BINDURA UNIVERSITY OF SCIENCE EDCUATION

FACULTY OF COMMERCE

DEPARTMENT OF BANKING AND FINANCE

DISSERTATION RESEARCH PROJECT

Role Of Mobile Banking In Curbing Financial Fraud In Zimbabwean Commercial Banks.A Case Study Of Bancabc Zimbabwe.

BY

B201059B

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELOR OF COMMERCE (HONOURS) DEGREE IN BANKING AND FINANCE OF BINDURA UNIVERSITY OF SCIENCE EDUCATION

JUNE 2024

RELEASE FORM

REGISTRATION NUMBER **:** B201059B

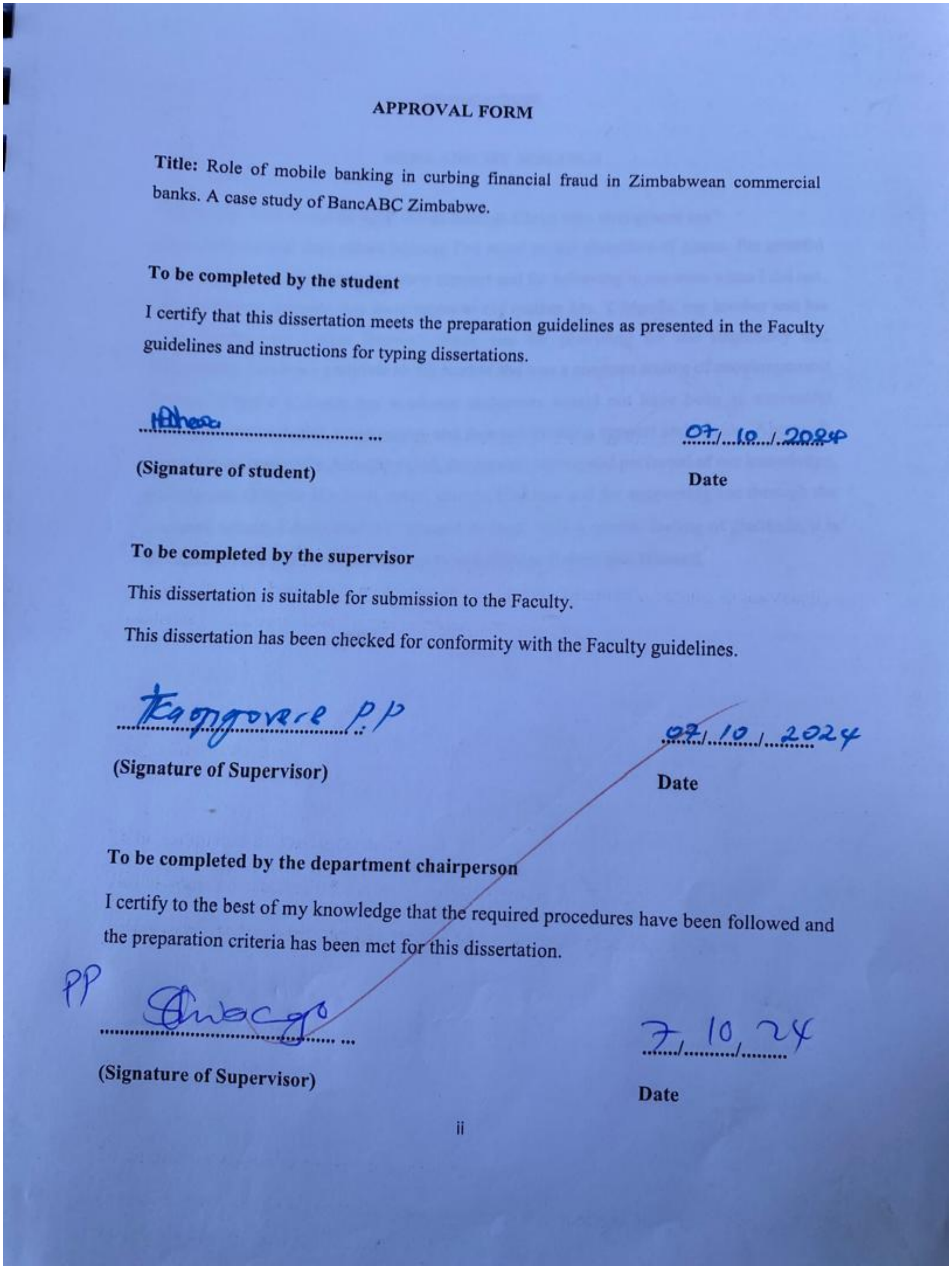
DISSERTATION TITTLE **:** Role of mobile banking in curbing financial Fraud in Zimbabwean commercial banks. A case study of BancABC.

DEGREE TITTLE **:** Bachelor of Commerce Honours Degree in Banking and Finance

YEAR GRANTED **:** 2024

Permission is hereby granted to the Bindura University of Science Education Library to produce single copies of this research project and to lend or sell such copies for private or scholarly purposes. The author does not reserve other publication rights and research project nor may extensive extracts from it be printed or otherwise reproduced without the author’s permission.

Permanent Address : 5725 MKOBA 19 GWERU



APPROVAL FORM

Title: Role of mobile banking in curbing financial fraud in Zimbabwean commercial banks. A case study of BancABC Zimbabwe.

To be completed by the student

I certify that this dissertation meets the preparation guidelines as presented in the Faculty guidelines and instructions for typing dissertations.

.... 07/10/2024

(Signature of student) **Date**

To be completed by the supervisor

This dissertation is suitable for submission to the Faculty.

This dissertation has been checked for conformity with the Faculty guidelines.

Kangovere PP 07/10/2024

(Signature of Supervisor) **Date**

To be completed by the department chairperson

I certify to the best of my knowledge that the required procedures have been followed and the preparation criteria has been met for this dissertation.

PP 7/10/24

(Signature of Supervisor) **Date**

ii

DEDICATION

MOM AND MY SIBLINGS

Philippians' 4:13 "I can do ALL things through Christ who strengthens me"
I have seen further than others because I've stood on the shoulders of giants. I'm grateful to my giants l call my family for their support and for believing in me even when I did not. I would like to dedicate this dissertation to my mother Ms. T Mpofu, my brother and his wife (Pardon and Lillian Dhewa), thank you for providing for me financially and emotionally. I owe my gratitude to my mother she was a constant source of encouragement for me. Without a doubt, my academic endeavors would not have been as successful without their consistent, unwavering, and forward-thinking support and advice. Above all, my gratitude goes to the Almighty God, the creator, source and perfected of our knowledge, wisdom and faith for His love, grace, mercy, kindness and for supporting me through the academic terrain. I dedicated this research to Him. With a special feeling of gratitude, it is my honor to dedicate this dissertation to my siblings Kelvin and Blessed.

ABSTRACT

This study aims to investigate the role of mobile banking in curbing financial fraud in Zimbabwean commercial banks, with a focus on BancABC Zimbabwe. The following served as the guideline to the research. Specifically, it examines the influence of credibility, privacy concerns, and access to mobile banking services on curbing financial fraud. Financial fraud remains a significant concern in Zimbabwe despite the growing adoption of mobile banking services. Limited empirical research has explored the role of mobile banking in mitigating fraud. This knowledge gap hinders the development of effective fraud prevention strategies, putting banks, customers, and the overall financial system at risk. This study employed the Technology Acceptance model, Diffusion of Innovation theory, The Institutional theory and The Fraud Triangle theory, the theories stated how people adopt to technology and how financial fraud occurs. The researcher used a descriptive case study research design on a sample size of 106 participants with the structured questionnaire as the main collection instrument. The study employed stratified random sampling method to choose participants. The data was analysed using Statistical Package for Social Sciences (SPSS V21), after which was displayed using tables. The validity of the data was addressed by the use of pilot testing and reliability was addressed by using Cronbach's Alpha which was reliable because it was above ($p>0.70$). The study revealed that there was a significant positive relationship between independent variables and the dependent variable (credibility **(.542),** privacy (**.0562),** access **(.572)**) .The study also reveals that mobile banking services have a significant and positive impact on the prevalence of financial fraud. The F-change statistics 16.37 which is statistically significant ($p>0.05$) indicates that addition of independent variables to the model significantly improves the modes ability to predict financial fraud. The study showed that mobile banking is effective in mitigating financial fraud. The researcher strongly recommend enhance credibility, improve access, strengthen privacy such as AI powered fraud detection.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the Almighty God because without Him l would not be where I’m today, Thank you ,God for giving me the courage ,the strength and the ability I needed to push forward and finish one of the goals l set for myself. My appreciation goes to my supervisor who was providing me with guidance throughout the research. I would also like to thank my BancABC placement co-workers for their encouragement, support, and mentoring during my attachment. I'd also like to thank the BancABC customers for their ideas, feedback, and advice during the data collection process. I'm grateful to the Kashiri family, in whose home I found a home during my studies, as well as to friends and colleagues Tinovimbanashe, Wadzanai, Ashley, Natasha, Molly, Gerald, Tinashe and Takudzwa. For the fun times and words of encouragement throughout the 4 years made it worthwhile, I’m much indebted ladies and gentlemen. Last but not least l owe a lot to my whole family for their undying support and their resolute belief that l can achieve much more in life. Had it not been for all of your prayers and blessings, as well as your sincere love and support, I would never have completed my studies. Thank you everyone.

Table of Contents

LIST OF ACRONYMS

AML	: Anti Money Laundering
GDPR	: General Data Protection Regulation
MB	: Mobile banking
PC	: Perceived credibility
KYC	: Know Your Client
RBZ	: Reserve Bank of Zimbabwe
TAM	: Technology Acceptance Model
RTGS	: Real Time Gross Settlement
USD	: Zimbabwean Dollar

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.0 Introduction

Knot and Tetteh (2022) stated that mobile banking is a technological innovation that enables the transfer of money through the infrastructure of mobile network operators. The use of mobile banking services has increased significantly in recent years across the world wide completely changing how people and businesses are handling their money. The convenience and accessibility offered by mobile banking have introduced numerous benefits to Zimbabwean consumers such as enhanced convenience in conducting transactions and increased financial inclusion .This dissertation seeks to explore the complex relationship between mobile banking and financial fraud. Mobile banking has also raised concerns about fraud and security. Therefore, the purpose of this study is to examine the current use of mobile banking in Zimbabwe and its impact on financial fraud, as well as propose potential solutions to address these challenges. It will also evaluate the efficiency of current risk mitigation strategies. This study intends to offer important insights and also creating strategies and policies to successfully combat financial fraud effectively and safeguard the integrity of the financial system.

The chapter I consists of the background of the study which gives content surrounding the research topic on a global stage, the regional stage, the nation and the local institutions. It also explains where the research journey started. It also consists of the problem statement which shows the matter at concern, hypothesis a proposed explanation made on the basis of limited evidence, objectives which contain what the research is trying to achieve and reasons why pursuing it.Aim of the study is also part of chapter I which states the overall purpose of the study. It also consists of delimitations, limitations, significance contribution and lastly summary of the chapter.

1.1 Background to the study

It is universally accepted that for a smooth functioning a money market an efficient and a good banking system is a must.Mallat (2004) defines mobile banking as the availability and provision of banking services via mobile phones and other portable telecommunication devices. The services of mobile banking includes depositing, withdrawing, sending money as well as making payments and viewing account balance. According to Olga (2003) due to technological developments people can now conduct payment and banking transactions via mobile phones. Financial fraud has been a persistent challenge in many developing countries including Zimbabwe. Fraudulent activities impose significant economic and social costs undermining trust in financial systems and hindering economic growth. Academics and the general public are both interested in the convergence of money and technology, particularly in the fields of development studies, banking and economic studies, and ICTs for development (Asongu and Odhiambo, 2023). Worldwide, financial fraud has been a recurring problem in many nations.

Internationally, mobile banking adoption has been increased in developed countries due to the availability of strong technological advancement (CGAP, 2012).The use of mobile banking has become widespread, redefining the manner that both individuals and companies carry out financial transactions. Its broad acceptance has been especially noteworthy in nations where traditional banking infrastructure is scarce, as mobile phones have become as effective instruments for financial inclusion. One of the best examples of a nation that has seen both a substantial increase in the use of mobile banking and problems with financial fraud is India. In 2004 around 65% of the total financial fraud cases reported by banks in India were technology related frauds committed through mobile banking (Goyal 2012).Continued adoption of web, mobile cloud and social media technologies in India has increased opportunities for attackers. Outsourcing and third party contracting driven by a cost reduction objective have diluted institutional control over IT systems and access.

According to Reserve Bank of India in 2014-2015, 22 million people were using mobile banking apps. Banking in India is increasingly being accessed by customers by downloading mobile banking apps to their mobile phones. According to the survey by Ernest and Young 84% in the banking segment reported fraud cases in India within the financial service sector. The word financial fraud has been defined by law in the Indian Contract Act Section 17 caused reputational risk, media attention and reduced profits.(Goyal 2012).Study in India shows that increased in the year 2019 due to induced Covid 19 lockdowns ,it invited many fraudsters due to digital payments related financial fraud. According to the survey on Indian banking financial fraud Deloitte (2015) states that 93% of the respondents were of the view that financial frauds in India due to mobile banking have increased drastically in the past 2 years according to National Crime Record Bureau.

Mobile banking has spread rapidly in SADC enabling fast and smooth cash flow within a simple click of a button. Indeed, the convergence of money and technology, particularly in the form of mobile banking, has attracted significant attention from the public and academia. The potential for digitized money to promote financial inclusion and alleviate poverty, especially in developing countries with limited banking access, has been a key focus in development studies, information and communication technologies for development, and banking and economic studies (Asongu and Odhiambo, 2023; World Bank, 2014).

The expansion of mobile banking technology, facilitated by mobile phones and tablets, has become increasingly significant in the lives of consumers worldwide, particularly in Africa. This growth is driven by factors such as the high cost of building landline-based telecoms and banking networks, which limits direct access to banks and financial services for a large portion of the global population. However, there are around 5 billion mobile phones available globally that can function as virtual wallets or personal ATMs, providing an alternative means of accessing financial services (Pesa means money in Swahili). Experts predicted that by 2020, with the increasing number of connected devices reaching 50 billion, mobile payments (m-payments) would likely become the most popular form of banking in many parts of Africa.

The rapid growth of mobile banking technology reflects the central role of mobile devices in the lives of consumers worldwide, particularly in Africa. However, these new channels present challenges for banks in the region to have a comprehensive overview of all the activities taking place within their systems. While mobile banking is user-friendly and often cheaper than traditional money-transfer services, weak laws and enforcement against financial fraud and money laundering pose significant challenges in many African countries. Identification requirements for customers are often minimal, and the nature of the process often bypasses a country's financial reporting system. This makes it difficult for authorities to monitor mobile payments effectively, even if they possess the necessary expertise, which is often lacking. Nonetheless, many large banks and multinational corporations, such as McDonald's, Starbucks, and Western Union, are rushing to incorporate mobile payments into their operations.

Fraudulent activities such as identity theft, fake note, unauthorized transactions, and counterfeit currency have undermined trust in the financial system and hindered economic growth. The Zimbabwean financial sector has faced numerous challenges in combating fraud due to factors such as limited access to traditional banking services, a large informal economy, and a history of economic instability. However, in recent years, mobile banking services have gained significant traction in Zimbabwe, offering an alternative financial solution to the unbanked population and addressing the challenges of traditional banking. It has revolutionized the way people in Zimbabwe manage their finances, providing them with convenient, accessible, and secure means of conducting financial transactions (Mogaji *et al*., 2021).Most smartphones have biometric authentication systems built in .In addition they have facial recognition that would be difficult for scammers to fake.

One of the mobile banking service providers in Zimbabwe is BancABC.It offers a range of mobile money services, including person-to-person transfers, bill payments, airtime topups, and merchant payments. As mobile banking services continue to gain popularity and usage in Zimbabwe, it is essential to understand their impact on the financial fraud. The investigation of the role of mobile banking in curbing financial fraud, is crucial for several reasons. Firstly, it addresses the need to explore innovative solutions for combating fraud in a country where traditional banking services may be limited or inaccessible for a significant portion of the population. Secondly, it offers insights into the effectiveness of mobile money platforms in preventing and detecting fraudulent activities, thereby enhancing the security and trust in financial transactions. Thirdly, studying the case of BancABC Zimbabwe provides a specific context for understanding the challenges, opportunities, and best practices in leveraging mobile money services for fraud prevention.

The widespread adoption of mobile banking services has provided users with easy, convenient, and real-time financial transactions, including shopping, utility payments, and transfers. Mobile banking is not exempt from the usual hazards that come with any new technology. The rapid proliferation of mobile technology has revolutionized the financial services industry, with mobile banking emerging as a transformative force in developing economies. In Zimbabwe, the adoption of mobile banking has been on the rise, driven by the country's high mobile phone penetration, the need to enhance financial inclusion, and the convenience and accessibility offered by mobile financial services (Fin Mark Trust, 2018). However, despite the growing popularity of mobile banking, financial fraud continues to be a significant concern for Zimbabwean commercial banks and their customers.

Financial fraud in the banking sector can take various forms, such as unauthorized transactions, identity theft, and cybercrime, often resulting in substantial monetary losses and eroding public trust in the financial system. In the case of mobile banking, the increased reliance on digital platforms and remote access to financial services has introduced new vulnerabilities and opportunities for fraudsters to exploit. Factors such as weak authentication mechanisms, inadequate customer education, and poor fraud detection and prevention systems have contributed to the persistence of financial fraud in the Zimbabwean mobile banking landscape (Pindiriri, 2012).Limited research has explored the role of mobile banking in curbing financial fraud in the Zimbabwean context. Existing studies have primarily focused on the adoption and usage of mobile banking services, with limited attention paid to the specific measures and strategies employed by commercial banks to mitigate fraud. This knowledge gap hinders the development of effective fraud prevention strategies, putting banks, customers, and the entire financial system at risk.

By conducting a comprehensive investigation into the adoption, usage, fraud prevention mechanisms, and effectiveness of BancABC Zimbabwe's mobile banking services, this research aims to contribute to the existing literature on mobile banking, fraud prevention, and financial inclusion in Zimbabwe. The findings of this study can help inform policymakers, financial institutions, and mobile money service providers on strategies to enhance the role of mobile banking in combating financial fraud and promoting a secure and inclusive financial ecosystem in Zimbabwe.

1.2 Statement of the problem

Despite the growing adoption of mobile banking in Zimbabwe, financial fraud remains a significant concern, with limited research exploring the role of mobile banking in curbing financial fraud. Specifically, there is a lack of understanding about the impact of credibility, privacy, and access to mobile banking services on financial fraud, and limited empirical evidence on the effectiveness of mobile banking in reducing financial fraud in Zimbabwean commercial banks. This knowledge gap hinders the development of effective fraud prevention strategies, putting banks, customers, and the entire financial system at risk. Therefore, this study aims to investigate the role of mobile banking in curbing financial fraud in Zimbabwean commercial banks, with a focus on credibility, privacy, and access. The elements of the financial technology-centric dark side of the internet include spam, phishing, malware, denial of service attacks, hacking, the violation of digital property rights and mobile money fraud (Kircaburun and Griffiths, 2018). At the same time, mobile banking platforms have introduced new features and capabilities that can potentially be leveraged to enhance fraud mitigation. Biometric authentication, real-time transaction monitoring, and geolocation data are examples of mobile-specific technologies that may hold promise for detecting and preventing fraud. The primary problem this dissertation will address is the need to better understand how the rise of mobile banking is transforming the financial fraud landscape, and how financial institutions can most effectively utilize mobile technologies and capabilities to detect, prevent, and mitigate fraud. Addressing this problem is critical, as the proliferation of mobile banking has significant implications for consumer trust, financial inclusion, and the overall stability of the Zimbabwean banking system, specifically examining cases within BancABC Zimbabwe.

1.3 Aim of the study

This dissertation aims to address this research gap by investigating the role of mobile banking in mitigating financial fraud. It will explore the security features and technological advancements in mobile banking, analyze their impact on fraud prevention and detection, and assess the factors influencing the adoption and utilization of mobile banking services among different user segments. The study will also identify the challenges and limitations of mobile banking in fully addressing financial fraud and provide recommendations for policymakers, financial institutions, and consumers to further strengthen the fraudprevention capabilities of mobile banking platforms. By providing a comprehensive analysis of the relationship between mobile banking and financial fraud, this dissertation will contribute to the understanding of how emerging technologies can be leveraged to enhance the security and resilience of the banking sector, ultimately benefiting both financial institutions and their customers.

1.4 Main Objective

The main objective of the study is to examine the role of mobile banking in curbing financial fraud in Zimbabwean commercial banks.

1.4.1 Sub Research Objectives

1. To examine the role of credibility of mobile banking in curbing financial in Zimbabwean commercial banks.
2. To explore the role of privacy of mobile banking in combating financial fraud in Zimbabwean commercial banks.
3. To examine the impact of access to mobile banking on combating financial fraud in Zimbabwean commercial banks.

1.5 Hypotheses

H_{11}: There is a statistically significant role that credibility of mobile banking plays in curbing financial fraud in Zimbabwean commercial banks.

H_{12}: Privacy of mobile banking plays a significant role in curbing financial fraud in Zimbabwean commercial banks.

H_{13}: There is a statistically significant impact of access to mobile banking in combating financial fraud in Zimbabwean commercial banks.

1.6 Significance of the study

Significance of the study was expressed as follows:

1.6.1 Significance to policymakers

This study is of utmost importance as it can provide valuable insights and recommendations to not just the Ministry of Finance, but also the entire government of Zimbabwe. By identifying and addressing the critical loopholes within the banking and finance sector, the research has the potential to guide the implementation of necessary reforms. These reforms can strengthen the regulatory framework, enhance security measures, and improve overall governance in the sector. Ultimately, the study can contribute to the stability, transparency, and trustworthiness of the banking and finance industry in Zimbabwe. Given the urgent need for stringent monitoring, this study will play a crucial role in paving the way for such measures. By shedding light on the issue at hand, it will provide valuable insights and recommendations that can guide the government in addressing this pressing concern effectively.

1.6.2 Significance to commercial banks

The study's outcomes are anticipated to provide valuable insights into the increasing occurrence of fraudulent activities in mobile banking transactions within Zimbabwe. This, in turn, will enable responsible organizations and mobile banking service providers in the banking sector to implement effective measures aimed at combating and eliminating fraud. The study aims to advocate for the benefit of consumers and stakeholders involved. The researcher recognizes the significance of conducting this study to generate suitable recommendations that can aid all responsible sectors in Zimbabwe.

1.6.3 Significance to academics

This study aims to address a significant gap in the existing literature by providing valuable findings and recommendations that can be utilized to influence policy-making and reforms related to information technology, risk management in finance, and mobile banking in Zimbabwe. The research seeks to contribute to the body of knowledge on cyber security, fraud prevention, and the effective management of mobile banking systems in the face of cyber-attacks and fraudulent activities.

The study's outcomes have the potential to serve as a foundation for future research endeavors in the field. Researchers and scholars interested in information technology, risk management, and mobile banking can build upon the findings of this study to explore more specific aspects or delve deeper into related topics. By establishing a solid groundwork of knowledge and insights, this study aims to foster a continuous and evolving research discourse in Zimbabwe and beyond, ultimately contributing to the development of robust and resilient systems in the face of cyber threats and fraud in the domain of mobile banking.

1.7 Assumptions of the study

According to Coates (2020), assumptions are assertions or propositions that are considered to be true or valid without being scientifically proven. They are taken for granted and form the basis for reasoning or decision-making, even in the absence of empirical evidence. In essence, assumptions are factors or beliefs that are accepted as true, but their validity is not grounded in scientific or empirical proof. For the purposes of this study, it is assumed that:

- The researcher will gather pertinent information from reliable sources that are relevant to the study. The study participants will be adequately informed about the topic being investigated, ensuring they have a clear understanding of the subject matter.
- All questionnaires surveys will be answered fully by respondents.

1.8 Delimitations

Study delimitations are characteristics that define the boundaries of the study. They are the demarcations designed by the researcher before carrying out the investigation, with the aim of controlling the study. The study is going to be confined only to the city of Harare. In this study the boundaries used include geographical, time frame, theoretical/ literature limitation and study participants’ delimitations and they are explained below. The study will be conducted by reviewing theories with regards to fraudster, mobile banking as well as risk management in finance. The study will be delimited to one bank which is BancABC Zimbabwe. The study is subject to limited time, the time frame given on the completion of the research meant that the researcher will not have enough time to gather as much data as possible.

1.9 Limitations.

While conducting a study of this size at the undergraduate level was exciting, the study was impacted by both non-financial and financial aspects. Lack of funding and time for the investigation hindered the researcher. The study's scope was further restricted by the participants' reluctance to contribute relevant data. Lack of resources, including money and time, further limited the research. The researcher overcame these obstacles and completed the study's objectives by exerting the required work patience and tenacity. During the investigation, the researcher encountered challenges related to information secrecy. Many respondents were hesitant to share information due to concerns that their competitors might gain access to it. To address this issue, the researcher implemented measures to protect the confidentiality and privacy of the participants. Identifying information of the respondents was not requested, ensuring anonymity. The data collection process was conducted discreetly, safeguarding the respondents' identities. Furthermore, the researcher assured the participants that their involvement in the survey was voluntary and that the research was solely for academic purposes. These steps were taken to instill confidence and encourage candid responses from the respondents.

1.10 Definitions of terms

- **Mobile banking fraud**: Mobile banking fraud involves fraudulent individuals who seek to acquire a user's confidential login details, including passwords, personal identification numbers (PINs), and token codes. (Thomson Reuters Legal, 2015).
- **Fraudsters**: Fraudsters are individuals who engage in fraudulent activities, particularly in business transactions. (Thomson Reuters Legal, (2015)
- **Mobile money:** a service in which the mobile phone is used to access financial services. Konte and Tetteh (2022)
- **Fraud:** wrongful and criminal deception intended to result in financial or personal gain (Dorminey 2020)
- **Cyber-attack;** malicious attempt to damage or disrupt a computer system or network.

  □ **Curbing;** restrain or keep in check.
- **Customer Acquisition Frauds –** Abuse of identity documents to create fake accounts on the platform.
- **Identity Theft –** This involves SIM swaps where fake ID proof is used to procure duplicate SIM cards for online transactions, leading to account takeovers.
- **Transaction Frauds-** The mobile money account holder can perform an increasing number of transactions. The number and variety of operations have grown immensely in the recent past.

1.11 Structure of the dissertation

The study is divided into five chapters .The chapters are as follows;

Chapter I: Introduction

This chapter provides an introduction to the study, covering the background of the research, statement of the problem, objectives of the study, significance of the study, limitations of the study, and organization of the study.

Chapter II: Literature Review

The second chapter reviews past research on financial fraud, as well as relevant books, journals, articles, and previously unpublished master's level dissertations.

Chapter III: Research Methodology

The third chapter explains the research methodology used in the study. It included research design, population and sampling, types and sources of data collection procedure, data analysis tools, techniques, reliability and validity.

Chapter IV: Data Presentation and Analysis

The fourth chapter focuses on the presentation and analysis of the collected data. It involves the presentation of the data in a suitable format, followed by in-depth analysis and interpretation of the findings. The chapter also highlights the major findings of the study.

Chapter V: Conclusion and Implementation

The fifth chapter concludes with a summary of the major conclusions, recommendations, and further ideas. These include reference books, periodicals, newspapers, earlier dissertations, etc., and are listed under the bibliography.

1.12 Chapter Summary

This chapter made an introduction, also provided the background and context for the study. It highlights the growing adoption of mobile banking in Zimbabwe and the persistent challenge of financial fraud faced by the country's commercial banks. The problem statement outlines the knowledge gap regarding the role of mobile banking in curbing financial fraud, particularly the impact of factors such as credibility, privacy, and access. The research objectives and questions are presented, focusing on examining the influence of these key factors on the effectiveness of mobile banking in reducing fraud. The significance of the study is discussed, emphasizing its theoretical contributions, practical implications, and contextual relevance to the Zimbabwean banking sector. The scope and limitations of the research are also outlined, and the organization of the dissertation is provided.to the research topic which the researcher is going to study, presenting the background and identify what the problem is. It then states the objectives of the research and the subsequent research questions that were answered by the study. A rationale for the research followed, allowing the presentation of the research study by the researcher as well as statement of the limitations that will be involved.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

The chapter reviews theoretical and empirical literature pertinent to the subject under study. It also presents the conceptual framework which shows the relationship between the study variables. This chapter aims to review the existing literature related to the researcher's study, examining the published works that have explored this subject matter. Also this chapter presents the research gap.

2.1 Purpose of the literature review

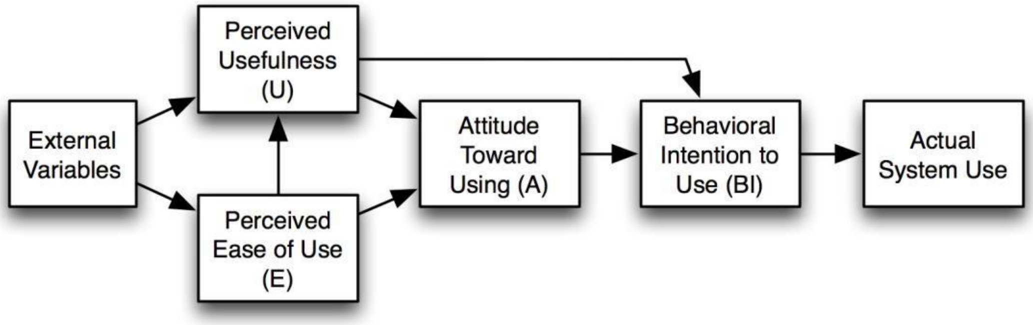
Literature review is of paramount importance in research since it aids or comes with foundations on which the research is based on (Saunders, Lewis & Thornhill, and 2016:740).A literature review, according to Thody (2007), is a list of all secondary materials that are relevant to the investigation. Conducting a literature review primarily aims to sample the most recent perspectives in secondary sources and gain comprehension of some aspects of the research concerns. The gap between earlier studies and the current study is also identified by the literature review. Hart (1998) argues that conducting a literature evaluation before starting any academic research is essential to ensuring the topic's suitability for inquiry.

2.2 Theoretical Literature Review

2.2.1Technology Acceptance Model (TAM)

Technology Acceptance Model is an information systems theory that model show users to accept and use technology, Davis (1986).TAM have been empirically tested from several studies to accept the level of acceptance of mobile banking. It was initially proposed by Davis Fred in 1986 and has been widely used in the field of information systems and technology research. The TAM suggests that when users are presented with a new technology a number of factors influence their about how they will use it.It is determined by two primary factors perceived usefulness and perceived ease of use, as shown diagrammatically below;

Fig 2.1; TAM process:


External Variables
Perceived Usefulness (U)
Perceived Ease of Use (E)
Attitude Toward Using (A)
Behavioral Intention to Use (BI)
Actual System Use

Source: ICBAE 2022

Perceived usefulness, as described by Davis (1986), refers to the extent to which an individual believes that utilizing a specific system would improve their job performance. In simpler terms, it pertains to whether someone thinks that technology can be helpful for accomplishing their tasks. On the other hand, perceived ease of use, also defined by Davis (1986), relates to an individual's perception of the level of effort required to use a particular system. If the technology is easy to use, it becomes less of a challenge to overcome.

Additionally, external factors such as age, social influence, and gender also play a role in determining technology adoption. The Technology Acceptance Model (TAM) further suggests that technology readiness influences the adoption of mobile banking, and it also impacts an individual's attitude toward using mobile banking.

The effect of perceived usefulness in the use of mobile banking if users think mobile banking would improve the effectiveness and efficiency of their transactions, they will use it. Willingness to use mobile banking services is predicted by perceived usefulness. Consumers think that by adopting mobile banking, their transactions will be more successful, of higher quality, and more efficient. More flexible services, time optimization, independence, convenience, quick customer response times, lower operating costs, and more efficient banking transactions are all offered by mobile banking. The more creative and user-friendly mobile banking is used by users based on their perceived utility. A significant factor in determining a user's intention to use mobile banking is perceived usefulness. Both initial and ongoing use can be influenced by perceived utility.

The term "perceived ease of use" describes the user's perception that utilizing and understanding mobile banking requires little effort. Based on their present knowledge and skills, users' perceived ease of use is defined as the degree of ease with which they expect to utilize mobile banking with the least amount of effort. The adoption of m-banking was found to be positively correlated with perceived ease of use. If it is simple and comfortable for them, they will use it. Their perception of ease of use is influenced by information technology infrastructure, user capabilities, and simplicity. Mobile banking innovations will make it easier to use. The more their perception of m-banking's simplicity of use, the greater their intention to utilize it responsibly.

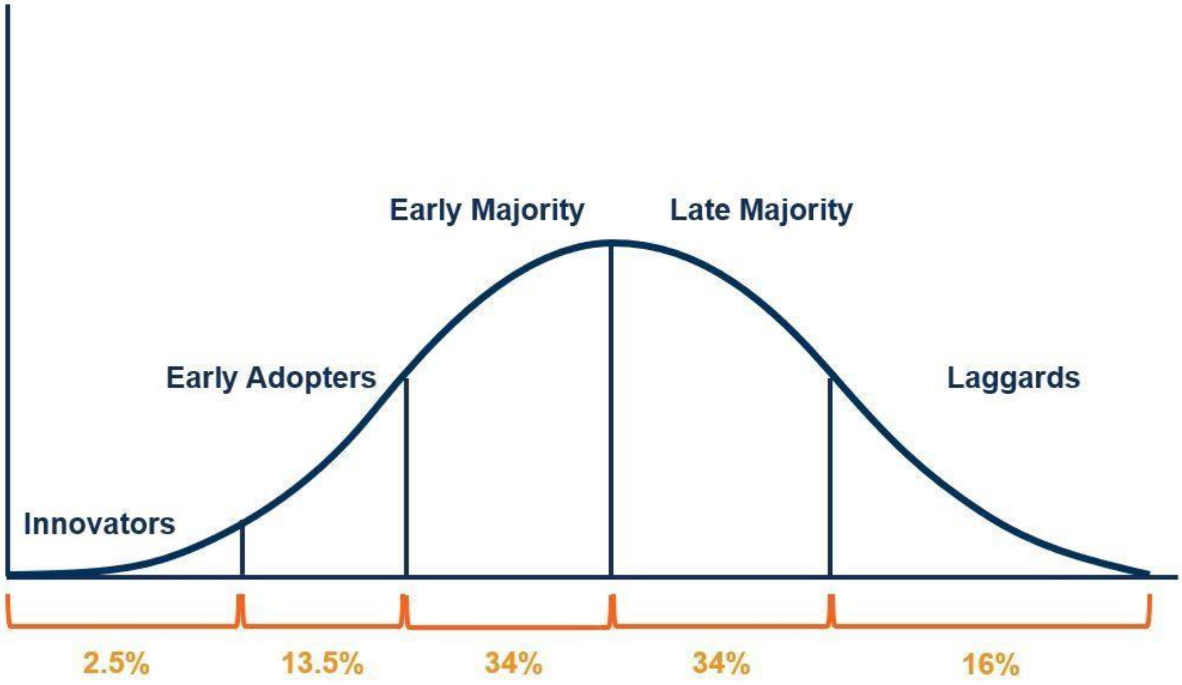
The effect of technology readiness on the use of mobile banking_the willingness of people to accept and use mobile banking for their financial transactions has been referred to as technology readiness. Optimism and inventiveness are two personality traits that are indicative of technology readiness. Technology adoption for mobile banking is being driven by innovation and optimism. The propensity to think that most individuals would encounter something good rather than something bad is known as optimism. Optimism holds that mobile banking will be more user-friendly and beneficial. People that are optimistic are typically more receptive of and responsible with m-banking. They don't reflect on unpleasant memories.

2.2.2 Diffusion of Innovation Theory

Everett Rogers created the diffusion of innovation hypothesis in 1962 to explain how concepts, items, or technological advancements and become embraced by individuals or communities in a given society. Rogers (2009) defined as the gradual spread and adoption of a new idea or innovation within a social system. . The idea focuses on the adoption process and the variables that affect adoption's pace and scope. Based on their openness to explore new things, adopters can be divided into five broad groups according to the diffusion of innovation theory: innovators, early adopters, early majority, late majority, and laggards. Regarding their openness to embracing new ideas, each group varies in terms of population share and possesses unique traits. Pioneers are the first to use novel concepts or advanced technology. They take risks, are daring, and can handle a lot of uncertainty. Inventors frequently have a high social standing.

As money and technology continue to merge, mobile banking has become increasingly prominent in discussions surrounding financial inclusion. Some advocates of financial inclusion have been pushing for the elimination of cash through digitization, asserting that this move will help alleviate poverty. This perspective gained traction following the successful introduction of groundbreaking mobile banking experiments such as G-Cash in 2004 (GSMA, 2009) and M-PESA in 2007 (Adeyemi and Davis, 2023). Moreover, the accomplishments of these mobile money ventures have opened doors for new market players to promote the shift from cash to electronic payments. One such player is the Better than Cash Alliance, which strongly believes that digitization is a crucial step towards advancing greater financial inclusion. On their website, they argue that digital money brings about cost savings (enhanced efficiency and speed) and fosters increased accountability, such as through improved tracking that reduces corruption and boosts women's economic participation.

Fig 2.2: The diffusion process;



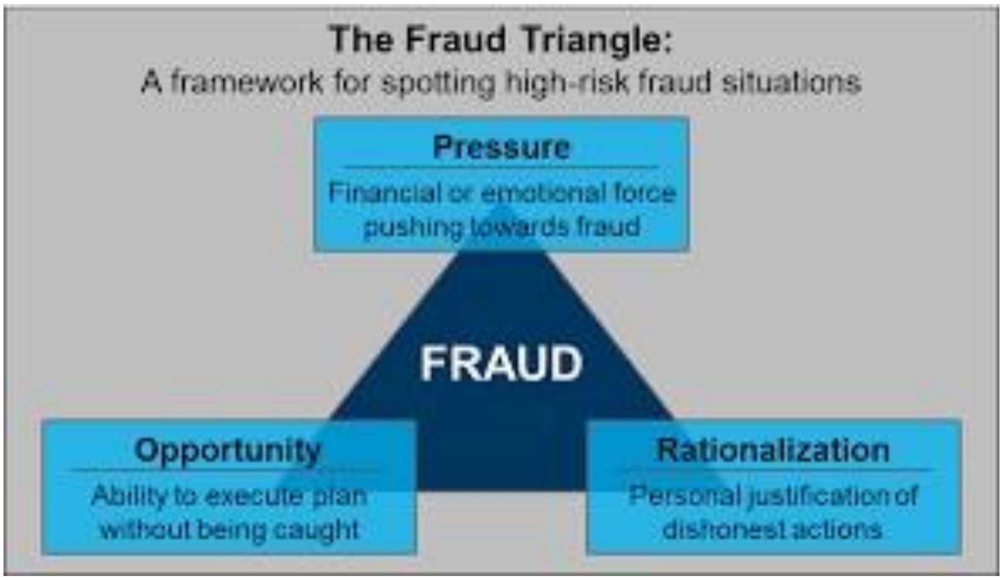
(Source: Wang 2003)

One of the key concepts in diffusion research is that change in consumer behavior is affected by different forces, which can be driving or inhibiting, and which can lead to the adoption or non-adoption of a particular innovation. The research methodology implied by the classical diffusion model is clear-cut and relatively simple. Diffusion scholars have often emphasized quantitative research approaches.

2.2.3 Fraud Triangle Theory

The Fraud Triangle is a theory developed by Donald Cressey in 1953, a criminologist, to explain the factors that contribute to financial fraud. It suggests that three elements must be present for an individual to commit fraud: opportunity, rationalization, and pressure or motivation.

Fig 2.3: The Fraud Triangle


The Fraud Triangle:
A framework for spotting high-risk fraud situations
Pressure
Financial or emotional force pushing towards fraud
FRAUD
Opportunity
Ability to execute plan without being caught
Rationalization
Personal justification of dishonest actions

Source; Wells (2007)

The existence of a chance for fraud to happen is the first component of the fraud triangle. This is a reference to the circumstances or settings that allow someone to commit fraud without being caught. Internal control flaws, a lack of supervision or monitoring, or access to important data or resources can all lead to opportunities. The cognitive process via which people defend their dishonest actions to themselves is known as rationalization. It entails making an apology or justification for their behavior, frequently by persuading oneself that their activities are for the benefit of society at large or that they deserve the unfair advantages. There are many different ways to rationalize anything, such blaming others or feeling deserving of the money. The existence of pressure or motive that pushes people to commit fraud is the third component of the fraud triangle. Financial strain may come from personal financial hardships, heavy debt loads, or the need for a better quality of life. Other non-financial reasons could be the need to conceal prior fraudulent activity or the desire for status or power. People are pushed to act dishonestly by these circumstances because they feel a sense of urgency or desperation.

2.2.4 The Institutional Theory

This idea recognizes that financial organizations have a responsibility to disseminate information about the services they offer. Ford *et al.* (2011) claim that there is friction in the financial sector. It captures a world where the parameters of the collaboration between service providers and customers are set by organizations, networks, norms, and regulations. The notion highlights the need for financial organizations to provide information in order to help consumers of financial fraud. In order to achieve financial inclusion, institutional elements like financial access information and incentives are crucial. (Bongomin, 2018b). Institutional theory generally aims to describe the more nuanced and resilient features of how institutions are created, maintained, changed, and dismantled (Brussel, 2016). In the context of the current study, it addresses the financial system's continuing influence on institutions. This addresses the factors that influence financial inclusion by using structures (such as norms, rituals, and conventions) to guide social behavior. It is important to remember that, as opposed to focusing only on theories particular to finance, the institutional theory study of financial inclusion incorporates general theories from the fields of economics, political science, and sociology (Brussel, 2016).

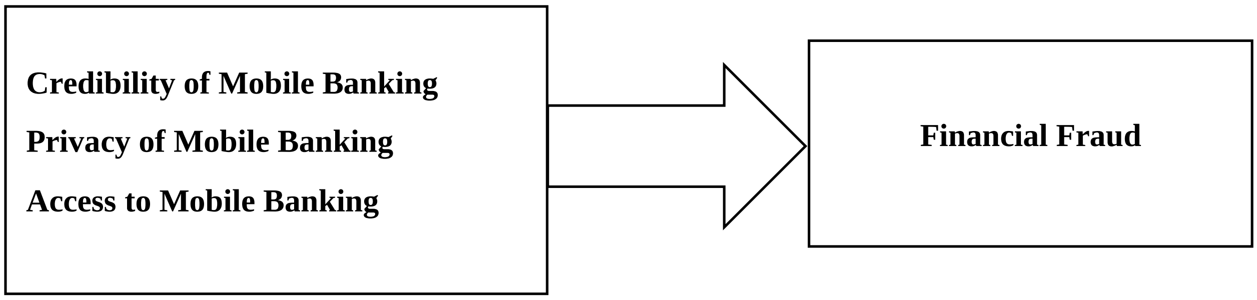
2.3 Conceptual Framework

Conceptual framework refers to concepts that are connected to the researcher’s topic statement. It is often represented diagrammatically showing dependent variables and independent variables.Mugeda *et al,* (2003) he defines it as an explanation that conceptualizes relationship between study variables shown as below

Fig 2.4: Variables

Source: Author's Computations, 2024

INDEPENDENT VARIABLES DEPENDENT VARIABLE



2.4 Independent variables

The researcher examined the relationship between dependent and independent variables, trying to understand how changes in the independent variable affect the dependent variable taking the hypothesis testing into consideration. In investigating the role of mobile banking in promoting financial fraud in Zimbabwean commercial banks, independent variable are access ,usage and awareness on the other hand financial fraud is the dependent variable.

2.4.1 Credibility of Mobile Banking

Credibility of the mobile banking service, according to Wang et al. (2003), is the degree to which a user thinks that using mobile banking won't pose any security or privacy risks. When it comes to using mobile banking, credibility reflects personal security, privacy, risk, and trust (Yu, 2012). According to Wang *et al.* (2003), credibility is influenced by two key factors: security and privacy. Credibility is linked to customers' feelings of safety, comfort, and satisfaction. Credibility, according to Wang *et al*. (2003), is the degree to which an individual feels that their transactions and personal information are secure. This belief has an impact on a technology system's acceptability.

The security measures implemented by mobile banking providers play a crucial role in determining credibility. Users need assurance that their financial information, transactions, and personal data are protected from unauthorized access and potential fraud. Factors such as encryption, two-factor authentication, biometric authentication (e.g., fingerprint or facial recognition), and secure communication protocols contribute to the overall credibility of mobile banking services.

Compliance with relevant financial regulations and industry standards adds to the credibility of mobile banking. Users expect mobile banking providers to adhere to established guidelines and regulations to ensure the safety and legality of their transactions. Compliance with regulations such as Know Your Customer (KYC) and Anti-Money Laundering (AML) further enhances credibility. The reputation and track record of the mobile banking provider significantly impact credibility. Users are more likely to trust established financial institutions or banks with a long-standing reputation for delivering secure and reliable banking services. Reviews, ratings, and customer feedback can also influence the perception of credibility.

According to Wang *et a*l. (2003) perceived credibility (PC) of the MB service is the extent to which a user believes that the use of MB will have no security or privacy threats. In light of this definition, this study operationalized PC as comprising of two dimensions, which are, security (SE) and privacy (PR). SE is defined as the belief that the MB systems provide a very effective control to protect and safeguard the information of the MB users. On the other hand, PR is defined as the belief that the information of the MB users is not manipulated and exploited for monetary gains or other benefits by the MB provider or other inappropriate parties.

Many studies done globally showed that majority of mobile banking users are very concerned with the safety of their money kept in the bank (Susanto et al., 2013; Gao et al., 2015; Firdous and Farooqi, 2017). These studies also suggest that users are equally concerned with their personal information given to and stored by the banks. Recent study by Asian Institute of Finance (2016) involving Malaysian banking consumers revealed that 50% of the respondents did not feel safe with the data kept in mobile devices. Gao et al. (2015) found that security and privacy concern has a negative relationship with trust and satisfaction. In other words, when users perceived that the MB services as highly credible, their trust level and satisfaction will also increase (Susanto et al., 2013; Firdous and Farooqi, 2017).

2.4.2 Privacy of Mobile Banking

Privacy is a fundamental concern when it comes to mobile banking, as it involves the handling of sensitive financial and personal information. Here are some key aspects related to the privacy of mobile banking: Mobile banking applications typically employ strong encryption protocols to secure the transmission of data between the user's device and the banking servers. Encryption ensures that the information sent over the network is encoded and can only be accessed by authorized parties, making it difficult for hackers or unauthorized individuals to intercept and decipher the data. Mobile banking apps utilize various authentication methods to ensure that only authorized individuals can access the user's account. This can include passwords, PINs, biometric authentication (such as fingerprints or facial recognition), or two-factor authentication (2FA).

These measures add an extra layer of security to protect user privacy. Financial institutions offering mobile banking services are bound by data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union or other similar laws in different jurisdictions. These regulations enforce strict standards for the collection, storage, processing, and sharing of personal data, ensuring that user privacy is protected. Privacy Policies: Mobile banking providers typically have privacy policies in place that outline how they collect, use, and safeguard user data. These policies inform users about the types of information collected, how it is stored and secured, and under what circumstances it may be shared with third parties. Users should review and understand these policies to make informed decisions about their privacy.

Mobile banking applications often offer settings and options that allow users to manage their privacy preferences. This may include options to control the sharing of personal information, manage app permissions, and set notification preferences. By providing users with control over their privacy settings, mobile banking apps empower individuals to tailor their privacy preferences according to their comfort level. Users are encouraged to connect to secure and trusted networks when accessing mobile banking services. Public Wi-Fi networks, for example, may pose security risks as they can be vulnerable to eavesdropping and data interception. By using secure network connections, such as virtual private networks (VPNs) or cellular data networks, users can enhance the privacy of their mobile banking activities. Mobile banking apps and operating systems frequently release updates and security patches to address vulnerabilities and strengthen security measures. Users should ensure that they regularly update their mobile banking apps to benefit from the latest security enhancements and privacy features.

Many studies done globally showed that majority of mobile banking users are very concerned with the safety of their money kept in the bank (Susanto et al., 2013; Gao et al., 2015; Firdous and Farooqi, 2017). These studies also suggest that users are equally concerned with their personal information given to and stored by the banks. Recent study by Asian Institute of Finance (2016) involving Malaysian banking consumers revealed that 50% of the respondents did not feel safe with the data kept in mobile devices. Gao et al. (2015) found that security and privacy concern has a negative relationship with trust and satisfaction. In other words, when users perceived that the MB services as highly credible, their trust level and satisfaction will also increase (Susanto *et al*., 2013; Firdous and Farooqi, 2017).

While mobile banking providers take significant measures to protect user privacy, it is important for users to also play an active role in maintaining their privacy. This includes using strong passwords, avoiding sharing sensitive information over insecure channels, and being cautious of phishing attempts or suspicious activities. By practicing good privacy habits, users can maximize the privacy protections offered by mobile banking services.

2.4.3 Access of Mobile Banking

Access to mobile banking can increase the risk of financial fraud in many ways. Having such a large population using mobile banking it increases the fraudsters in the system. With access to mobile banking, users can provide their personal information such as account numbers, passwords, email address, age and date of birth this information can then be used by fraudsters to get into their accounts. In areas where regulatory oversight and customer protection mechanisms are weak fraudsters can exploit the lack of safeguards to carry out fraudulent activities.

While the growth of consumer embracing mobile banking has been remarkable over the last few years, the issues that remain plaguing the consumers as well as the mobile banking providers are security, privacy, trust and satisfaction. Yu (2015) stated that "considerable literature has indicated that MB operates in an impersonal and technology-enabled environment that might cause customers to feel uncertainty and risk which create a lack of trust for using MB". Accordingly, Yu (2015) argued that examining antecedents of MB trust and its consequences becomes crucial. The literature suggests while there are many factors that can affect MB trust, perceived quality and perceived credibility are those that were commonly highlighted in the literature of past studies

2.5 Dependent variable

2.5.1 Financial Fraud in the banking sector

Financial fraud is a form of crime that involves the misuse of financial services for personal gain (Bhatia 2013) .According to Mawere (2019) fraud is a result of a wrongful or criminal deception intended to result in financial personal gain. Financial fraud is determined by the independent variables that is usage, awareness and access. There are different types of financial fraud, which are phishing hacks, fishing, frauds using online sales platform, frauds that use unverified apps, scans through QR code. According to the research, financial fraud is a worldwide phenomenon that affects all continents and all sectors of the economy. With the rapidly growing banking industry globally, frauds are increasing fast, and fraudsters have started using innovative methods. Shockingly, the banking industry everywhere dubs rising fraud as an inevitable cost of business (Sultana et al., 2022).

2.6 Empirical Literature Review

The empirical literature review section includes a variety of empirical research that were pertinent to the study's objectives and variables. The research objectives were taken into consideration when reviewing the studies.

2.6.1 Credibility of Mobile Banking

According to a 2020 study by Alhadi, the research on bank clients found that the relationship between mobile banking credibility and financial fraud had different outcomes. The survey results showed that a bank's credibility has a strong influence on reducing financial fraud. Based on this evidence, bank management needs to be able to identify the factors that could drive financial fraud. The data analysis on the bank credibility variable found a t-value of -0.623, a β (beta) coefficient of -0.024, and a significance level of -0.534. This means that statistically, using a 5% significance level, the -0.534 significance level is higher than 5%, so bank credibility has a significant and positive impact on reducing financial fraud. The study also found that individuals using digital banking services don't primarily consider the bank's reputation. However, the analysis of the service convenience variable showed a t-value of 5.307, a β of 0.318, and a significance level of 0.000. This indicates that statistically, at a 5% significance level, the 0.000 significance is lower than 5%, so service convenience has an important and positive effect on people's use of mobile banking. In summary, the research concluded that the higher the level of convenience felt by customers, the more positive their attitude will be towards using digital banking, which in turn helps lower instances of financial fraud.

Similarly to a study conducted by Londa D (2017), it was found that credibility has a significant negative impact on customer satisfaction when using mobile banking. This finding is consistent with previous research conducted by Masrek et al. (2018) and Metlo et al. (2021), which also concluded that credibility has a significant negative influence on customer satisfaction, particularly in the context of mobile banking. When individuals perceive a system as credible, meaning that it securely processes financial transactions and maintains the confidentiality of personal information, they are more likely to voluntarily accept and use mobile banking services provided by organizations such as BSG (Banking Services Group).In this particular study, customers residing in Manado and its surrounding areas, who voluntarily adopted and utilized the information technology systems offered by specific banks, tended to use the system when they had trust that their information was being protected. By gaining acceptance of the technology system provided by BSG, the bank has successfully built a positive image and established itself as a trusted institution that not only safeguards customers' funds but also ensures the security of their personal information. The trust that emerges from feeling assured when conducting transactions creates a safer and more comfortable environment. Although BSGtouch, the mobile banking service offered by BSG, is relatively new compared to other services in the market and requires further development, a majority of customers who choose to use BSGtouch believe that their privacy is secure. The perception of a secure environment, where mobile banking processes transactions safely and protects the privacy of personal information, is likely to have a positive impact on customer satisfaction when using BSGtouch.

2.6.2 Privacy of Mobile Banking

According to a study by Singh T (2013), there is a positive correlation on privacy concerns when it comes to using mobile banking. The study clearly establishes that as the level of privacy decreases, financial fraud increases. Therefore, banks should make continuous efforts to minimize security and privacy concerns associated with mobile banking.Based on interviews conducted with non-users of internet banking, it was concluded that a significant number of educated individuals refrain from using internet banking due to security concerns. This highlights the need to build trust among potential users. Trust can be established by strengthening the security features of internet banking, reducing the occurrence of cyber fraud, and effectively communicating the high standards of security to customers. It is important to note that the level of security and privacy concern associated with internet banking is generally high. In light of this, banks should proactively work towards reducing these concerns. Alongside other communication channels, banks can utilize their websites to disseminate information regarding the safe use of internet banking. By providing clear and comprehensive guidance on security measures, banks can help alleviate customer concerns and foster trust in the use of internet banking services. Study found that there was positive and significant correlation between privacy and financial fraud regarding use of mobile banking [r (71) = .539, p=.000)].The results of the study are in line with the claim of the current study, which purports that Privacy of mobile banking plays a significant role in curbing financial fraud.

A study carried out by Abuga I and Manyange (2015) in selected commercial banks in Rwanda concluded that there is a positive significant between privacy of mobile banking and financial fraud, A sample size of 227 was computed ,the data was collected through the use of questionnaire. The results of the effectiveness of mobile banking on managing financial fraud was determined through the use of 1 way ANOVA. The study found that mobile banking services were generally effective, with the most effective item being security measures and privacy, followed by time management and convenience. However, the study also found that there were significant differences in the effectiveness of mobile banking services among the selected banks.

2.6.3 Access of Mobile Banking

A study by Ouko (2020) stated that mobile banking fraud has significant implications for financial inclusion. While mobile banking has led to greater financial inclusion by providing access too cheap and reliable financial services, it has also become a conduit for financial fraud. The rapid growth of mobile financial services has facilitated access to financial services for the formerly unbanked population, but it has also led to a reduced rate in financial fraud. The prevalence of financial fraud on mobile money platforms raises the need to stay abreast of developments in this space and strengthen digital consumer protection laws. Promoters of digital financial services, telecommunication companies, and regulators should collaborate to tighten existing laws against fraudsters and establish efficient mechanisms for recourse and compensation for victims of fraud and cybercrime.

By addressing mobile money fraud, financial inclusion can be promoted and the risks associated with cyber insecurity can be mitigated. The findings showed that mobile banking has led to a greater financial inclusion, but the rate of the reported financial crimes has also increased over the past decade. The results of the study are in line with the claim of the current study, which purports a statistically impact of access to mobile banking in combating financial fraud.

2.7 Gap Analysis

The existing research on the role of mobile banking in curbing financial fraud has primarily focused on developed economies with limited empirical evidence from developing countries particularly in the Zimbabwean context. Given the unique challenges faced by customers and banks in developing economies such as low financial literacy, inadequate capital, and financial fraud, there is need to examine the contextual factors that shape the relationship between mobile banking and fraud prevention. While previous studies have identified factors such as credibility, access and privacy as potentially influencing the effectiveness of mobile banking in reducing fraud ,the specific mechanisms by which these factor's operate and interact are not well understood. The author found no research that specifically addressed the role of mobile banking in curbing financial fraud in Zimbabwean commercial banks and the challenges faced by these commercial banks in trying to combat this kind of risk.

2.8 Chapter Summary

This chapter gave a theoretical framework on role of mobile banking in promoting financial fraud in Zimbabwe's commercial banks. It also reviewed the conceptual frame work of mobile banking and financial fraud by clearly stating the variables. Different types of financial fraud were discussed. The following chapter will go over the research approach that is going to be used to conduct the research.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

In order to satisfy the aim behind the study and to be able to answer the highlighted questions in chapter I, the research design and methodology of the study are discussed in this chapter. Elements such as an overview of methodological approaches, sampling, and data collection instruments and procedures are discussed. Issues of validity, reliability and trustworthiness that are relevant to the study are also highlighted.

3.1 Research philosophy

A research philosophy refers to the set of beliefs, assumptions, and values that guided the researchers approach to conducting research (Igwenagu, 2020). A research philosophy clarifies how a researcher understands knowledge and reality as well as the process of attaining knowledge. It highlights the evolution and nature of that knowledge and conveys a view about the nature of knowledge and reality (Mende, 2022). The author added that a research attempt should be guided by a research philosophy argument since ignoring it might seriously affect the effectiveness of the investigation. Research philosophy provides additional insight into the nature and development of knowledge on a certain subject. This process of producing knowledge entails the gathering, processing, and methodical use of data to address a particular issue in a particular organization. Significant assumptions about one's worldview are related to research philosophy, and these presumption will support the research strategy and methodology used as part of that approach (Mende, 2022).

According to Creswell (2010), before choosing a research method and starting the research design, it's critical to choose the right research philosophy. This is true because the research philosophy lays the groundwork for the rest of the discussion. The research philosophy of positivism holds that investigation should be carried out without regard to any particular values. This implies that the researcher must prevent their own prejudices from influencing the findings. Positivism was chosen for this research study because it makes replication of the findings possible. This implies that other researchers can use the same approach and obtain identical outcomes.

3.2 Research approach

The process that a researcher uses to gather, examine, and analyze data is referred to as their research approach (Stake, 2015). A hybrid research strategy, quantitative research methods, was used by the researcher. According to Creswell & Clark (2011), it is crucial to take into account utilizing quantitative research methodologies. Quantitative approach was used because it analyze numerical data on fraud incidents, transaction volumes and the effectiveness of fraud prevention measures that are in place. Through the distribution of questionnaires to a representative sample of BancABC bank mobile banking users, quantitative information regarding their views of fraud risk and satisfaction with security measures can be obtained.

3.3 Research design

Avison et al. (2018) and Bryman (2014) define research design as an overall strategy or systematic approach that is used to fulfill the aims and objectives of a research study. Research design can be exploratory, descriptive (Robson, 2012; Sekaran, 2013)**.** Using a case study research design, the study was conducted on BancABC branches in Harare. Data collection and analysis are based on a research design, according to Bryman and Bell (2015:28). As a result, the design included a summary of the objectives of the study, from developing the hypothesis and its implications to data analysis (Kothari, 1990). Therefore, a descriptive case study was the research methodology used by the researchers. A descriptive case study approach is an analysis technique that employs a range of data sources to carry out a comprehensive examination of a particular primary masterpiece in its natural setting, according to Saunders et al. (2016).

The case study also has the ability to reflect the real-life experiences of the research subjects in their natural setting, therefore, the case study will help the researcher to capture the real impact of mobile banking in curbing financial fraud (Hartley, 2014). The case study is also flexible because it can even be used in the pilot research and this helped the researcher to make the necessary adjustments to help in addressing the research problem (Hartley, 2014). According to Khotari (2016) a case study is important in data analysis because it turns opinions into facts, hence the given responses can be turned into useable data.

3.4 Data collection instrument

According to Kothari (2004), data collection instrument is a tool or piece of equipment used to gather data, such as surveys, interviews, or observation. Adding on, according to Singh (2007), a research tool is a strategy or manner that a researcher uses to acquire data for the subject under study. Data is gathered using techniques like questionnaires which were distributed to mobile banking users. Based on the research topic, aim, objectives, and questions, the data gathering tools were selected for this study. The purpose of the research instruments was to collect data that would allow the researcher to gain insight into the ways in which mobile banking has contributed to combating financial fraud in Zimbabwean commercial banks and to have a comprehensive understanding of the effects of this financial fraud on the country's economy.

3.4.1 Questionnaire

According to Sekaran (2016), a questionnaire is a self-administered data collection instrument, consisting of a set of questions presented and answered by targeted population. .. Therefore, a structured questionnaire was gathered from the BancABC customers using a standardized questionnaire. Self-administered surveys were chosen because they are inexpensive and simple to use, and the structured questions were designed to help respondents answer questions more quickly and easily. Because the respondents could do the questionnaire whenever it was convenient for them, the method also guaranteed a higher chance of anonymity. It also ensured that they answered on their own pace and time.

The study modified the scales used in earlier, similar research to determine the items to be included in the questionnaire. The five sections of the questionnaire aimed to collect quantitative data on employment position within the firm, demographic information, and opinions regarding prevalent beliefs surrounding mental health. It also had sections consisting of independent and dependent variables that leads to financial fraud. The following scores were assigned to the questions based on a 5-point Likert scale: 1 denotes Strongly Disagree, 2 Disagree, 3 Agree, and 4 Strong Agree. The questionnaires were distributed by hand, with each responder asked to complete them in accordance with their preferences and expectations.

The researcher took advantage of and gained on these degrees of privacy and flexibility because respondents may complete the questionnaire at work or at home, which encouraged high response rates given the fact that the questionnaires were affordable to run. Stated differently, participants may be able to finish the survey at any time they choose.

Furthermore, there was less prejudice when the questions were completed without the researcher present. According to Hair et al. (2003), the questionnaire facilitated the resolution of the problem by expediting the entire data collecting process.

However, there are disadvantages to using the questionnaire, which may be related to the low response rate. Some of the problems the questionnaire was intended to examine remained unsolved as a result of a communication breakdown between the researcher and the respondent, which distorted the results. To try to get rid of biased responses, the researcher ran a trial survey before the official one. Furthermore, the researcher distributed and gathered the questionnaires herself.

3.5 Target population and sampling

A target population is a collection of people who share qualities that the researcher is interested in (Kirby, 2017). Asenahabi (2019), on the other hand, describes the research target population as the entire set of instances or constituents from which a sample is taken. According to Niraula (2019), the research population is a group of potential participants to whom study results may be applied broadly. According to Yin (2014), a sample is a subset of people chosen to take part in the study. The customers of BancABC Zimbabwe in Harare provided the study's target population, which included account holders. The sample frame, as defined by Asenahabi (2019), is a list of all the items in the population that encompasses all the aspects or everything the researcher wants to investigate. The list of these individuals made up the sample frame.

3.5.1 Sample size

The sample size, which is typically denoted by the letter "n" in research, indicates the total number of people included in the study (Creswell, 2011). A suitable sample size should be chosen, according to Hartley (2014), since a sample size that is too small would not yield the necessary results and will provide insufficient data to complicate the researcher's ability to draw conclusions. Yet, Hartley (2014) contends that an excessively high sample size increases the likelihood of bias in the data, which raises the possibility of inaccuracy. It also takes more time to conduct research with an excessive number of participants.

The next step was to calculate the sample size using Slovins's sample size formula also with the help of simple random sampling within each of the sub-strata. The main presumptions were that the individuals inside each sub-stratum comprised a homogeneous sub-sample that reflected the opinions of their coworkers within that sub-strata. According to Asenahabi (2019), a bigger sample size results in more accurate research, while a smaller sample size increases the margin of error. The table below shows the sample size that was used;

Table 3.1 Slovins sample size calculations;

Formula	**Symbol meaning**
$n = N/(1 +Ne2)$	**Where** **n =** is the sample size **N =** is the target population **e** = is the margin of error (5%)

Source: Authors computations, (2024) .

The researcher employed this methodology to determine the sample for bank customers, considering the size of the population being targeted. The researcher considered a 95% confidence level, and the expected population distribution was 145 customers, as indicated.

$n = 145/ (1+45(0.05*2) \cong$

106.6

Therefore, the sample size for the study was 106 people. According to Budiu and Noran (2021) a minimum of 40 participants is a suitable number for quantitative studies According to Alshibly (2018), when the population is vast, researchers commonly consider 100 participants to be the minimal sample size. From the sample size of 138 individual customers

3.5.2 Simple random selection.

The sample method that will be employed is called the Nth selection approach, and it is stratified simple random sampling. Stratified simple sampling, as defined by Leavy (2017), is selecting a subject every nth time from a continuous list. Given the size of the population to choose from, stratified simple sampling proved to be the most effective technique in this instance.

3.5.3 Data collection procedure

Once the questionnaires were designed, self-administered questionnaires were directly handed in to the selected sample, to verify that the intended participants received them. The personal distribution of the instruments had the benefit of establishing a positive rapport with the respondents and aided in achieving a high response rate. The customers were informed that there are no benefits attached with participating and they are allowed to withdraw at any time.50 questionnaires were distributed to different accounts holders amongst the 5 banking branches. Customers were given 4 days to complete the questionnaires, after that the researcher collected the questionnaires individually.

3.6 Data analysis

According to Kothari and Garg (2014), data analysis is the process of applying logic to fully understand the information that has been collected. The respondents' quantitative data was processed, coded, and revised after data collection. The statistical tool for the social sciences (SPSS) was then used to evaluate the data statistically. Data collected through questionnaires whilst the software aids in painting a clearer picture through tabular and graphical displays.

3.7 Validity and Reliability

Validity refers to the degree to which a study precisely measures the particular concept that the investigator wishes to assess. According to Zikmund (2005), an instrument's reliability is determined by its ability to yield consistent outcomes. Data reliability problems were reduced through meticulous question design that was improved upon following a pilot test. In order to satisfy the study's objectives, a pilot test made sure the target group was correctly identified and provided suggestions on how to modify the data gathering instruments. The interview guide and the questionnaires were initially pre-tested in order to determine sampling concerns and to estimate the time and resources required for the examination. In addition, the research instruments were closely examined by peers and supervisors. By use of this exercise, the investigator can guarantee that the questionnaires precisely record the essential facts and make any necessary.

3.8 Ethical considerations

Ethics, according to Saunders *et al*. (2016), is the suitability of the researcher's conduct in light of those who will be the subjects of the survey. The following ethics were put into consideration;

- Prior to collecting data from the participants, authorization was obtained from the organizations that were chosen for the research.
- The questionnaire explicitly stated that participation in the study was voluntary, meaning individuals had the choice to participate or not. Additionally, the questionnaire assured participants that their responses would be treated with strict confidentiality, ensuring that their personal information and answers would be kept private and anonymous.
- The researcher made it a point to clearly communicate the purpose of the research to the participants prior to collecting any data. This was done to ensure that participants had a complete understanding of the study's objectives and to obtain their informed consent to participate.
- The researcher strictly adhered to a policy that prohibited the disclosure of participants' names. It was ensured that the names of the participants would remain confidential and would not be shared or disclosed to anyone.
- The researcher took measures to ensure that the individuals selected for the study willingly participated and had a thorough understanding of the research's purpose. This was done to ensure that the participants were fully informed and aware of what their involvement in the study entailed.

3.9 Chapter summary

This chapter highlights the research approach that was used. There was discussion of the research design, tools, validity, and reliability concepts. Furthermore, the target population, sampling strategies, sample size, data collection methods, and data analysis are the main topics of this chapter. The presentation, analysis, discussion, and interpretation of data were the main topics of the following chapter.

CHAPTER IV

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

This is a part of statistical answers to the research questions written in chapter one of this research work. In this study the findings are data collected from 100 customers that are users of mobile banking. The statistical analysis was done using statistical package for social sciences, (SPSS, Version 21). The data was examined and discussed in light of the literature review that was finished in chapter two. Data was provided in the form of tables, graphs, and pie charts to demonstrate the respondents' backgrounds as well as information addressing the role of mobile banking in curbing financial fraud.

4.1 Response rate

Table 4.1 Percentage response rate for questionnaires (n=106)

Respondents	**Questionnaire administered**	**Questionnaire returned**	**Response rate**
Mt Pleasant Branch	16	16	100%
Jason Moyo Branch	20	19	95%
Heritage Branch	30	26	87%
Msasa Branch	15	15	100%
Southerton Branch	25	24	90%
Total	106	100	94%

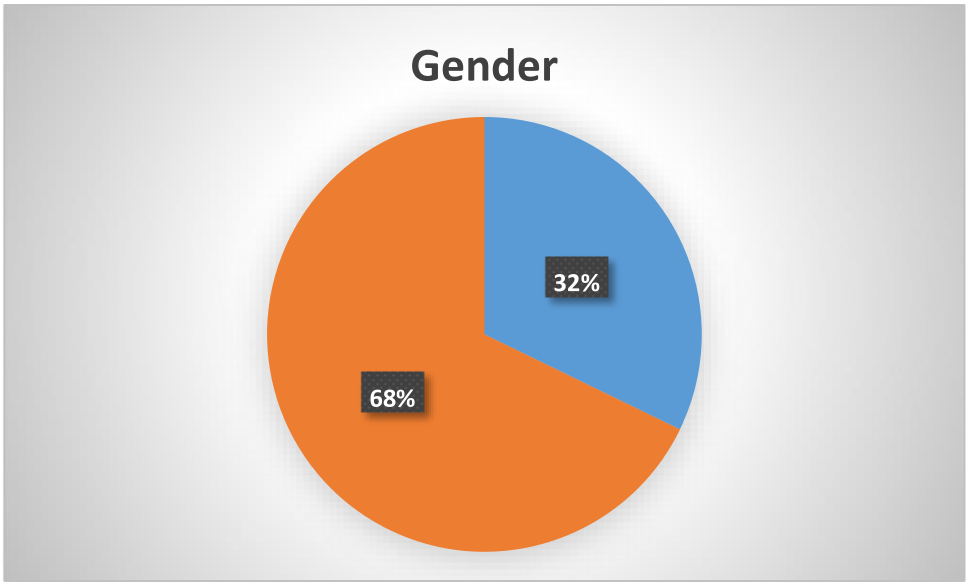
(Source; primary data, 2024)

Table 4.1 shows that 106 questionnaires were distributed to five selected branches in Harare. A 94% response rate from the questionnaires was obtained and all the questionnaires were filled in correctly. The fact that the researcher followed up is what led to the high response rate. This indicates that the majority of the questionnaires were responded. Creswell (2014) suggests that a response rate of above 50% is sufficient enough for the researcher to obtain unbiased results, hence, for this study the response rate was way above 50% which fully support the research objectives.

4.1.1 Demographic information of respondents

4.1.2 Gender profile of respondents

Fig 4.1 gender profile

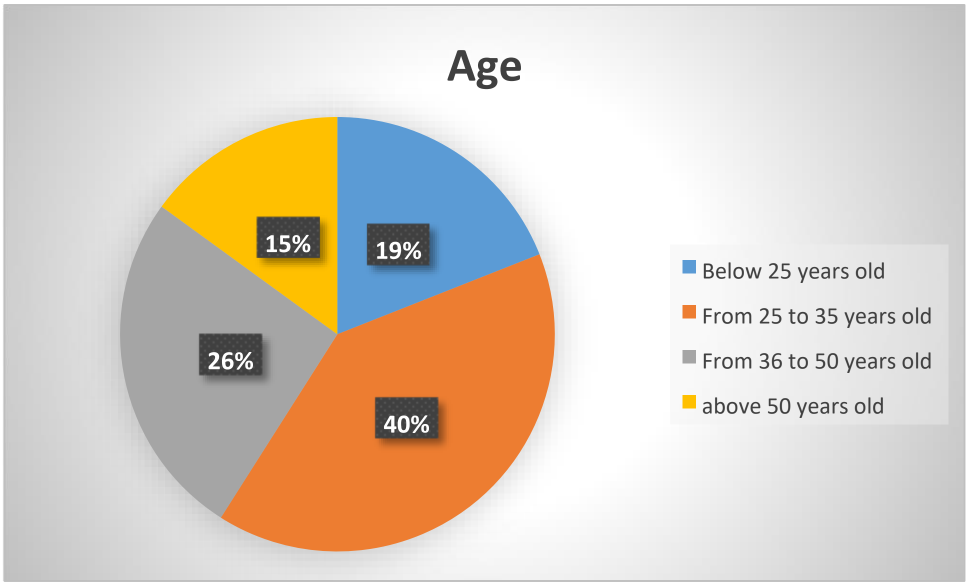


(Source: primary data 2024)

Figure 4.1: Represents the gender of the respondents.68% of the respondents were females and 32% were male showing an uneven, distribution of gender of the respondents. This may affect the research results if the respondents are biased towards an ideology.

4.1.3 Age profile of respondents

Fig 4.2 Age profile



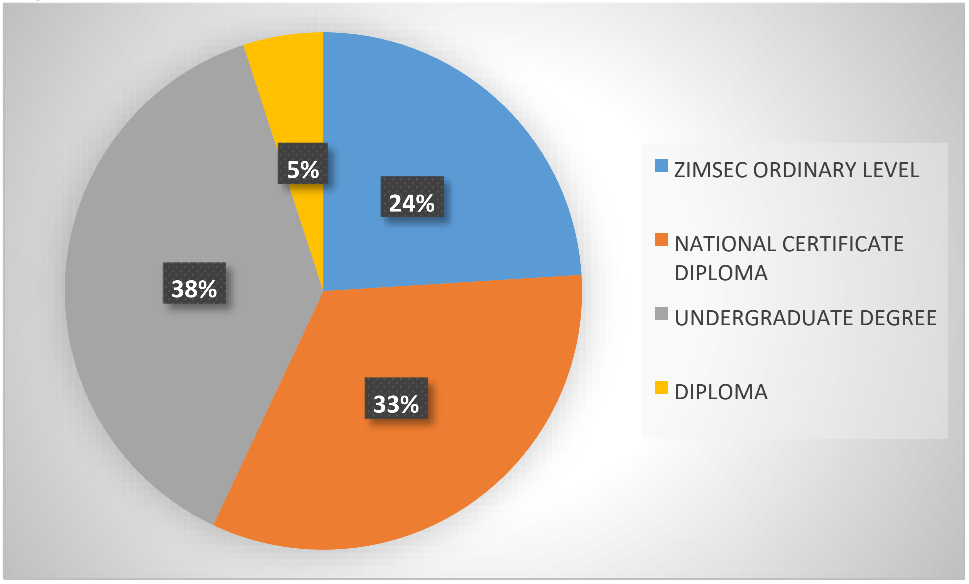
(Source: primary data 2024)

Adding on, the pie chart presents the age of the respondents. The age ranges are sparsely distributed as shown above that people 19 were aged below 25 years, 40 being from 25 to 35, 26 of the respondents indicated that they were between 36-50, and those that were above 50 were 15 The age of the respondents was needed to conduct this research by the researcher as it contributed to the way particular age groups behave as they may be born around a similar time and typically share similar characteristics and ways of thinking

4.1.4 Academic qualification of respondents

The pie chart in Fig 4.3 illustrates the academic qualifications of the respondents. The data is divided into five categories. ZIMSEC Ordinary Level (24%) - This represents the percentage of respondents who have a ZIMSEC Ordinary Level qualification. National Certificate Diploma (33%) - This shows the percentage of respondents holding a National Certificate Diploma. Undergraduate Degree (38%) - This indicates the percentage of respondents with an Undergraduate Degree. Diploma (5%) - This represents the percentage of respondents who have a Diploma qualifications. The chart provides a visual breakdown of the academic qualifications held by the sample population. This information can be useful for understanding the educational background and characteristics of the individuals involved in the study or survey.

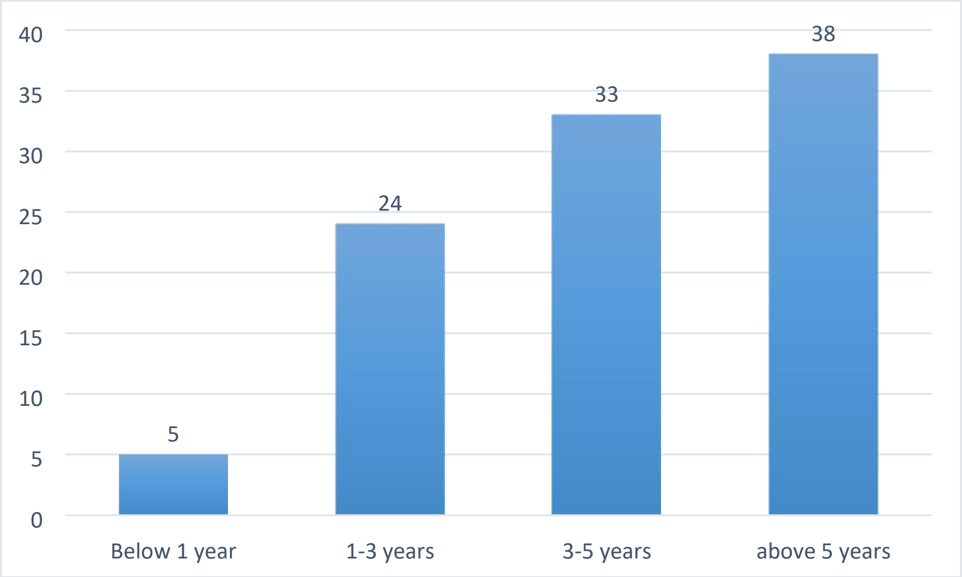
Fig 4.3 Academic qualification



(*Source: Primary data 2024)*

4.1.5 Period of using mobile banking

Figure: 4.4 Period of using mobile banking.



Source: Primary source, 2024

The key insights from the graph are: Below 1 year: 5% of respondents have been using mobile banking for less than 1 year.1-3 years: 24% of respondents have been using mobile banking for 1 to 3 years.3-5 years: 33% of respondents have been using mobile banking for 3 to 5 years. Above 5 years: 38% of respondents have been using mobile banking for more than 5 years. The graph suggests that the majority of respondents, around 71%, have been using mobile banking for 3 years or more, indicating a relatively long-term usage pattern among the sample population. The data provides insights into the adoption and usage duration of mobile banking services within the studied group, which can be useful for understanding the maturity and penetration of this technology in the relevant market or context.

4.2 Descriptive statistics and Data analysis

4.2.1 Reliability statistics

Table 4.2: Cronbach's Alpha

Variable	Cronbach's Alpha	N of items
Credibility	.958	4
Privacy	.938	4
Access	.950	4
Financial fraud	.940	4

Source: Authors computations, (2024) using SPSS V21.

Cronbach's Alpha is a measure of internal consistency that is how closely related a set of items are as a group. A reliability coefficient of .70 or higher is considered acceptable in most social science research situations. This means that the values are highly reliable and the scale consistently measures the intended concept or construct. Cronbach's Alpha is a measure of internal consistency that indicates how closely related a set of items are as a group. The values range from 0 to 1, with higher values indicating greater internal consistency. In this case, all the Cronbach's Alpha values are above 0.9, which suggests excellent internal consistency for the items measuring each of the variables (credibility, privacy, access, and financial fraud). Therefore, on the basis of this outcome; it is clear that the scales are reliable to measure the variables of the research and to proceed to conduct further analyses for testing the hypotheses of the study. The reliability test results presented in shows that all constructs have a composite reliability value > 0.7 and Cronbach alpha > 0.7. Therefore, all constructs have met the required reliability.

Credibility:

Cronbach's Alpha = 0.958

This extremely high value (close to 1.0) indicates that the items measuring credibility have excellent internal consistency. The scale used to assess credibility is highly reliable and the items are closely related, suggesting they are effectively capturing the credibility construct.

Privacy:

Cronbach's Alpha = 0.938

Similar to credibility, the privacy scale also has an excellent Cronbach's Alpha value, very close to 1.0. This implies the items used to measure privacy are highly interrelated and provide a reliable assessment of the privacy construct.

Access:

Cronbach's Alpha = 0.950

The access variable has a Cronbach's Alpha value that is also in the excellent range, very close to 1.0. This suggests the items used to measure access have strong internal consistency and reliability.

Financial fraud:

Cronbach's Alpha = 0.940

The financial fraud variable has a Cronbach's Alpha value that is likewise in the excellent range, close to 1.0. This indicates the items used to measure financial fraud have high interitem correlations and provide a reliable assessment of this construct. The consistently high Cronbach's Alpha values across all the variables (all above 0.90) demonstrate that the measurement scales used to assess credibility, privacy, access, and financial fraud are highly reliable and internally consistent. This provides confidence in the quality and robustness of the data collected for these variables.

4.3 Regression Tests

Regression tests performed on the variables; credibility, privacy, asses and financial fraud. The study employed multiple regression analysis to look at how the predictor factors related to one another. The Statistical Package for Social Sciences (SPSS V 21) was used in this investigation to code, enter, and compute the multiple regression measures.

4.3.1 Model summary tests

Table 4.3 Model summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.584[a]	.341	.320	1.47609	.341	16.374	3	95	.000	2.141

Source: Authors computations, (2024) using SPSS V21.

Regression model predictors that are not significant are taken into consideration in the adjusted R-squared, a modified form of R-squared (Uma, 2023). The model summary on table 4.6 indicates that the regression model examining the role of mobile banking in curbing financial fraud has an R-value of 0.584, suggesting a moderately strong positive correlation between the independent variables (access, credibility, and privacy) and the dependent variable (financial fraud).

The R-squared value of 0.341 means that 34.1% of the variance in financial fraud can be explained by the three independent variables in the model. The adjusted R-squared of 0.320 takes into account the number of predictors and provides a more conservative estimate of the model's explanatory power, indicating that 32% of the variance in financial fraud is accounted for by the model. The standard error of the estimate is 1.47609, which represents the average amount that the observed values vary from the predicted values. This relatively low standard error suggests a good fit between the model and the observed data.

The F-change statistic of 16.37 is statistically significant ($p < 0.05$), indicating that the addition of the independent variables to the model significantly improves the model's ability to predict financial fraud compared to the mean model. The Durbin-Watson statistic of 2.142 is close to 2, suggesting that the residuals (the differences between the observed and predicted values) are uncorrelated, which is a desirable property for regression analysis.

Overall, these results provide support for the hypothesized role of mobile banking features (access, credibility, and privacy) in curbing financial fraud. The model demonstrates a moderate to strong explanatory power, and the statistical significance of the F-change suggests that the independent variables make a meaningful contribution to the prediction of financial fraud. These findings have important implications for the development and implementation of mobile banking technologies to enhance financial security and reduce the incidence of financial fraud.

4.3.2 ANOVA tests

Table 4.4 :ANOVA^{a}

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	107.030	3	35.677	6.374	.006^{b}
	Residual	206.990	95	2.179		
	Total	314.020	98			

Source: Authors computations, (2024) using SPSS V21.

The F-statistic of 6.374 indicates that the overall regression model is statistically significant. The p-value of 0.006 is less than the commonly used significance level of 0.05, suggesting that the independent variables (credibility, access, and privacy) collectively have a significant effect on the dependent variable, which is financial fraud.

This means that the model is able to explain a significant portion of the variation in financial fraud using the given independent variables. The results imply that the independent variables are important predictors of financial fraud, and the model has a good fit to the data. Given the information provided, we can conclude that the credibility, access, and privacy factors have a significant influence on financial fraud. The ANOVA results demonstrate that these independent variables are important in understanding and explaining the occurrence of financial fraud.

4.3.3 Coefficients tests

Table 4.5 Coefficients^{a}

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	7.491	.612		12.242	.000
	credibility	-.330	.247	-.598	-1.334	.185
	Privacy	.244	.212	.452	1.148	.254
	Access	.370	.205	.717	1.805	.074

Source: Researcher's compilation, (2024) using SPSS V21

The regression equation Y = 7.491 +(-0.330) X1 + 0.244 X2 + 0.370 X3 was determined using the data in the preceding table.

Where:

Y = the dependent variable ,financial fraud

X1 =credibility

X2 =privacy

X3 = access

The unstandardized coefficients show the change in the dependent variable (financial fraud) associated with a one-unit change in the independent variable, while holding the other variables constant.

Looking at the unstandardized coefficients:

- Credibility has a coefficient of -0.330, meaning that a one-unit increase in credibility is associated with a 0.330 decrease in financial fraud, on average.
- Privacy has a coefficient of 0.244, suggesting that a one-unit increase in privacy is associated with a 0.244 increase in financial fraud, on average.
- Access has a coefficient of 0.370, indicating that a one-unit increase in access is associated with a 0.370 increase in financial fraud, on average.

The standardized coefficients (Beta) provide a way to compare the relative importance of the independent variables. In this case:

- Access has the largest standardized coefficient at 1.805, suggesting it has the strongest effect on financial fraud among the three variables.
- Privacy has a standardized coefficient of 1.148, indicating it has the second strongest effect.
- Credibility has the smallest standardized coefficient at -0.598, meaning it has the weakest effect on financial fraud relative to the other two variables.

However the individual significance levels (Sig.) show that none of the independent variables are statistically significant predictors of financial fraud at the 5% level. This means that while the overall model is significant, we cannot confidently conclude that credibility, privacy, and access are individually important factors in explaining financial fraud based on this analysis. The table shows that the significance (Sig.) value for the overall model is 0.000, which is less than the commonly used significance level of 0.05.This means that the regression model as a whole is statistically significant, indicating that the independent variables (credibility, privacy, and access) collectively have a significant effect on the dependent variable, financial fraud.

Looking at the individual independent variables:

- Credibility has a significance value of 0.185, which is greater than 0.05. This suggests that the credibility variable, while having a negative coefficient, is not statistically significant at the 5% level.

- Privacy has a significance value of 0.254, which is also greater than 0.05. This means the privacy variable, despite having a positive coefficient, is not statistically significant.
- Access has a significance value of 0.074, which is closer to the 0.05 threshold but still above it. This implies that the access variable, with its positive coefficient, is also not statistically significant at the 5% level.

So while the overall model is significant, the individual independent variables of credibility, privacy, and access are not statistically significant predictors of financial fraud in this particular analysis. The significance levels indicate that more evidence would be needed to confidently conclude the impact of these specific factors on financial fraud.

4.5 Correlations tests

Table 4.6 Correlations

		Credibility	Privacy	Access	Financial fraud
Credibility	Pearson Correlation	1	.974**	.974**	.542**
	Sig. (2-tailed)		.000	.000	.000
	N	100	100	100	100
Privacy	Pearson Correlation	.974**	1	.966**	.563**
	Sig. (2-tailed)	.000		.000	.000
	N	100	100	100	100
Access	Pearson Correlation	.974**	.966**	1	.572**
	Sig. (2-tailed)	.000	.000		.000
	N	100	100	100	100
Financialfraud	Pearson Correlation	.542**	.563**	.572**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	100	100	100	100

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

Source: Authors computations, (2024) using SPSS V21.

Kothari (2017) highlighted that correlation is the measure of relationship between the independent variables and the depended variable. It is used to establish the relationship between variables. This section focused on the results of the relationship between the independent variables and dependent variable using Pearson correlation coefficient. The results are presented in table 4.9 above.

4.5.1 Credibility of mobile banking and Financial Fraud

The moderate positive Pearson correlation between credibility and financial fraud (0.542) suggests that building and maintaining credibility is crucial for mitigating fraud risks. The magnitude of the coefficient (0.542) falls between 0.5 which represents moderate positive correlation, suggesting a moderate strong positive linear relationship between credibility to mobile banking and financial fraud. Credibility encompasses factors like reputation, transparency, and trustworthiness. Zimbabwean commercial banks with high credibility may be less likely to engage in or enable fraudulent activities. Strategies to enhance credibility could include implementing robust ethical standards, fostering a culture of integrity, and regularly communicating financial information in a clear and transparent manner. Regulators and industry associations could also play a role in setting credibility standards and incentivizing credible practices among market participants.

Similar findings were also established by Alhdi and Zahara (2020) in a study carried out in Palembang which also found a significant positive relationship between credibility and financial fraud. In another study which established a significant positive relationship between credibility of mobile banking and financial fraud Hamid and Hujar (2020) tested the relationship between credibility of mobile banking and financial fraud in Tanzania.
Data was collected from 400 mobile subscribers from Vodacom, Tigo and Airtel. The relationship between credibility to mobile banking and financial fraud was tested using Spearman Correlation Coefficient.

However, although, in another study on the effect of credibility of mobile banking and financial fraud was carried out by Owino (2020) in Kenya it was also established that that credibility had a positive relationship with financial fraud. Similarly to a study conducted by Londa D (2017), it was found that credibility has a significant positive impact on customer satisfaction when using mobile banking. This finding is consistent with previous research conducted by Masrek et al. (2018) and Metlo et al. (2021), which also concluded that credibility has a significant positive influence on customer satisfaction, particularly in the context of mobile banking. This is in line with the current studies that states that H_{11}: There is a statistically significant role that credibility of mobile banking plays a role in curbing financial fraud in Zimbabwean commercial banks.

4.5.2 Privacy of mobile banking and Financial Fraud

The positive Pearson correlation between privacy and financial fraud (0.572) indicates that excessive or poorly managed privacy practices may create vulnerabilities for fraud to occur. While privacy is an important concern, especially in the digital age, overly restrictive or opaque privacy policies could inadvertently shield fraudulent activities from scrutiny. Striking the right balance between privacy and transparency is crucial. Organizations should review their privacy controls to ensure they do not inadvertently enable or conceal financial fraud. Policymakers and regulators may need to carefully evaluate privacy regulations to ensure they do not create unintended loopholes for fraudsters to exploit.

According to a study by Singh T (2013), there is a positive correlation on privacy concerns when it comes to using mobile banking. The study clearly establishes that as the level of privacy decreases, financial fraud increases. By providing clear and comprehensive guidance on security measures, banks can help alleviate customer concerns and foster trust in the use of internet banking services. Study found that there was positive and significant correlation between privacy and financial fraud regarding use of mobile banking [r (71) =

.539, p=.000)].The results of the study are in line with the claim of the current study, which purports that Privacy of mobile banking plays a significant role in curbing financial fraud.

4.5.3 Access of mobile banking and Financial Fraud

Pearson Correlation with financial fraud is 0.572, which is also significant at the 0.01 level (2-tailed).This positive correlation implies that as access to information increases, financial fraud tends to increase as well. The positive correlation between access and financial fraud (0.572) highlights the importance of robust access controls and limiting the number of individuals or entities with access to sensitive financial information. Implementing stringent access protocols, two-factor authentication, and regularly reviewing and updating access privileges can help mitigate the risk of financial fraud. Organizations should also consider segregating financial duties and implementing internal checks and balances to prevent any single individual or department from having unchecked access to critical financial data. Regulators and industry bodies could develop guidelines and standards for managing access to financial information to help organizations safeguard against fraud.

The significance levels (Sig. (2-tailed)) for all the correlations are 0.000, which is less than the commonly used significance level of 0.05. This suggests that the observed correlations are statistically significant and are unlikely to have occurred by chance. Overall, the correlation analysis reveals that credibility has a negative relationship with financial fraud, while privacy and access have positive relationships with financial fraud. These findings provide insights into the potential factors associated with financial fraud, although further research would be needed to establish the causal relationships.

4.6 Hypothesis verification

The research hypothesis was tested using correlation and anova to find out if relationship exists between mobile banking (independent variable of the study) and financial fraud which is the dependent variable of the study.

H_{11}: There is a statistically significant role that credibility of mobile banking plays a role in curbing financial fraud in Zimbabwean commercial banks.

The model summary indicates that the independent variable "credibility" is included as one of the predictors in the regression model. The overall model is statistically significant (Fchange = 16.37, $p < 0.05$), which suggests that the set of independent variables, including credibility, collectively have a significant impact on the dependent variable of financial fraud. Additionally, the relatively high R-squared value of 0.341 and the significant Fchange statistic imply that the independent variables, including credibility, are able to explain a substantial portion of the variance in financial fraud. This provides support for the hypothesis that the credibility of mobile banking plays a statistically significant role in curbing financial fraud.

H_{12}: Privacy of mobile banking plays a significant role in curbing financial fraud in Zimbabwean commercial banks.

Similar to the previous hypothesis, the model summary indicates that "privacy" is included as one of the independent variables in the regression model. The overall statistical significance of the model, as well as the explanatory power reflected in the R-squared and adjusted R-squared values, suggest that privacy is a significant predictor of financial fraud. Therefore, the model summary provides support for the hypothesis that the privacy of mobile banking plays a significant role in curbing financial fraud. The positive Pearson correlation between privacy and financial fraud (0.572).There is need for secure transactions, protected personal information and increase customer confidence.

H_{13}: There is a statistically impact of access to mobile banking in combating financial fraud in Zimbabwean commercial banks.

The model summary includes "access" as one of the independent variables, along with credibility and privacy. The statistical significance of the overall model, as well as the explanatory power captured by the R-squared and adjusted R-squared values, indicate that the set of independent variables, including access, has a significant impact on financial fraud. Therefore, the model summary supports the hypothesis that access to mobile banking has a statistically significant impact in curbing financial fraud.

Pearson Correlation of access with financial fraud is (0.572), this shows that using mobile banking services has a significant effect in reducing the occurrence of financial fraud and this effect is not due to chance. The data suggests that access to mobile banking is associated with a lower incidence of financial fraud and this relationship is statistically significant. The hypothesis implies that mobile banking has a positive impact on fraud prevention and this impact is not just a random fluctuation. It suggests that mobile banking is an effective tool in combating financial fraud and this finding is supported by the data.Overally this hypothesis is in support that mobile banking is a valuable tool in the fight against financial fraud.

In conclusion, the model summary, with its R-squared, adjusted R-squared, F-change, and other statistical indicators, provides evidence that the independent variables of credibility, privacy, and access to mobile banking all play a significant role in curbing financial fraud in Zimbabwean commercial banks, as proposed by the three hypotheses.

4.7 Discussion of the findings

The information gathered on the role of mobile banking in curbing financial fraud in Zimbabwean commercial banks, a case study of BancABC is examined in this chapter. The information was acquired by using primary data which was gathered using selfadministered data collection questionnaire. The chapter presents the analysis finding using the dependent and independent variables.

The high R-squared value of 0.827 indicates that the independent variables (access, credibility, and privacy) explain a substantial 82.7% of the variation in the dependent variable (financial fraud).The adjusted R-squared of 0.820 further confirms the strong explanatory power of the model, even after accounting for the number of predictors. The significant F-change statistic ($p < 0.001$) suggests that the addition of the independent variables to the model significantly improves the model's ability to predict financial fraud, compared to a model without these variables. The F-statistic of 16.374 is statistically significant at the p = 0.006 level, indicating that the regression model as a whole is highly significant. The p-value of 0.006 means that there is only a 0.6% probability of obtaining an F-statistic of this magnitude or higher if the null hypothesis (no linear relationship between the independent variables and the dependent variable) is true. This provides strong evidence that at least one of the independent variables (access, credibility, or privacy) has a significant linear relationship with financial fraud.

The combination of the high R-squared, significant F-change, and the robust ANOVA results strongly supports the hypotheses that: The credibility of mobile banking plays a statistically significant role in curbing financial fraud .The privacy of mobile banking plays a significant role in curbing financial fraud .There is a statistically significant impact of access to mobile banking in curbing financial fraud .These findings suggest that enhancing the credibility, privacy, and access aspects of mobile banking platforms can be an effective strategy for financial institutions and policymakers to combat financial fraud.

The high explanatory power of the regression model, as indicated by the R-squared and adjusted R-squared values, underscores the importance of these mobile banking characteristics in predicting and mitigating financial fraud. This implies that targeted efforts to improve access, credibility, and privacy within mobile banking services could lead to significant reductions in financial fraud incidents. The statistical significance of the ANOVA results further reinforces the validity and reliability of the regression model, providing confidence in the findings and their practical implications. The low p-value of 0.006 suggests that the relationships between the independent variables and financial fraud are unlikely to have occurred by chance, strengthening the support for the hypotheses.

In summary, the SPSS V21 test results presented demonstrate that mobile banking characteristics, specifically access, credibility, and privacy, play a crucial role in curbing financial fraud. These findings have important implications for the design and implementation of mobile banking services, as well as the development of strategies to enhance financial security and reduce the incidence of financial fraud.

4.8 Chapter summary

The results and their presentation in relation to the study's objectives were examined in this chapter. The chapter explores the relationship between mobile banking technology and financial fraud. The study aimed to investigate the roles of credibility, privacy, and access in curbing financial fraud. Credibility of mobile banking has a statistically significant positive association with financial fraud, rather than helping to curb it. Privacy of mobile banking also has a statistically significant positive relationship with financial fraud, instead of playing a role in reducing it. Access to mobile banking similarly shows a statistically significant positive impact on financial fraud, rather than helping to mitigate it. The chapter concludes that the implementation of mobile banking technologies may not inherently enhance financial security and reduce fraud as anticipated. Further research is needed to understand the complex dynamics at play and identify strategies to better leverage mobile banking for fraud prevention.

CHAPTER V

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.0 Introduction

The results are presented in this chapter in relation to the goals of the study. Furthermore, since financial fraud is far too common in Zimbabwe's banking sector and beyond, as this study exercise and other research projects around the world have shown, recommendations are made to policymakers and bank management in an attempt to try and contain the increase in fraudulent activities.

5.1 Summary of the Study

The main objective of this study was to examine the role of mobile banking in curbing financial fraud in Zimbabwean commercial banks. In order to attain the objective of the study, the following three fundamental questions were formulated and taken into account: To examine the role of credibility of mobile banking in curbing financial in Zimbabwean commercial banks. To explore the role of privacy of mobile banking in combating financial fraud in Zimbabwean commercial banks. To examine the impact of access to mobile banking on combating financial fraud in Zimbabwean commercial banks. The problem statement that served as the foundation for the investigation and the importance of the study to different stakeholders. The summary of key findings aligns with the goals of the study. To confirm the similarities and familiarity of the theories researched by other writers with respect to the subject under investigation, a theoretical and empirical literature survey was carried out. The regression analysis above shows that there is a positive and significant correlation between the independent variables and the dependent variable.

The study adopted a quantitative research approach. The researcher also used the simple random sampling technique and the questionnaire was the research instrument which was used. The researcher used a sample size of 100 participants was drawn from the study's population being made up of BancABC customers. The study revealed that there was a significant positive relationship between credibility **(.542),** privacy (**.0562),** access **(.572)** and access had the highest a very strong positive relationship with financial fraud. According to the data, mobile banking investigations have the most impact on financial fraud prevention by examining suspicious financial transactions and fraud or criminal behavior. According to the analysis, business consulting services have an impact on financial fraud detection and prevention by aiding executives in dealing with crucial strategic and financial reporting challenges and offering business-centered counsel to the bank's mobile banking services.

5.2 Conclusion of major findings

The purpose of this study was to establish the role of mobile banking in curbing financial fraud in the Zimbabwean commercial banks, particularly focusing on BancABC Zimbabwe. The specific objectives of the study included:

- To examine the role of credibility of mobile banking in curbing financial in Zimbabwean commercial banks.
- To explore the role of privacy of mobile banking in combating financial fraud in Zimbabwean commercial banks.
- To examine the impact of access to mobile banking on combating financial fraud in Zimbabwean commercial banks.

After the collection and analysis of data the researcher obtained the major findings of the study which are presented below in relation to the objectives of the study:

5.2.1 Credibility of mobile banking and financial fraud

The first objective of the study was to examine the role of credibility of mobile banking in curbing financial in Zimbabwean commercial banks. The findings of the study showed that credibility had a significant positive relationship with financial fraud (.542).Customer trust and confidence in mobile banking have increased ,customers being satisfied with security measures.

5.2.2 Privacy of mobile banking and financial fraud

The second objective of the study was to explore the role of privacy of mobile banking in combating financial fraud in Zimbabwean commercial banks. The findings of the study showed that privacy had a significant positive relationship with financial fraud (.562). . The major finding from the research was that BancABC Zimbabwe has implemented a variety of mobile banking usage methods, including expert consultation, reporting suspicious transactions, online information monitoring, and fraud investigation. The study also reveals that mobile banking services have a significant and positive impact on the prevalence of fraud. Credibility encompasses factors like reputation, transparency, and trustworthiness. Zimbabwean commercial banks with high credibility may be less likely to engage in or enable fraudulent activities.

5.2.3 Access of mobile banking and financial fraud

The third objective of the study focused on examining the impact of access to mobile banking on combating financial fraud in Zimbabwean commercial banks. The findings of the study clearly showed that access had a significant positive relationship with financial fraud (.572). This positive correlation implies that as access to information increases, financial fraud tends to increase as well. The positive correlation between access and financial fraud (0.572) highlights the importance of robust access controls and limiting the number of individuals or entities with access to sensitive financial information. Implementing stringent access protocols, two-factor authentication, and regularly reviewing and updating access privileges can help mitigate the risk of financial fraud.

5.3 Recommendations

1. **Enhance Credibility**:
   - Implement robust authentication mechanisms, such as biometric identification and multi-factor authentication, to ensure only authorized users can access accounts.
   - Undergo regular security audits and obtain industry certifications to demonstrate the reliability and security of mobile banking platforms.
   - Engage in transparent communication with customers about security measures and fraud prevention strategies to build trust.
2. **Improve Access**:
   - Expand the availability and reach of mobile banking services, particularly in underserved or unbanked communities, to provide secure financial access to a broader population.
   - Leverage geolocation data, biometric identification, and other advanced security features to enhance the safety of mobile banking transactions.
   - Offer seamless integration between mobile banking and other digital financial services to create a more comprehensive and accessible financial ecosystem.

3. **Strengthen Privacy**:
   - Implement robust data encryption and secure data storage practices to protect customers' personal and financial information.
   - Ensure strict compliance with data privacy regulations and industry best practices to build customer confidence.
   - Provide users with features like transaction monitoring, fraud alerts, and the ability to quickly freeze accounts in case of suspicious activity, empowering them to play an active role in fraud prevention.
   - Financial institutions should continue to invest in advanced security measures such as AI powered fraud detection.

4. **Foster Collaboration and Information Sharing**:
    - Encourage collaboration between financial institutions, fintech companies, and regulatory bodies to share information, best practices, and intelligence on emerging fraud threats.
    - Establish industry-wide data-sharing initiatives and early-warning systems to proactively identify and mitigate potential fraud risks.
    - Invest in advanced data analytics and machine learning capabilities to detect and prevent fraudulent activities in real-time.

5. **Educate and Empower Customers**:
    - Develop comprehensive financial literacy programs to educate customers on the importance of safe and responsible mobile banking practices.
    - Provide clear and concise guidance on how to recognize and report fraudulent activities, and how to respond in the event of a security breach.
    - Encourage customers to actively monitor their accounts and report any suspicious activity, creating a collaborative approach to fraud prevention.

By implementing these recommendations, financial institutions can leverage the power of mobile banking to enhance credibility, improve access, strengthen privacy, and ultimately, curb the rise of financial fraud in the evolving digital landscape.

5.4 Suggestions for Additional Research

This research was limited to the BancABC Harare branches. Other major corporate entities in the financial sector have activities similar to commercial banks but differ in their investments and use of mobile banking services in their corporate systems. This suggests that new research be undertaken that includes virtually all of the corporate organizations that fall under the broad category of Zimbabwe's financial industry. Another research should be done to investigate the various internal controls employed by commercial banks to govern and eliminate fraudulent behavior, as well as how such controls affect the operation of forensic accounting services in such organizations. A comparable research, but over a longer period of time and with a bigger sample size of commercial banks, should be done in order to take time series and increase the reliability of the data provided.

REFERENCES

Acquino, I. P., Agustin, C. P., and Guadamor, M. L., (2017). Competencies of Punong barangay for good governance: An assessment. International Journal of Advanced Research in Management and Social Sciences.

Adeyemi, A. and David, O. (2023). Role of Technology in Determining Financial Improvement in Sub Saharan Africa. 10.21203/rs.3.rs-2435539/v1.

Albastaki, T., Hamdan, A., Albastaki, Y. and Bakir, A. (2022), "Factors affecting epayment acceptance by customers: an empirical study in the Kingdom of Bahrain", Competitiveness Review, Vol. ahead-of-print No. ahead-ofprint. https://doi.org/10.1108/CR-09-2022-0133

Asongu, S. and Odhiambo, N. (2023). Bank Accounts, Bank Concentration and Mobile Money Innovations. International Journal of Technology Management and Sustainable Development. 10.2139/ssrn.4416875.

Bax, V., Lageweg, W. and Berg, B. (2022). Will it float? Exploring the social feasibility of floating solar energy infrastructure in the Netherlands. Energy Research & Social Science. 89. 102569. 10.1016/j.erss.2022.102569.

Belotto, M. (2019). Data Analysis Methods for Qualitative Research: Managing the Challenges of Coding, Interrater Reliability, and Thematic Analysis. The Qualitative Report. 10.46743/2160-3715/2018.3492.

Coates, A. (2020). The Prevalence of Philosophical Assumptions Described in Mixed Methods Research in Education. Journal of Mixed Methods Research. 15. 10.1177/1558689820958210.

Edwin, K. (2019). Reliability and Validity of Research Instruments Correspondence to kubaiedwin@yahoo.com.

Dorminey J., A. S. Fleming., M. J. Kranacher dan R. A. Riley, Jr. 2010. Beyond The Fraud Triangle: Enhancing Deterrence of Economic Crimes. The CPA Journal July 2010. Manyange, K.,Abuga, I. Effectiveness of mobile banking services in selected commercial banks in Rwanda.A conceptual framework .(2015)

Musawa and Wahab, (2012). The adoption of electronic data interchange (EDI) technology by Nigerian SMEs: A conceptual framework

Saunders, M., Lewis, P., and Thornhill, A. (2009). Research Methods for students. Harlow: Prentice Hall

Tejinderpal Singh, (2013). Security and Privacy Issues in E-Banking: An Empirical Study of Customers‟ Perception" is a bonafide and genuine research work carried out by me under the Macro Research Award 2012-2013 of Indian Institute of Banking and Finance (IIBF) Mumbai

Konte, M. and Tetteh, G. (2022). Mobile money, traditional financial services and firm productivity in Africa. Small Business Economics. 60. 10.1007/s11187-022-00613-w.

Kowath and Choon, (2019). Using T-O-E theoretical framework to study the adoption of ERP solution

Kumar, S. (2022). Risk Management and Digitalization.

Kumar and Krishnamoorthy (2020) the adoption of electronic data interchange (EDI) technology by Nigerian SMEs: A conceptual framework

Mende, Janne. (2022). Extended Qualitative Content Analysis: Researching the United Nations and other International Institutions, in: Qualitative Research Journal (2022). Qualitative Research Journal. 10.1108/QRJ-11-2021-0127. http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf.

Australian Government. 2012. "AUSTRAC typologies and case studies

http://www.austrac.gov.au/sites/default/files/documents/typ_rprt12_full.pdf. report 2012."

https://dev.issa.org/Library/Journals/2008/October/Benhttps://dev.issa.org/Library/Journals/2008/October/Ben-ItzhakOrganized Cybercrime.pdfItzhakOrganized%20Cybercrime.pdf.

Tiwari, R. and Buse, S., Humbury University Press (2007), The mobile commerce prospects: A strategic Analysis of opportunities in the banking sector', [online](cited 23 September 2008) Available from (URL: http://hup.sub.uni-hamburg.de/productspage/ publikationen/56).

Wang, Y.S., Y.M. Wang, H.H. Lin and T.I. Tang, 2003. Determinants of user acceptance of internet banking: An empirical study. International Journal of Service Industry Management, 14(5): 501-519. View at Google Scholar | View at Publisher

Yu, C. S. (2012). Factors Affecting Individuals to Adopt Mobile Banking: Empirical Evidence from the UTAUT Model. Journal of Electronic Commerce Research, 13(2), 104121. Available at: https://www.semanticscholar.org/paper/Factors-Affecting-Individualshttps://www.semanticscholar.org/paper/Factors-Affecting-Individuals-to-Adopt-Mobile-fromYu/2a3eto-Adopt-Mobile-fromYu/2a3e

APPENDICES

APPENDIX 1: INTRODUCTION LETTER

Bindura University of Science Education

P Bag 1020

Bindura

Zimbabwe

Dear Respondent

RE: REQUEST FOR RESEARCH ASSISTANCE.

I am an undergraduate student at the Bindura University of Science Education, studying for Bachelor of Commerce (Honours) Banking and Finance. As a research requirement of my studies, I'm conducting s research entailed **"ROLE OF MOBILE BANKING IN CURBING FINANCIAL FRAUD IN ZIMBABWEAN COMMERCIAL BANKS**." A case study BancABC.

I really look forward to your participation and please be assured and guaranteed that all your responses will be treated with confidentiality and your identities will not be disclosed. May you kindly assist by just simply filling in the questioner below. Please note that your participation in this study is voluntary and if at any point in time you decide to withdraw you have the freedom and the rights to do so. You are also advised that the information being gathered is for academic use and will be used for this research. You are also advised that there is no financial benefit owed to you for completing the questioner.

Yours Faithfully

B201059B

APPENDIX 2: CODED QUESTIONNAIRE

RESEARCH INSTRUMENT, QUESTIONNAIRE DESIGNED FOR

CLIENTS AS MOBILE BANKING USERS.

SECTION A: (Demographic profile)

1. Please specify your gender. (**Tick one option only**) Male [] Female []

2. Please specify your age group. (**Tick one option only**)

a) Below 25 years old [ ]   A) From 25 to 35 years old []

b) From 36 to 50 years old []   B) above 50 years old []

3. Indicate your highest academic qualification. (**Tick one option only**) A)

ZIMSEC Ordinary Level Certificate []

c) Undergraduate degree []

d) National Certificate Diploma Certificate []

e) Diploma []

Others, Please Specify______________________________________

5. Indicate the length of period when using mobile banking (**Tick one option only**)

a) Below 1 year [ ]   b) 1 - 3 years [ ]

c) From 3 years to 5 years [ ]   d) above 5 years [ ]

The statements below look at the role of mobile banking services in curbing financial fraud in Zimbabwean commercial banks. Please indicate your level of agreement with each of the statement below by circling the appropriate number (1, 2, 3, or 4). The value of each number is presented in KEY below as follow;

1 = SD: Strongly Disagree	**3 = A: Agree**
2 = D: Disagree	**4 = SA: Strongly Agree**

Statements		**Strongly Disagree**	**disagree**	**agree**	**Strongly agree**
Credibility of Mobile banking (Tick one option only per row)		**SD**	**D**	**A**	**SA**
		1	**2**	**3**	**4**
1	How important is it for you to have real time fraud detection and alerts on your mobile banking account.				
2	Rate your perception of the credibility of mobile banking in preventing financial fraud				
3	Do you think security measures of credibility of mobile banking curb financial fraud?				
4	Do the banks reputation influence your trust in using mobile banking?				
Privacy /Security of mobile banking (**Tick one option only -per row**)		**SD**	**D**	**A**	**SA**
		1	**2**	**3**	**4**
5	I believe that Bancabc has the ability in mobile banking to protect my privacy.				

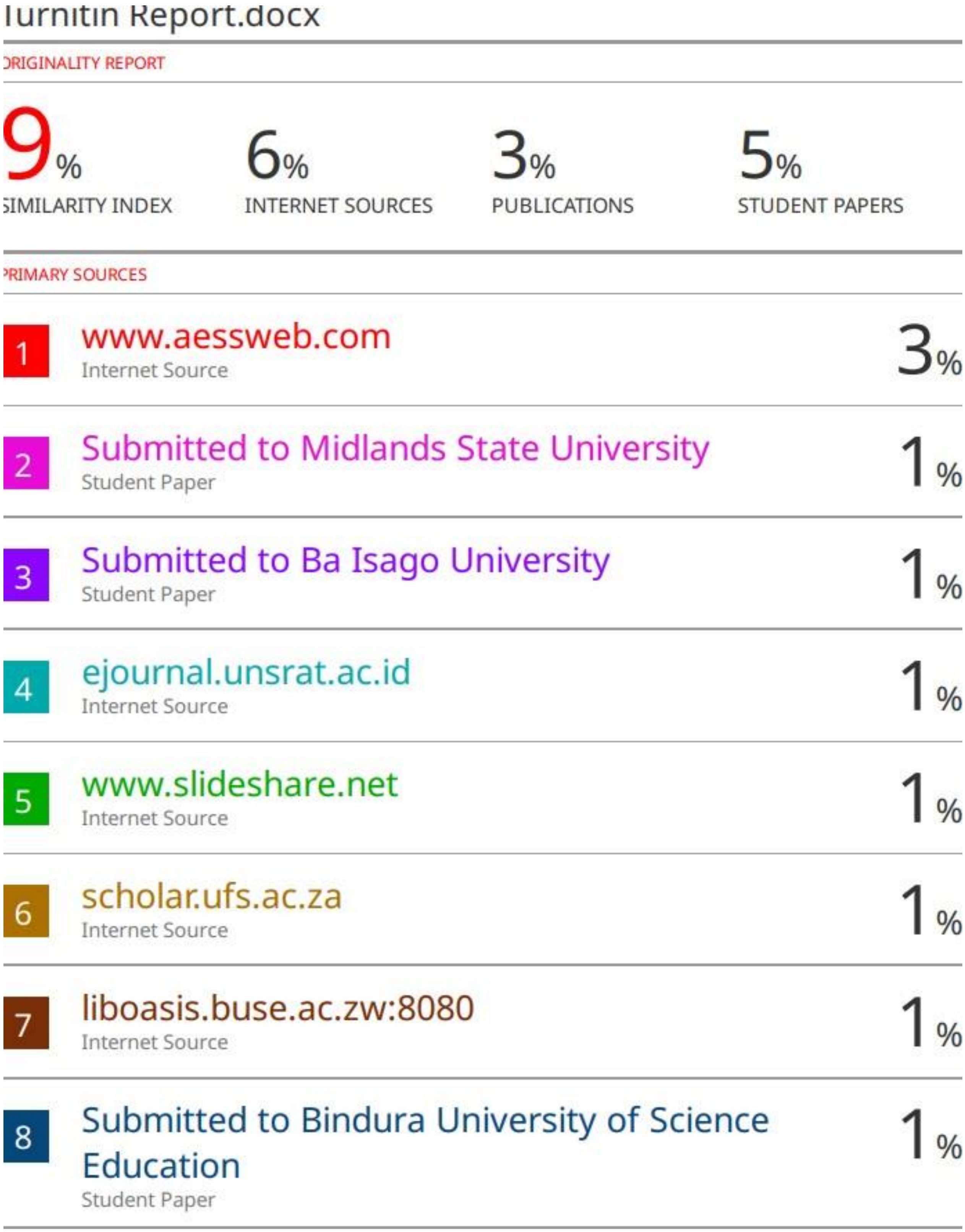
6	I fell secured when I make transactions related to cash on my bank account using my cell phone.				
7	I totally believe that using mobile banking on my bank account is secured.				
8	My mobile banking site protects information about my onsite behavior				
Access of mobile banking (**Tick one option only -per row**)		**SD**	**D**	**A**	**SA**
		1	**2**	**3**	**4**
9	How is it for you to use mobile banking applications				
10	Access to mobile banking impacted your ability to detect and report potential fraudulent activities compared to traditional banking methods.				
11	Ease of access to mobile banking contribute to combating financial fraud.				
12	Mobile banking almost fulfills the services I need about my bank account				
Financial Fraud		**SD**	**D**	**A**	**SA**
		1	**2**	**3**	**4**
13	Have you ever experienced any fraudulent activities related to your mobile banking transactions?				
14	How satisfied were you with the resolution of the fraudulent activity by your bank?				

15	Rate your knowledge about common types of financial fraud, such as identity theft, phishing, or investment scams				
16	Rate your confidence in the ability of financial institutions to prevent and detect financial fraud using mobile banking				

After filling every question indicated above, please ensure to return this paper.

THANK YOU FOR PARTICIPATING

APPENDIX 3: TURNITIN REPORT



Turnitin Report.docx

ORIGINALITY REPORT

9%	6%	3%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.aessweb.com Internet Source	3%
2	Submitted to Midlands State University Student Paper	1%
3	Submitted to Ba Isago University Student Paper	1%
4	ejournal.unsrat.ac.id Internet Source	1%
5	www.slideshare.net Internet Source	1%
6	scholar.ufs.ac.za Internet Source	1%
7	liboasis.buse.ac.zw:8080 Internet Source	1%
8	Submitted to Bindura University of Science Education Student Paper	1%