskOptics. (2021, June 14). Password Management Risks: Protect Your Castle. Retrieved from RiskOptics: <https://reciprocity.com/blog/password-management-risks-protect-your-castle/>
- Sekaran, U. and Bougie, R. (2016) *Research Methods for Business: A Skill-Building Approach*. 7th Edition, Wiley & Sons, West Sussex.

- Seon. (2023, April 19). Seon. Retrieved from Seon:
<https://seon.io/resources/dictionary/biometric-verification/>
- Taylor, P. (2023, Jan 18). Statista. Retrieved from Statista Web Site:
<https://www.statista.com/statistics/1082290/number-of-mobile-money-subscriptions-in-uganda/>
- Times, T. E. (2023, July 16). The Economic Times. Retrieved from The Economic Times Website: <https://economictimes.indiatimes.com/definition/fraud>
- University of Pretoria. (2017). Chapter 4 : Research Design and Methodology, 3(Chapter 4),67–95.
- Wasswa, H. (2017). The Role of Mobile Money in Promoting Financial Inclusion in Uganda. African Journal of Economic Review.
- Wiktionary (2019). “ Study population .” Definitions.net. STANDS4 LLC, 2019. Web 16Jul 2019.<<https://www.defitions.net/definition/study+ population>

APPENDIX I: QUESTIONNAIRE

A QUESTIONNAIRE TO BE FILLED BY RESPONDENTS (MOBILE MONEY USERS IN KAMPALA DISTRICT)

Dear respondent,

I am **Ndyemanya Rosemary Marion** registration number S20B33/028 a student of Uganda Christian University, Mukono pursuing a Bachelor of Science in Accounting and Finance. I am currently conducting a study entitled “. **The Risk Management and Fraud Control in Mobile Money Services Post Covid-19.**” The study is purely for academic purposes and the information given will be treated with utmost confidentiality. I therefore, humbly request you to spare some time and answer the following questions. Thank you for your time and co-operation.

Instructions: -

1. Your name may not be necessary
2. Tick or write answers in full where applicable.

SECTION A: GENERAL INFORMTION

1. Gender

a) Male

b) Female

2. Marital Status

a) Single

b) Married

c) Others

3. Age bracket (years)

a) 18-35

b) 36-55

c) 56 and above

4. Highest level of education attained

a) Certificate b) Diploma c) Degree

5. How long have you worked in a mobile money business.

a) Below 1 year b) 1-3 years c) 3-5 years

d) Above 5years

SECTION B: The relationship between Customer Verification and Fraud Control

On a scale of 1-5, tick the appropriate box on how you strongly agree or disagree with the statements given on examining the relationship between customer verification and fraud control in the study context.

SCALE	1	2	3	4	5
	Strongly Disagree	Disagree	Not sure	Agree	Strongly Agree

	Statement	1	2	3	4	5
6.	Elevated fraud during Covid-19 prompted enhanced customer verification					
7.	Strengthening customer verification processes boosts security in mobile money services.					
8.	Strong customer verification mechanisms reduce occurrence of fraud					
9.	Using fingerprints or facial recognition for verification adds strong protection against fraud in mobile money					
10.	Continuous monitoring detects irregularities for timely fraud prevention					

SECTION C. The relationship between Password Strength and Fraud Control.

On a scale of 1-5, as used in the section above, tick the appropriate box on how you strongly disagree, disagree, not sure, agree or strongly agree with the statements given on examining the relationship between password strength and fraud control in the study context.

	Statement	1	2	3	4	5
11.	A strong and unique password for your mobile money account reduces the risk and fraud.					
12.	A mix of upper- and lower-case letters, numbers, and special characters, contribute to creating a strong password.					
13.	Updating mobile money account password contribute significantly to reducing the risk of					

	fraud.					
14.	Regular Security updates reduces the risk of unauthorized access.					
15.	Enforcing lockouts and monitoring for suspicious activity cuts password attack risks.					

SECTION D. The relationship between Audit Checks and Fraud control

6. On a scale of 1-5, as used in the section above, tick the appropriate box on how you strongly disagree, disagree, not sure, agree or strongly agree with the statements given on examining the relationship between Audit checks of mobile money accounts and fraud control in the study context.

	Statement	1	2	3	4	5
16.	Conducting regular audit checks helps in detecting and preventing fraudulent activities.					
17.	External audits provide valuable insights into potential fraud risks and control weaknesses					
18.	Continuous monitoring of transactions is an effective strategy to identify and respond to fraud.					
19.	Auditing allows the development and implementation of targeted mitigation plans.					
20.	Audit checks promote accountability within mobile money businesses.					

APPENDIX II: INTRODUCTORY LETTER FOR DATA COLLECTION.



UGANDA CHRISTIAN
UNIVERSITY

A Centre of Excellence in the Heart of Africa

SCHOOL OF BUSINESS

1st Aug 2023

TO WHOM IT MAY CONCERN

Name: NDYEMANYA ROSEMARY MARION Reg. No. 520833/028

A bachelor's student who is seeking permission from your office to collect data for his/her dissertation titled

"THE RISK MANAGEMENT AND FRAUD CONTROL IN MOBILE MONEY SERVICES POST COVID-19."
A CASE STUDY ON KAMPALA DISTRICT, UGANDA.

We shall be grateful if you could render assistance to him/her in collecting the necessary data for his/her dissertation.

The Uganda Christian University School of Business thanks you in advance

Mukisa Simon Peter
Research coordinator