ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE

CORPORATE FINANCE DEPARTMENT: SPECIALTY IN INVESTMENT MANAGEMENT

THE EFFECT OF DIGITAL BANKING FRAUD ON CUSTOMER SERVICE UTILIZATION

A RESEARCH THESIS SUBMITED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR MSC IN CORPORATE FINANCE SPECIALTY IN INVESTMENT MANAGEMENT

BY:

FEBEN WONDIMU

ADVISOR:

MENGISTU B. (PHD)

JUNE, 2025

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE

CORPORATE FINANCE DEPARTMENT: SPECIALTY IN INVESTMENT MANAGEMENT

THE EFFECT OF DIGITAL BANKING FRAUD ON CUSTOMER SERVICE UTILIZATION

A RESEARCH THESIS SUBMITED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR MSC IN CORPORATE FINANCE SPECIALTY IN INVESTMENT MANAGEMENT

BY:

FEBEN WONDIMU

ADVISOR:

MENGISTU B. (PHD)

JUNE, 2025

ADDIS ABABA, ETHIOPIA

Table of Contents

List of Tables VI
List of Figures VII
List of Abbreviations VIII
Declaration of Authenticity IX
Approval Sheet X
Acknowledgment XI
ABSTRACT XII
CHAPTER ONE 1
Introduction 1
1.1 BACKGROUND OF THE STUDY 1
1.2 STATEMENT OF THE PROBLEM 2
1.3 RESEARCH QUESTION 4
1.3.1 GENERAL RESEARCH QUESTION 4
1.3.2 SPECIFIC RESEARCH QUESTION 4
1.4 OBJECTIVES OF THE STUDY 5
1.4.1 GENERAL OBJECTIVES OF THE STUDY 5
1.4.2 SPECIFIC OBJECTIVES OF THE STUDY 5
1.5 SCOPE OF THE STUDY 5
1.6 SIGNIFICANCE OF THE STUDY 6
1.7 ORGANIZATION OF THE STUDY 7
CHAPTER TWO 8
2.1 Theoretical Literature Review on Fraud 8
2.1.1. Definition of fraud 8
2.1.2. Theories of Fraud 9
2.2.3 Types of fraud 11
2.3.4 Technology and banking 15
2.3.5 Fraud prevention strategy 16
2.2. Empirical Literature Review 17
2.3 Research Hypotheses 22
2.4 Literature Gap 22
2.5 Conceptual Framework 23
CHAPTER THREE 24

Research Methodology 24
3.1 Introduction 24
3.2 Research approach 24
3.3 Research Design 24
3.4 Target Population 25
3.5 Sampling Techniques and Sample Size of the Study 25
3.6 Methods of Data Analysis 26
3.7 Model Specification 27
3.8 Reliability and validity of instruments 28
CHAPTER FOUR 29
DATA PRESENTATION AND ANALYSIS 29
4.1 Introduction 29
4.2 Response Rate of Survey 29
4.3. Demographic profile of Respondents 29
4.3.1 Reason for use of mobile banking 32
4.3.2 Users of Specific digital bank 33
4.3.3 Cross checking of why respondents are using the specific digital banking products of each bank 33
4.3.4 Type of digital banking the respondents are using 35
4.3.5 Which product of digital banking is the respondents are using from each specific Banks 36
4.4 Analysing the effect of fraud in digital banking on customer service utilization 37
4.5 The outcomes of descriptive statistics measures 38
4.5.1 Types of Fraud in Digital Banking 38
4.5.2 Fraud Prevention Measures 39
4.5.3 Customer Awareness 40
4.5.4 Perceived Fraud Risk 42
4.5.5 Fraud Incidents 43
4.5.6 The Effect of Fraud in Digital Banking on Service Utilization 44
4.6 The Relationship between Independent variables and Service Utilization 45
4.7 Results for Assumption of Multiple Regression Analysis 47
4.7.1 Normality Distribution Test 47
4.7.2 Linearity Test 48
4.7.3 Multi-collinearity Test 49
4.7.4 Homoscedasticity 49

4.7.5 Test of Auto-correlation 50
4.8 Regressions Analysis 51
4.9 ANOVA (Analysis of Variance) 52
4.10 Coefficients of Regression Analysis 52
4.11 Hypotheses Testing 54
CHAPTER FIVE 56
SUMMARY, CONCLUSION AND RECOMMENDATION 56
5.1 Introduction 56
5.2 Summary 56
5.3 Conclusion 58
5.4 Recommendation 58
5.5 Limitation of the study 59
5.6 Suggestion for further research 59
Bibliography 60
Appendix A 65

List of Tables

Table 4. 1 Demographics profile of Respondents 30
Table 4. 2 why respondents are using the specific digital banking products of each bank 33
Table 4. 3 product of digital banking customers are using from each specific bank 36
Table 4. 4 Scaled Likert Criterion 38
Table 4. 5 Knowledge of customers about type of digital banking 38
Table 4. 6 Knowledge of customers about fraud prevention measure taken 39
Table 4. 7 The customer awareness about fraud 40
Table 4. 8 customers perceived fraud risk 42
Table 4. 9 Fraud Incident the customers are experiencing 43
Table 4. 10 The Effect of Fraud in Digital Banking on Service Utilization 44
Table 4. 11 coefficient size of correlation 45
Table 4. 12 the relationship between independent variables and Service Utilization 46
Table 4. 13 test of multicollinearity 49
Table 4. 14 Test of Auto-correlation 50
Table 4. 15 model summary 51
Table 4. 16 Test of ANOVA 52
Table 4. 17 Regression Coefficient Analysis of the model 53

List of Figures

Figure 2.1 Conceptual Framework 23
Figure 4. 1 The reason for using digital banking 32
Figure 4.2 Which bank do the users use mostly? 33
Figure 4. 3 Type of digital banking do users are using 35
Figure 4. 4 Test of normality 48
Figure 4. 5 P-P Plot of Regression Standardized Residual 48
Figure 4. 6 Scatterplot of standardized residuals 50

List of Abbreviations

ACH	Automated Clearing House
ATM	Automated Teller Machine
ATS	Automatic Transfer System
BEC	Business Email Compromise
BOA	Bank of Abyssina
CBE	Commercial Bank of Ethiopia
CBN	Central Bank of Nigeria
CE	Customer Experience
CLRM	Classical Linear Regression Model
DSS	Decision Support Systems
ECSIAC	Ethiopian Cyber Security and Information Assurance Center
EPN	Electronic Payment Network
EFT	Electronic Fund Transfer
GST	General Strain Theory
IB	Internet Banking
ICT	Information and Communications Technology
JIBC	Journal of Internet Banking and Commerce
KYC	Know Your Customer
NBE	National Bank of Ethiopia
PIN	Password Identification Number
POS	Point Of Sale
SLR	Systematic Literature Review
SMS	Short Message Service
SSL	Secure Socket Layer

Declaration of Authenticity

I, Feben Wondimu hereby declare that the research paper titled "The Effect of Digital Banking Fraud on Customer Service Utilization" submitted based on actual and original work done by me. All sources I have used are indicated and have been properly referenced.

Declared by:

Name Feben Wondimu

_____ _____

Name Signature & Date

Approved by

This Thesis has been submitted for the examination with my approval as College Supervisor.

Advisor: Mengistu B. (PhD)

_____ _____

Name Signature& Date

Approval Sheet

The undersigned certify that we have read and hereby recommend that Addis Ababa University accept the thesis submitted by Feben Wondimu, entitled "The Effect of Digital Banking Fraud on Customer Service Utilization", in partial fulfilment of the requirements for MSC in corporate finance, speciality in investment management.

Submitted by:
Full Name: Feben Wondimu

Signature: _____
Date: _____

Approved by:
Name of Supervisor: Mengistu B. (PhD)

Signature: _____
Date: _____

Name of Internal Examiner: _____

Signature: _____
Date: _____

Name of External Examiner: _____

Signature: _____
Date: _____

Acknowledgment

Foremost, I would like to give my praise to the Almighty God for the support and guidance throughout the journey of my education. Next, I would like to express my sincere gratitude to my advisor Dr. Mengistu Bogale for his guidance, assistance and suggestion in finishing my research paper.

A heartfelt thank you goes to my family, whose unwavering support and wise counsel provided me with strength and encouragement during this endeavour.

I extend my special appreciation to the digital banking customers at the selected Commercial Banks who participated in the questionnaire and data collection process. Your contributions were vital to my research.

Lastly, I would like to acknowledge my dearest friends and colleagues, whose support and camaraderie enriched my academic experience and made this thesis possible.

ABSTRACT

This study investigates the effect of digital banking fraud on customer service utilization in Addis Ababa, Ethiopia, focusing on four major commercial banks: Commercial Bank of Ethiopia (CBE), Awash Bank, Dashen Bank, and Bank of Abyssinia (BOA). Using both qualitative and quantitative approaches, the research adopts descriptive and explanatory designs, collecting data from 400 digital banking users selected through purposive and convenience sampling. The data were analysed using descriptive statistics, Pearson correlation, and multiple linear regression, with all key regression assumptions fulfilled to ensure the validity and reliability of the findings. The results revealed that customers aged between 25 and 34 showed higher levels of digital banking utilization, likely due to greater digital literacy and familiarity with technology, while users with higher education levels were more aware of fraud risks and more engaged with digital platforms. Gender differences were present but not significant, indicating increasing adoption by both male and female users. The regression analysis confirmed that fraud-related factors such as fraud type, fraud prevention measures, fraud incidents, customer awareness, and perceived fraud were significant predictors of digital banking service utilization. Among these, fraud prevention measures had the greatest positive impact, suggesting that trust in security features motivates usage. Customer awareness also positively influenced usage, emphasizing the importance of educating users about fraud threats and protective behaviours. Interestingly, perceived fraud had a positive relationship with utilization, possibly reflecting greater user confidence in managing risks. Conversely, actual fraud experiences negatively impacted usage, indicating that exposure to fraud erodes trust and discourages continued use. Although fraud type showed a positive association, it was not statistically significant. The model explained 70.7% of the variance in digital banking utilization, confirming the strong predictive power of these fraud-related factors. Based on these findings, the study recommends that banks strengthen digital security systems through technologies such as multi-factor authentication, encryption, and fraud detection; launch regular awareness campaigns to educate users on emerging fraud types and safe practices; offer responsive support after fraud incidents, including compensation and emotional reassurance; promote best practices like using strong passwords and avoiding public Wi-Fi; and conduct regular customer feedback collection to align digital strategies with user concerns.

Keywords: Service Utilization, Digital Banking, Digital Fraud, Financial Institution

CHAPTER ONE

Introduction

1.1 BACKGROUND OF THE STUDY

(Tijani, J. A., & Ilugbemi, A. O., 2015) Emphasized that the financial system now offers an infinite number of banking opportunities through electronic banking. Customers of banks and other stakeholders now enjoy greater flexibility and convenience thanks to the development of technology-driven payment systems (Kelvin, 2012). In recent years, the rapid advancement of technology has revolutionized the banking sector, leading to the widespread adoption of digital banking services. This transformation has provided customers with unprecedented convenience, allowing them to conduct financial transactions anytime and anywhere.

In the digital age, there has been a surge interest in financial services that need to be developed and modernised in the last year. This has created significant challenges for academics and marketers, as opposed to encouraging banks to improve the electronic services they offer to customers in order to retain existing ones and try to draw in new ones. Additionally, banks must keep up with technological advancements in order to differentiate themselves in the services they provide (Tamiru, 2017). Customers may now conduct transactions with ease using online platforms, smartphone applications, and digital payment gateways. As a result of the previously unheard-of convenience and efficiency brought about by the digital revolution. (Rabsan, 2000) Asserts that because online banking allows clients to access financial services outside of the banking hall, it guarantees consumer satisfaction. Similarly, banks have benefited greatly from e-banking since it has raised consumer satisfaction and loyalty (Oumlil and Wilian, 2000) but in addition to these amazing advantages, the spread of technology has created new opportunities for fraud, which has seriously jeopardised the security and integrity of banking systems.

Digital banking fraud erodes consumers' trust in digital financial services in addition to jeopardising their financial security. Customers' engagement and willingness to use digital banking systems may suffer as they get more conscious of the possible risks connected to online transactions. This trade-off between danger and convenience calls for a careful examination of how fraud affects consumer behaviour and perceptions in the context of digital banking. According to (Rezaee, 2004) electronic fraud is still on the rise, despite the

unprecedented measure to minimize the incidence of electronic fraud, because the fraudsters continually devices new strategic ways of committing electronic fraud.

As noted by (Yonas, 2020), in Ethiopia, digital banking is in its infancy stage facing significant challenges, particularly concerning fraud and cyber security. The sector suffers from a lack of transparency, as incidents of digital banking fraud are not usually disclosed publicly, which limits customers' and stakeholders' understanding of the associated risks. This opacity undermines trust in digital banking services, as there is little information available regarding fraud and cyber security threats.

Research indicates that insufficient information about fraud and cyber security can heighten customer anxiety and make them hesitant to use digital services. Moreover, banks frequently prioritize various fraud management strategies but fail to effectively communicate these initiatives to their customers, leading to a reactive rather than proactive stance on fraud prevention. Consequently, the digital banking environment in Ethiopia is marked by a knowledge and trust gap that could impede the growth and development of this crucial sector. This study analysed the effect of digital banking fraud on customer service utilization of digital financial services within selected commercial banks. It aims to give financial institutions useful information by investigating the different forms of fraud that are common in the sector; evaluating consumer Knowledge; investigating the connection between perceived fraud risk and customer engagement. The results provided useful suggestions for strengthening security protocols, boosting client confidence, and eventually creating a more safe and interesting digital banking experience.

1.2 STATEMENT OF THE PROBLEM

The inability of banks to fulfil their functions effectively stems from various risks they face that are not properly managed (Papazoglou, 2003). One significant risk that is increasingly problematic is the banking risk linked to fraud. It has become a worldwide threat to the banking sector (Ramamoorti, S., Morrison, D., & Koletar, J. W., 2009). Furthermore, banks tend to implement various fraud management strategies without sufficiently communicating these measures to the public, leading to a reactive rather than proactive approach to fraud prevention. For the digital banking sector in Ethiopia to mature and gain customer trust, it is essential to improve transparency about fraud incidents, enhance customer education on cyber security, and foster proactive communication from banks. Addressing these issues will

help create a more secure and reliable digital banking environment, encouraging greater customer utilization of digital services.

A lack of transparency in fraud reporting can significantly erode customer trust in digital banking services. When financial institutions do not openly communicate about fraud incidents, customers may become uncertain about the safety of their assets and the institution's capability to protect their interests. This uncertainty can ultimately lead to a decline in customer confidence and loyalty. Studies have demonstrated a clear correlation between transparency and customer trust in financial institutions. For example, research by (Birnbrich, 2012) found that customer familiarity with fraud prevention measures positively influences the quality of customer relationships, enhancing loyalty. Effective communication regarding fraud prevention is thus crucial for maintaining trust and satisfaction among customers.

Further research by (Gupta, V., & Shukla, S, 2024) examined the role of legal and regulatory frameworks in shaping consumer trust in digital banking. Their findings suggest that transparent regulations and proactive customer relationship management are vital for building consumer confidence. When banks are open about their security measures and regulatory compliance, customers are more inclined to trust and remain loyal to the institution. Additionally, a study conducted in Kenya (Gitonga, 2018) identified transparency as a key driver of customer confidence in financial services, underscoring the importance of clear communication about services and potential risks. In conclusion, prioritizing transparency in fraud reporting and security communications is essential for fostering strong, loyal relationships between financial institutions and their customers.

The challenges of digital fraud in the banking sector are evident in various contexts, such as the notable case of Yes Bank and DHFL in India, where regulatory frameworks and advanced authentication mechanisms have been implemented to address these issues. The Reserve Bank of India (RBI) has introduced stringent guidelines and real-time monitoring systems to effectively detect and prevent fraud. In Kenya, transparent regulatory frameworks and proactive customer relationship management have been crucial in fostering consumer trust, with studies indicating that clear communication about services and potential risks is vital for maintaining customer confidence. On a global scale, research on data analytics-based auditing has demonstrated how advanced techniques can enhance audit decision-making and

fraud detection. The use of decision support systems (DSSs) founded on data analytics have improved the accuracy and efficiency of fraud detection in digital banking transactions in a global perspective. Collectively, these examples highlight the importance of transparency and technological solutions in combating fraud, suggesting that financial institutions adopting similar approaches can strengthen customer trust and enhance their fraud prevention capabilities. In order for intermediation to be effective, the banking public demands accountability, fairness, and transparency in their daily operations. Even though there have been documented instances of fraud in the industry, there are still a number of significant issues that need to be resolved. These include determining the substantial consequences of fraud cases that have been identified, figuring out how to reduce or eliminate the number of employees involved in fraud cases, and drastically lowering the amount of money involved in fraud cases. (Webalem, 2021)

Digital banking's rapid expansion has changed how people access and use financial services. However, this shift has also been accompanied by an increase in fraudulent activities, which puts consumer involvement and trust at serious danger. Despite the advancements in technology aimed at enhancing security, customers remain concerned about the safety of their financial information and transactions. This study analysed how fraud in digital banking affects customer utilization of digital financial services within selected commercial banks. Understanding these dynamics is crucial for developing strategies that not only enhance security measures but also foster customer confidence and satisfaction in digital banking platforms.

1.3 RESEARCH QUESTION

1.3.1 GENERAL RESEARCH QUESTION

How does fraud in digital banking affect customer utilization of digital financial services in selected commercial banks in Addis Ababa?

1.3.2 SPECIFIC RESEARCH QUESTION

- ✓ What is the level of customers' understanding of the types of fraud prevalent in digital banking across selected commercial banks?
- ✓ How aware are customers of the potential risks associated with digital banking fraud?
- ✓ In what ways does the perception of fraud risk influence customer utilization of digital banking services?

- ✓ How do incidents of fraud affect customers' usage patterns of digital financial services offered by commercial banks?

1.4 OBJECTIVES OF THE STUDY

1.4.1 GENERAL OBJECTIVES OF THE STUDY

To analyse the impact of fraud in digital banking on customer utilization of digital financial services in selected commercial bank of Ethiopia.

1.4.2 SPECIFIC OBJECTIVES OF THE STUDY

- ✓ To assess the level of customer awareness regarding digital banking fraud.
- ✓ To evaluate the relationship between perceived fraud risk and customer utilization with digital banking services.
- ✓ To analyse the impact of fraud incidents on the frequency and volume of digital financial transactions by customers.

1.5 SCOPE OF THE STUDY

Despite the fact that there are thirty one commercial banks in Ethiopia, the study's scope is limited to four banking institutions. These commercial banks were chosen because of their greater experience and large number of customer base. This study examined how consumer's utilization of digital financial services within selected commercial banks in the Addis Ababa area that are affected by fraud in digital banking. The study concentrated on identifying the different forms of fraud that are common in these banks and investigating the ways in which these occurrences affect customer service utilization, including the volume and frequency of transactions. By focussing on these commercial banks, the study offered a thorough grasp of Addis Ababa's digital banking environment, including information on consumer attitudes, levels of trust, and usage of digital financial services. Although fraud is a broad notion, the researcher focused on specific types of fraud prevalent in digital banking, such as phishing, identity theft, and digital transaction fraud, within selected commercial banks in Addis Ababa region. It analysed how these fraud incidents impact customer's usage, including transaction frequency and volume, as well as overall utilization of digital financial services. Additionally, the research investigated customer perceptions of fraud and security, aiming to understand

how awareness of fraud influences their use of digital banking services. This focused approach provided insights into the relationship between fraud and customer utilization of digital banking services.

1.6 SIGNIFICANCE OF THE STUDY

This research provided valuable insights into the nature and extent of fraud in digital banking, helping stakeholders understand how different types of fraud affect customer perceptions and service utilization. By shedding light on these dynamics, the study can inform banks and financial institutions about the critical areas requiring attention and intervention. Understanding the specific ways in which fraud incidents influence customer trust and engagement is essential for developing targeted strategies that can mitigate these risks and enhance overall customer experience in digital banking.

This study offers practical contributions by equipping commercial banks with actionable insights to strengthen their fraud prevention strategies and boost customer trust in digital platforms. Academically, the study enriches the existing literature by examining the relationship between fraud experiences and customer service utilization in digital banking, emphasizing the necessity for interdisciplinary approaches in future research. Additionally, it paves the way for further studies to explore the long-term impacts of emerging technologies on fraud prevention and customer behaviour in the continuously evolving digital banking environment.

By identifying customer concerns and awareness levels regarding fraud, banks can tailor their services and risk management practices to better address these issues. This proactive approach ultimately leads to improved customer satisfaction and loyalty, while also contributing to the existing body of knowledge on digital banking, customer engagement, and fraud, paving the way for future research and innovation in the field of digital finance.

This study offers practical recommendations for financial institutions to strengthen security protocols and create effective fraud prevention strategies applicable to both digital and traditional banking settings. It points out critical areas for additional investigation, including the effects of technological innovations on fraud patterns and the success of different prevention strategies, thus laying the groundwork for future studies in this domain.

1.7 ORGANIZATION OF THE STUDY

The paper was organized into five chapters, starting with Chapter One: Introduction, which gives a structured background for the study and includes a thorough description of the statement of the problem, research questions, and objectives, is the first of five chapters that make up the paper. It also highlights the importance of the problem from local, regional, and global perspectives setting the foundation for additional investigation; it also describes the significance and constraints of the study. Chapter Two, Literature Review summarizes previous studies on the subject and placing the research in the context of larger scholarly debates. The research design and methodological approach, including population and sampling methodologies and data collection tools, are described in depth in Chapter Three. Chapter Four presents and analyses, the gathered data is presented and examined in light of the predetermined study questions and goals. The results are then interpreted using a variety of statistical techniques. Lastly, Chapter Five: Overview, Conclusion, and Suggestions highlight the study's importance and possible influence in the field by summarising the main findings, drawing inferences from the analysis, and providing recommendations.

CHAPTER TWO

2.1 Theoretical Literature Review on Fraud

2.1.1. Definition of fraud

According to (Adeyemo, 2012) Fraud is any unlawful behaviour characterized by deception, concealment, or a violation of trust." Such actions do not involve the use of threats, violence, or physical coercion. It is defined as an intentional act of deception carried out by one or more individuals. It can occur within management, either directly or through third parties. This deceptive behaviour aims to manipulate or misrepresent information for personal or organizational gain, often leading to financial loss or damage. (Rafles, Ginting., Ibnu, Aswat., Helma, Malini., 2023). Fraud is an intentional act of deceit designed to reward the perpetrator or to deny the rights of a victim. It is defined as a calculated misrepresentation that could give unauthorized benefits to people or entities. It is distinguished from corruption by its specific focus on deception for personal gain. (Rossouw, G. J., Mulder, L., & Barkhuysen, B., 2000) Fraud encompasses a wide range of behaviour united by the act of deception to perpetrate the crime. It is often associated with white-collar crime and can involve various forms of deceit, including identity theft, investment fraud, and more. (Mark Button, Branislav Hock, David Shepherd, 2022).

Fraud is a general legal term that encompasses dishonest actions aimed at using deception to unlawfully take money, property, or legal rights from another person or entity. In contrast to theft, which involves forcibly or secretly taking something valuable, fraud depends on deliberately misrepresenting facts to achieve this unlawful gain. (Longley, 2022)

Fraud can be defined in many ways due to its varied nature. For this paper, we will use the definition from the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, which describes fraud as any unlawful act marked by deceit, concealment, or betrayal of trust. Such acts do not rely on the threat of violence or physical force. Individuals and organizations commit fraud to acquire money, property, or services, evade payments or loss of services, or gain personal or business advantages. (IIA's, 2017).

Fraud is a worldwide problem that can occur in any organization at any time. Currently, instances of fraud are increasing, mainly driven by the global financial crisis and the resulting economic downturn. Different scholars, researchers, and authors have provided their own definitions of "fraud." This term includes actions like embezzlement, financial

misrepresentation, misappropriation, extortion, illegal wealth accumulation, deceit, bribery, false representation, theft, and the concealment of significant facts, among others.

2.1.2. Theories of Fraud

2.1.2.1 Fraud Triangle Theory

(Cressey, 1973) Explored the first theory of fraud in (1953), connecting it to human behaviour. His model, known as the "fraud triangle theory," identifies three conditions that can contribute to fraud: opportunity, pressure, and rationalization.

(Albrecht, W. S.Albrecht, C. C., Albrecht, C. O. & Zimbelman, M. F., 2009) Assert that fraud consists of three components: perceived pressure, perceived opportunity, and the rationalization of the fraudulent act. These three components are referred to as the fraud triangle. Each instance of fraud, whether directed against an entity or committed on its behalf, always involves these three elements.

Pressure

To identify motivations for fraud, researchers and anti-fraud professionals often look for financial pressures or incentives. The pressure to commit fraud can be significant, especially when organizations or employees strive to meet financial goals, compete with rivals, or recover from previous underperformance. Economic factors, such as a financial crisis, can intensify this pressure, heightening the temptation to commit fraud. To understand the incentives that promote fraudulent behaviour, researchers examine the link between structural incentives, like executive compensation frameworks, and the propensity to engage in fraudulent activities.

Opportunity

Opportunities for fraud increase when such activities remain undetected. Researchers and consultants often highlight internal structural factors, such as internal controls and auditing procedures, as key elements in identifying these opportunities. Economic conditions, like a financial crisis, can also enhance the chances for fraud. For instance, a company that has recently conducted layoffs may struggle to maintain an effective segregation of duties, which is crucial for preventing fraud. Additionally, researchers examine regulatory oversight, as it can influence the risk assessment of employees who might be tempted to commit fraud.

Rationalization

According to the fraud triangle, when opportunities for fraud are present along with motivation, a third essential element is the ability of employees to justify their actions. Employees may easily rationalize committing fraud if they feel that executives tolerate such behaviour or if they believe that fraud is common in their industry. Anti-fraud professionals

also consider economic factors that can serve as justifications for fraud, such as the notion that engaging in fraudulent activities is necessary for a business to survive a financial crisis.

Sutherland and Cressey's research indicates that individual acts of fraud are rarely the result of personal characteristics alone; instead, they are significantly shaped by environmental factors. Thus, the fraud triangle serves as a vital conceptual framework for identifying environments that promote fraud. By pinpointing situations with considerable pressure or incentives for fraudulent behaviour, unusual opportunities for fraud to remain undetected, and scenarios where employees can justify their actions, researchers and anti-fraud professionals can highlight companies, industries, and economic conditions that are especially susceptible to corruption.

2.1.2.2 Fraud Diamond Theory

(Wolfe, D. T., & Hermanson, D. R., 2004) Added a new component, “capability,” to the fraud triangle theory. They defined “capability” as the personal skills and traits that enable individuals to commit fraud. This new fraud theory is referred to as the “Diamond Fraud” theory. According to Wolfe and Hermanson, this theory posits that while “opportunity” paves the way for fraud, motive and justification identify the individual who commits it. Consequently, the individual must possess the “capability” to recognize and exploit the opportunity for fraud. Additionally, the inclusion of cognitive capabilities and biases addresses some of the potential limitations of the original fraud triangle.

Moreover, it is believed that any fraudster must possess the traits and ability to identify the opportunities that arise for committing fraud. Since the concept of capability was introduced, many have overlooked it and continued to rely solely on the original fraud triangle. This oversight fails to recognize that capability delves into the mental aspects necessary for committing fraud. By understanding these traits, owners, managers, and employees can gain insights into the behaviour of fraudsters. With this knowledge, everyone can contribute to preventing fraud in their workplaces. (Shelton A. M., 2014)

2.1.2.3 General Strain Theory

As noted by (Agnew, 2001), strain theory has its roots in the early 20th century through the contributions of Edwin Sutherland and Robert Merton. In the late 20th century, Robert Agnew (1992) revised strain theory and introduced General Strain Theory (GST). This theory suggests that strain arises from three main perspectives: (a) the failure to achieve positively

valued goals, (b) the removal of positive stimuli, and (c) the introduction of negative stimuli, which can lead to negative emotional responses.

2.2.3 Types of fraud

Unauthorized withdrawal

Unauthorized withdrawal refers to the act of taking or transferring money from a bank account without the account holder's consent or authorization (Yalew, 2021). These fraudulent activities happen when an individual, either intentionally or unintentionally, shares sensitive information like social security numbers and passwords with criminals or other parties

Financial statement fraud

Financial statement fraud involves deliberately misrepresenting or omitting financial information to mislead users of the financial statements. This can include manipulating numbers, changing accounting records, or presenting deceptive information to give a distorted view of a company's financial condition. (Gbadebo, A. D., Akande, J. O., & Adekunle, A. O, 2023)

Cheque fraud

Cheque fraud encompasses a range of illegal activities involving the manipulation or forgery of cheques to deceive individuals or financial institutions. It can take several forms, including forged cheques, which are altered or created without authorization, often featuring someone else's signature. Counterfeit cheques are another common type, where fraudsters produce fake cheques that closely resemble legitimate ones, making them difficult to identify. Additionally, stolen cheques involve the theft of cheques from individuals or businesses, which are then cashed or deposited by the thief. Lastly, altered cheques are legitimate ones that have been modified to change the amount or payee, allowing the fraudster to benefit from these alterations. (KUMAR, 2022)

2.2.3.2 Digital frauds

(Kim, G., & Shim, M. , 2016) Argue that the rise of the Internet has facilitated the expansion of online finance, presenting significant challenges to traditional banks. This shift has compelled these banks to adapt by embracing online platforms to enhance service efficiency. Given the rapid dissemination of information online, traditional banks must leverage the

benefits of Internet resources to boost their service effectiveness. (Lien, N., Doan, T., & Bui, T. N., 2020), from the perspective of commercial bank business transformation, the impact of information technology on traditional commercial banking business was discussed in depth.

Reflecting global trends, online financial fraud has surged significantly across the Americas, with many schemes taking advantage of the heightened demand for medical supplies and other vulnerabilities created by the pandemic. This surge has particularly affected private individuals and businesses in North America. According to the 2022 INTERPOL Global Crime Trend Report, the most prevalent types of fraud included impersonation, romance scams, tech support fraud, advance payment fraud, and telecom fraud. As a result, businesses and citizens in this region have faced substantial financial losses due to online fraud.

The African financial sector has undergone swift digital transformation, positioning the region as a global leader in mobile banking and money transfers. This shift has created numerous opportunities for criminals to engage in financial fraud. According to INTERPOL's 2023 African Cyber threat Assessment Report, business email compromise (BEC), phishing, and other forms of online fraud are rising concerns in Africa, driven by the quick shift to a more digital economy. Increased Internet access, combined with low levels of digital literacy, makes many Africans vulnerable to fraudsters and cybercriminals. (AFJOC, 2024)

2.2.3.2.1) Types of digital banking fraud

Phishing

(Trisolvena, M. N., & Saputra, N. H., 2024) Underscores the significant and escalating risk of phishing in cyber security, where cybercriminals employ various techniques to extract sensitive information from both individuals and organizations through fraudulent emails, websites, and messages. It classifies phishing into several categories, including web phishing, email phishing, smishing, whaling, and angler phishing, each with distinct methods to deceive victims. The research highlights the serious consequences of phishing, such as financial losses, data breaches, and reputational harm. It emphasizes the crucial role of awareness and education in combating phishing, recommending that individuals and organizations monitor their accounts, refrain from sharing personal information, and exercise caution with suspicious links. The research methodology, including literature reviews, case studies, and surveys, aims to identify patterns and formulate effective prevention measures. The paper concludes that proactive strategies and on-going research are vital for effectively addressing phishing in today's digital landscape.

Identity theft

(Reynolds, 2023) Defines identity theft as the illegal acquisition and misuse of another person's personal information, which benefits the offender while causing significant harm to the victim. It explores various methods used by criminals to obtain identity information, including hacking into systems, employing phishing scams, and stealing physical documents containing personal data. This highlights the adaptability and resourcefulness of identity thieves in exploiting vulnerabilities. Identity theft can take many forms, such as the misuse of existing accounts, the creation of new accounts fraudulently, or other unauthorized uses of personal information. This diversity underscores the complex and multifaceted nature of this crime.

Identity theft is primarily seen as a way for criminals to illegally obtain a victim's financial information to make money. This typically involves stealing bank account numbers and credit card details, which are then used to make unauthorized purchases or open fraudulent accounts in the victim's name. (Identity theft and financial loss, 2023)

POS

Point-of-sale (POS) refers to the site and system where retail transactions occur. A POS system combines hardware and software that enables businesses to handle sales transactions, typically consisting of a computer or tablet, a cash register, a barcode scanner, and a payment processing terminal. At the POS, customers pay for goods or services, and the system records transaction details, such as purchased items, total cost, and payment method. This information is vital for managing inventory and tracking sales. There are several types of POS systems, including traditional cash registers, mobile POS systems that operate on tablets or smartphones, and cloud-based systems that allow for remote access and management. POS systems are crucial for retail operations as they streamline the checkout process, enhance customer service, and provide valuable insights into sales patterns and customer behaviour. However, as the paper notes, POS systems are frequently targeted for fraud due to their direct role in financial transactions, underscoring the need for effective fraud detection measures to protect businesses from financial losses. POS systems are frequently targeted for fraudulent activities, where either employees or outside individuals manipulate the system to steal money or merchandise. This can involve actions such as processing false returns or modifying transaction amounts for personal gain. The research highlights the significance of assessing employee behaviour at the POS. By analysing individual transaction patterns in

relation to overall metrics, organizations can pinpoint employees who might be more inclined to commit fraud. This proactive strategy aids in reducing the risks associated with fraudulent activities. (Jamtgaard, M., & Nair, A., 2018)

Mobile banking

Mobile banking involves using mobile devices to access and manage financial services and transactions, enabling users to conduct various banking activities remotely for greater convenience and flexibility. This includes checking account balances, transferring funds, paying bills, and viewing transaction history directly from mobile devices, thus eliminating the need to visit physical bank branches. This capability enables users to conduct transactions anytime and anywhere, making it easier to manage finances on the go and saving both time and effort. Additionally, mobile banking enhances customer engagement by providing personalized services and timely notifications, improving the overall customer experience.

However, as mobile banking grows, so does the incidence of fraud. Common types of fraud include SIM swapping, where fraudsters gain control of a user's phone number to access their banking information; hacking and identity theft, where cybercriminals exploit vulnerabilities to steal personal and financial data; social engineering, which involves manipulating individuals into revealing sensitive information; denial of service attacks that overload systems to disrupt services; and account takeover, where unauthorized access is gained to a user's bank account. The increase in mobile financial fraud presents significant challenges for banks and the financial sector, as the lack of a comprehensive fraud management framework among stakeholders exacerbates these issues, making it difficult to effectively combat fraud. (Owiti, S., Ogara, S., & Rodrigues, A., 2022)

Internet banking

Online banking, often referred to as Internet banking, virtual banking, web banking, or home banking, is a system that allows customers of a bank or financial institution to conduct various financial transactions through the institution's website or mobile app.

E-transfer interception fraud occurs when cybercriminals redirect legitimate electronic transfers intended for a victim's account to their own. Vishing involves voice calls from fraudsters posing as representatives of financial institutions, convincing victims to disclose personal information over the phone. Application fraud happens when criminals open bank

accounts in a victim's name without consent, often using stolen identities for illegal activities like money laundering. SIM swapping tricks mobile service providers into transferring a victim's phone number to a fraudster's SIM card, allowing unauthorized access to online banking accounts by bypassing two-factor authentication. The automatic transfer system (ATS) scam involves setting up recurring transfers to fraudsters' accounts without the victim's knowledge, leading to on-going financial losses. Fake apps are counterfeit applications that mimic legitimate banking apps, deceiving users into providing personal information and often containing malware, typically downloaded from unofficial sources. (Mohari, 2024)

2.3.4 Technology and banking

Despite technological advancements and investments, 51 per-cent of surveyed banks reported encountering a significant number of false positives from their technology solutions, which hinders efficiency in fraud detection. Ineffective systems affect fraud management information, raising the question of whether banks' risks are hidden in plain sight. Inadequate reporting can also impair the Board and Risk Committee's ability to make informed decisions about resource allocation and investments, with the survey indicating that funding for fraud prevention is insufficient compared to the financial crime landscape.

Furthermore, the size and complexity of banking operations and processes can slow down the implementation of changes. In contrast, fraudsters are often quick to adapt their tactics. As fraud typologies like scams and identity theft/social engineering become more common, and as organized criminals exchange knowledge across jurisdictions to bypass bank fraud detection methods, banks acknowledge the necessity of continuously refining their fraud risk management strategies to effectively address these risks.

The tactics employed by both internal and external fraudsters are continuously evolving. As a result, banks must prioritize the operational efficiency and effectiveness of their digital fraud controls by utilizing advanced data analytics and human expertise to predict, prevent, and detect fraud. Inadequate reporting can also hinder the Board and Risk Committee's ability to make informed decisions regarding resource allocation and investments, with the survey indicating that funding for fraud prevention is insufficient compared to the overall financial crime landscape.

Technology alone is insufficient, as more than half of our global respondents reported that false positives hinder efficiency in fraud detection. Banks need to look beyond technology to achieve optimal results and performance in their fraud operating model, focusing on governance, people, processes, and technology.

2.3.5 Fraud prevention strategy

Fraudsters are becoming increasingly sophisticated and can swiftly modify their approaches. Banks must be agile in responding to emerging threats and adopt new strategies and technologies to effectively predict and prevent fraud. (Global banking fraud , 2019)

Successfully implementing an anti-fraud strategy requires an understanding that fraud is an ethical, legal, economic, and social issue. Both the government and organizational management must adopt a zero-tolerance policy toward fraud and foster an anti-fraud culture. To achieve this, it is essential to develop an anti-fraud strategy tailored to the unique characteristics of each organization. This strategy should align with the overall organizational strategy, ensuring that the code of business ethics and corporate governance are in harmony with the anti-fraud approach. Additionally, it is crucial to clearly define the powers and responsibilities related to fraud prevention and detection. While organizational leaders bear the primary responsibility for combating fraud, responsibilities should also be distributed among the board of directors, the audit committee, internal audit, internal control, lower-level managers, and all employees within the organization. (Todorović, Z., Tomaš, D., & Todorović, B., 2020)

The study highlights the critical role of education and awareness in combating cyber fraud, emphasizing the need to inform both customers and bank employees about the associated risks. Awareness programs can greatly reduce the chances of individuals becoming victims of cyber scams. Additionally, the implementation of advanced technology solutions is presented as an essential preventive measure, including multi-factor authentication systems that provide an extra layer of security and encryption techniques that safeguard sensitive data from unauthorized access. The paper also discusses the importance of using anomaly detection algorithms, which can reveal unusual transaction patterns that may signal fraudulent activity. Continuous transaction monitoring is vital for the timely detection and response to potential fraud. It concludes that by understanding and implementing these preventive measures, the banking sector can greatly reduce the risks associated with cyber fraud, thereby protecting customer assets and data while maintaining the integrity of the banking system

2.2. Empirical Literature Review

As technology advances, the digital transformation of banking has become a major trend in the global banking sector. Digital banking services, including online transactions, mobile apps, self-service kiosks, and AI-driven customer support, have reshaped the customer experience in financial services and significantly affected the industry's competitive landscape. Customer satisfaction is a key metric for banks looking to maintain their competitive advantage and achieve long-term growth. (Chu, H., & Zhan, X., 2024)

The study conducted by (Chauhan, S., Akhtar, A., & Gupta, A., 2022) aims to highlight how digital banking influences customers' evaluations of service experiences and to develop a framework that pinpoints the main factors of digital banking that impact banks' financial outcomes. By employing a structured literature review based on the preferred reporting items for systematic reviews and meta-analyses, this study analyses 88 articles published from 2001 to 2021, examining different facts of digital banking and their implications for financial performance.

The Incidence of fraud is a worldwide issue that impacts society in all spheres of life, and it affects no individual or institution. This study examined financial performance and fraud in Nigerian banks between 2002 and 2016. The Central Bank of Nigeria (CBN) statistical bulletin and NDIC annual reports served as the sources of the data that was analysed. The findings showed that the quantity of fraud (0.3354) has an impact on the performance of the banking industry. The study came to the conclusion that fraud is detrimental and suggested that a sufficient internal control system, capacity building, and a legal framework for fraud prevention be established. (Akande, F. I., Egwakhe, A. J., Benjamin, R., & Umukoro, E. J, 2024)

Strengthening data protection against illegal activities in the online environment has become necessary due to the rise in the volume of electronic transactions. The author highlights that offenders can be either individuals or legal entities, and that their objective is financial in nature. They may also achieve this purpose by interfering with the information system. A typical profile of a cybercrime criminal includes active use of information technology, expertise acting in an online setting, and a thorough understanding of digital procedures. The extent of illegal activity in this global network for communication and data exchange is continuously growing because the Internet has become an essential aspect of modern life.

According to the author, this is the cause of the increasing demand for information security, which he defines as the actual application of safeguards to shield data from outside influences in the online setting. In order to demonstrate the true severity of this contemporary form of criminal threat, this article provides a statistical analysis of the incidence of Internet scams from 2016 to 2020. (Milosevic, 2022)

Particularly in the shift from traditional banking methods to electronic banking services, information technology and infrastructure development based technology have played a significant role in constructing the future of the Indian financial system. This shift occurred for a number of reasons, including time and convenience, which allows users to easily transact their accounts at any time and from any location. Since then, a rise in online transactions has opened the door for more online fraud and cybercrime. The largest problem in the current environment is protecting client information and maintaining cyber security. Hackers and cybercriminals are now commonplace and have easy access to client data at any time or place. In many cases, customers have unintentionally become victims and prey because they think the mechanism is real. This study paper primarily focuses on cyber security, customer awareness, and ways to prevent electronic frauds. It also highlights the likelihood that customers will become the subject of phishing and hacking attacks, which are used to steal bank and personal information. This study also looks at how well-informed customers are about cyber security and digital frauds from the standpoint of nationalised banks. Only by identifying the methods and tactics used by attackers and establishing a robust defence and protection for bank clients' KYC can cyber security and infrastructure security be achieved. Additionally, it aims to identify the different elements that contribute to bank fraud that the consumer is unaware of. (Singh, K., Mistrean, L., Singh, Y., Barak, D., & Abhishek, P., 2024)

The study discovered that respondents were aware of different types of electronic banking fraud, especially automated teller machine fraud, indicating that customer awareness has a substantial impact on digital banking fraud. Preventing fraud requires greater knowledge and instruction about security measures, such as protecting personal identification numbers (PINs). The report emphasises the need for increased awareness activities by pointing out that institutional elements, such as a lack of monitoring and client education, expose banks and customers to fraudulent acts. (Amoh, J. K., Awunyo-Vitor, D., & Ofori-Boateng, K., 2021)
(Betts, M. J., Eshelby, L., & Whitehouse-Hayes, D., 2024) Presents the action and methods that should be used in order to manage, lead, and assess the effectiveness of fraud prevention.

It takes into account how important risk, data utilisation, control assessment, and fraud awareness are to successful fraud prevention. It describes the fundamental information needed to stop fraud, such as an awareness of fraud, fraudsters, and their tactics. It describes the preventative methods that must be used in an organisation. Both the human element of detection and the creation of successful awareness initiatives to improve the ability of individuals associated with an organisation to identify fraud will be highlighted.

Customer trust is essential for internet banking services to succeed. Few studies have looked at how people's perceptions of risk and bank reputation affect their usage of online banking services, despite the fact that other studies have looked at aspects that influence online trust. The goal of the current work is to close this gap. Through online trust, we specifically examined (1) how perceived risk and bank reputation impact the adoption of Internet banking services, and (2) how perceived risk influences bank reputation. Questionnaires were returned by 416 samples of Internet banking customers. Confirmatory factor analysis (CFA) and structural equation modelling (SEM) were used to evaluate and validate the model. The study found that both perceived risk and bank reputation had a substantial impact on online trust in service use; however, the relationship between perceived risk and bank reputation was not statistically significant. In addition to providing theoretical insights on online banking, perceived risk and bank reputation both play an important role in explaining users' online trust. (Tangmanee, C., & Sritadawut, N., 2021)

According to the study, functional indicators (like quality, trust, and convenience), mechanical indications (like website features, design, and perceived usability), and human indicators (like customer complaint resolution) all have an impact on customer experience (CE). This paper discusses how "gamification" can improve CE in technology-driven banking services and further combines CE with the service profit chain model. To link criteria connected to technology (gamification and digital banking indicators), customers (CE, customer satisfaction, and loyalty), and performance (financial performance), an integrative framework is suggested. It suggested that banking service providers may assess their financial results in light of how clients are affected by digital banking.

Fraud in digital banking has the potential to seriously damage consumer involvement and trust, as discovered by (Mbama, C., Ezepue, P., Alboul, L., & Beer, M., 2018). Customers may be unwilling to use digital banking services if they believe there is a substantial danger of fraud, which would reduce engagement and satisfaction. A significant element influencing

consumer satisfaction and loyalty is the perceived risk of digital banking, which can undermine trust and deter users from fully utilising digital services. Customer experience is greatly influenced by the speed, customisation, and usability of digital banking services. These service characteristics might be upset by fraud incidences, which can lead to a bad customer experience and lower service usage as clients may switch to safer alternative banking options. Additionally, to mitigate the negative consequences of fraud and maintain customer happiness, it is crucial to maintain good service quality and properly handle consumer complaints. In conclusion, even if digital banking has many benefits, the risk of fraud makes it difficult to engage customers and use services. To preserve trust and promote on-going usage of digital services, banks must put security and consumer satisfaction first.

The study conducted by (K., V., Ryzhenkova, 2024) emphasizes that banking fraud poses a threat to the sector and the broader economy, leading to serious negative consequences that affect the financial and economic security of the state. To ensure the effective operation of banking institutions and their financial security, a robust fraud detection and prevention system must be developed and implemented. This includes utilizing advanced software solutions and adhering to security standards within electronic payment systems, identifying potential threats, and employing appropriate measures to prevent and deter fraud in the banking sector. The article notes that to effectively prevent fraud, it is crucial to understand its nature.

As (Ahmad, I., Khan, S., & Iqbal, S., 2024) explores that the purpose of the study is to investigate and analyse the integration of digital technologies in the banking sector and its relationship with the rise of digital fraud, particularly focusing on online banking scams. To understand how digital banking technologies can be protected against online fraud, this research conducted a systematic literature review (SLR) covering digital banking, online fraud, and security measures. The key finding of the paper is that the adoption of digital technologies in banking has significantly contributed to the rise in digital fraud, especially in the form of online banking scams. The paper highlights that these frauds have become a global issue, evolving into a complex industry where cybercriminals employ advanced tactics, including phishing attacks, denial-of-service attacks, Trojan horses, malware, identity theft, and computer viruses. The findings stress the necessity for banks to implement advanced security measures to protect their online banking systems and the importance of on-going training and awareness initiatives for both bank employees and customers. Its focus on

the interplay between technology and fraud within the banking sector is a unique aspect. By conducting an SLR, this study examines the current security technologies utilized by banks to safeguard their online banking systems, providing valuable insights into the various measures employed to combat different types of cyber threats.

As (Jurjen, Jansen., Rutger, Leukfeldt., 2016) conducted a researcher to understand online banking fraud victimization in depth and to aid in the development of effective strategies to reduce such risks in the future. A qualitative study has examined the factors that contribute to online banking fraud victimization, revealing that victim characteristics significantly affect susceptibility to phishing and malware attacks. Additionally, there is a recognized need for more in-depth research on the factors leading to victimization, as it remains unclear whether certain individuals are at greater risk. Customers who fall victim to fraud in digital banking often inadvertently share sensitive information, such as their credentials, with fraudsters. Contributing factors include the vulnerability of targets and the lack of capable guardians, such as effective security measures. And another research by (Adegboyega, 2018) explored that customers who experience fraud in digital banking frequently become targets of phishing and malware attacks, often by responding to deceptive emails or phone calls and failing to recognize unusual elements in messages. This behaviour results in the unintentional disclosure of personal information. Additionally, fraudulent messages are often perceived as professional, which further diminishes suspicion and increases the likelihood of victimization.

(Sandal, Azhar., Manisha, Shahi., Vikas, Chhapola, 2020) Discusses the digitization of banking has led to a significant rise in e-banking fraud, which has developed into a sophisticated industry. Cybercriminals are employing advanced tools and techniques to steal sensitive information and perpetrate fraud. The study identifies several common tactics used by fraudsters, such as phishing, where deceptive emails or messages trick users into revealing personal information; malware, which involves the use of viruses and Trojans to breach systems and extract data; and identity theft, where personal information is stolen to impersonate individuals and gain access to their accounts. Key vulnerabilities within banking systems make them prone to fraud, often resulting from insufficient security measures and a lack of user awareness. To address these issues, the paper stresses the necessity of implementing strong security measures for online transactions, including regular updates to security protocols, educating users about recognizing phishing attempts, and utilizing multi-

factor authentication to enhance account security. Additionally, various banks are adopting advanced technologies to secure e-banking transactions, such as encryption, secure socket layer (SSL) protocols, and real-time fraud detection systems. It also discusses emerging techniques that could effectively combat e-banking fraud, including the use of certificate transparency to identify fraudulent certificates associated with banking fraud.

2.3 Research Hypotheses

The hypotheses listed below have been formulated based on the literature review and the problem statement discussed up to this point.

H1: Different types of fraud affect customer service utilization negatively

H2: Fraud incidents negatively impact customer service utilization.

H3: Higher perceived fraud risk reduces customer service utilization.

H4: Effective fraud prevention measures increase customer service utilization

H5: Greater customer awareness of fraud risks positively affects customer service utilization.

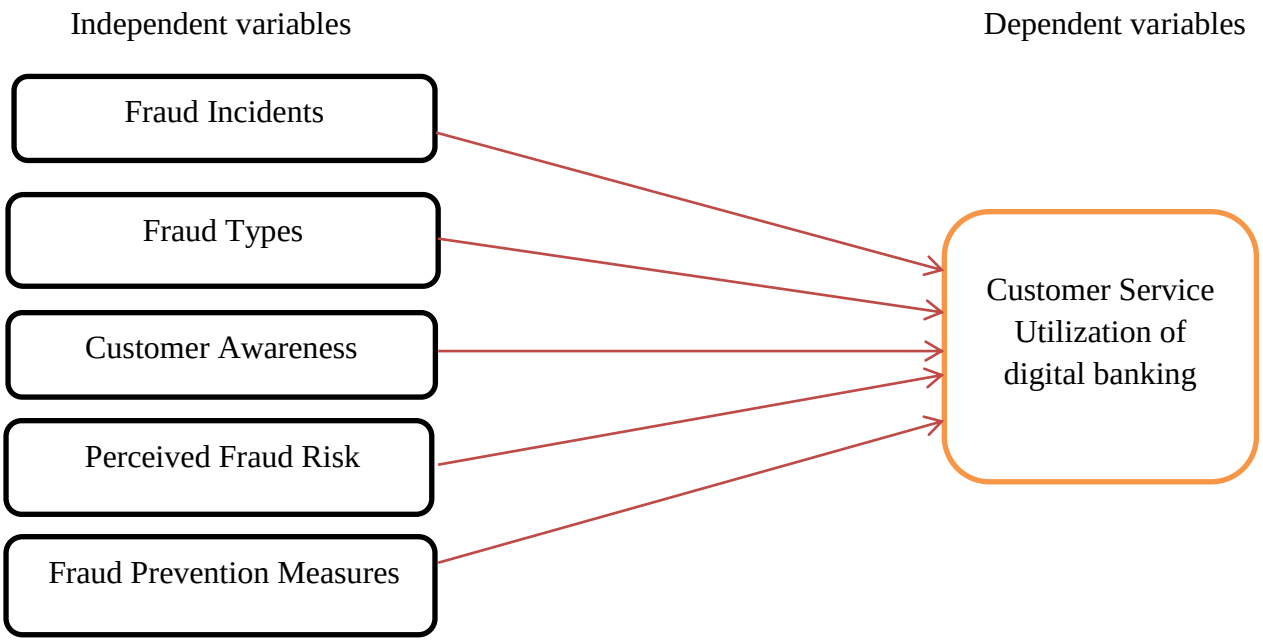
2.4 Literature Gap

While the reviewed literature extensively establishes the direct correlation between the growth of digital banking and the rise in financial fraud (Ahmad, 2024; Singh et al., 2024), and thoroughly documents the resulting negative impacts on customer trust, satisfaction, and bank performance (Mbama, 2018; Akande et al., 2024), a significant gap remains in the empirical evaluation of the proposed solutions. The literature consistently calls for a combination of technological safeguards and enhanced customer awareness initiatives (Sandal, 2020; Amoh et al., 2021). However, it lacks comparative studies that measure the relative effectiveness of these different preventative strategies. There is a notable absence of research that quantifies the specific impact of various awareness campaigns on reducing fraud victimization rates or that analyses how different post-fraud remediation efforts by banks influence the restoration of customer trust and loyalty. Consequently, while the literature identifies what needs to be done, it offers little empirical guidance on which interventions are most effective and how to best allocate resources between technological controls and human-centric education to optimally protect customers and maintain their confidence. As a result,

this study was focused how fraud in digital banking affects customer utilization of digital financial services being undertaken to bridge this knowledge and trust gap by clearly investigating the problems with possible recommendations.

2.5 Conceptual Framework

Figure 2.1 Conceptual Framework



Source: Compiled by the researcher

CHAPTER THREE

Research Methodology

3.1 Introduction

In describing research methodology, (Kothari, 2004) stated that it is a systematic manner of addressing research issues with a scope of the methods that are used to examine research problems and why researchers employ such methods. This portion of the study discusses how the research was done.

3.2 Research approach

Both qualitative and quantitative method was used in this specific study. Quantitative research, according to (De Vaus, 2002), is an empirical research technique that uses hypothesis testing to find correlations and general truths. A quantitative approach primarily employs numerical data and statistical analysis and is concerned with studying populations and samples (Neuman, 2000). T. Qualitative research is defined as "a form of social enquiry that focuses on the way people interpret and make sense of their experience and the world in which they live" by (Holloway, I., & Wheeler, S., 2002) The qualitative method is employed by different researchers to investigate people's behaviour, viewpoints, experiences, and emotions, with a focus on comprehending these components.

As a result, an open ended question was offered under the qualitative section, while most questions under the quantitative method will be presented for quantitative analysis and response. The gathered and examined data was consequently totalled and graded. As a result, the study included both methodologies, and the data collecting instruments was provided to accommodate both.

3.3 Research Design

Research design is the conceptual structure within which the research is conducted; it constitutes the blueprint for the collection, measurement and analysis of data. As such the design can be defined as a plan, structure and strategy of a research to find out alternative tools to solve the problems and to minimize the variances (Kothari, 2004). Moreover, research design is a framework or a plan to be followed for study and is used as a guideline for collecting and analysing data.

There are different types of research design, namely exploratory (emphasizes discovery of ideas and insights), descriptive (concerned with determining the frequency with which an

event occurs or relationship between variables) and explanatory (concerned with determining the cause and effect relationships).

In order to achieve the research objectives both descriptive and explanatory research designs was used for the study. The main purpose of descriptive research is to describe the state of affairs, as it exists at present time and is helpful in obtaining pertinent and precise information as well as to draw valid conclusion about the target population (Bryman, 2004) According to (Kothari, 2004) explanatory research design examines the cause and effect relationships between dependent and independent variables. It also enables a researcher to identify the extent and nature of cause-and effect relationships. Therefore, this research study described and assessed the effect of fraud on customer service utilization of digital banking in Addis Ababa city among selected four commercial banks.

3.4 Target Population

According to (Diamantopoulos, A., & Schlegelmilch, B. B, 2006) , a population is a group of items that a sample will be drawn from. Target population is the specific population about which information is desired. For the study, the target population included active user of digital banking or respondents who are living in Addis Ababa City, which include 4,543,567 amounts of digital banking users from CBE, 3,567,264, from Awash, 2,143,222 from Dashen and 2,755,779 from BOA that is equal to a total of 13,009,832 users.

3.5 Sampling Techniques and Sample Size of the Study

Sampling is the procedure a researcher uses to gather people, places or things to study. It is the process of selecting a number of individuals or objects from the population such that the selected group contains elements representative of the characteristics found in the entire group (Orodho, A. J., & Kombo, D. K., 2002). According to (Salant, P., & Dillman, D. A, 202) Sample is a member of survey respondents chosen from a wider community. Similarly, “Sampling is taking any portion of a population or universe as representative of that population or universe," states (Osuala, 2007). In this study, the researcher employed a purposeful sampling and convenience technique to select participants from the target population in those relevant experiences. The rationale for using purposive (judgmental) sampling was to concentrate on those who have knowledge (know-how) about digital banking practices, in Addis Ababa. The convenience sampling method was suitable to handle this; convenience sampling is the process of choosing study participants who are conveniently reachable and available (Saunders, M., Lewis, P., & Thornhill, A., 2009).

Convenience sampling seeks to get a sample of elements that are useful. Since (Yamane, 1967) method is a dependable approach that facilitates the straightforward extraction of a sample from the population, thereby rendering it a suitable choice for the study and it was used to calculate the sample size at a 95 confidence level. By using this technique, the sample size is adequate to produce results that are significant and to draw trustworthy conclusions about the population. A 95% confidence level offers a high degree of trust in the correctness of the study's conclusions by maintaining a balance between precision and applicability. The researcher used this formula since it is simple to grasp and commonly used.

Total population size N=13,009,832

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

$$n = \frac{13009832}{1 + 13009832(0.05)2}$$

n =400

3.6 Methods of Data Analysis

A descriptive and inferential data analysis method was used to analyse the data collected through a structured questionnaire with Statistical Packages for Social Science version 27. The descriptive statistics present using tables in the form of mean and standard deviation. Since the researcher aims to analyse the effect of fraud on customer service utilization, the study will use inferential statistical methods (such as regression analysis) to determine the strength and significance of these relationship. The Pearson's correlation coefficient was used to determine statistically significant correlation between variables (Fraud Incidents, Perceived Fraud Risk, Fraud Prevention Measures, Customer Awareness and Regulatory and Institutional Transparency). In addition OLS multiple regression and t- statistics were conducted to test the relationship between dependent and independent variable and the researcher used multiple regressions in order to identify the most influential factors of service utilization. To test the hypothesis based on the estimated coefficient by using OLS the model should fulfil assumption of CLRM (classical linear regression model). From those assumptions, multi-colinearity test and auto correlation test was conducted in this study. According to (Brooks, 2008) multi co-linearity means it is a problem that occurs when there is correlation between explanatory variable and it leads the individual variable to be insignificant. Besides, it makes difficult to draw inferences from the model. In this research correlation matrixes, will formed to check the possible degree of multi co-linearity. In

addition, Durbin-Watson test for hetero-scedasticity used with null hypothesis that variance of error is constant. Finally, for the proposed empirical model a regression analysis evaluated. Moreover, coefficients will determine for each variable. In addition, a relation between dependent and independent variables realized with the help of the model.

3.7 Model Specification

This study is developed by two sets of variables; these are the dependent variable (Customer Service Utilization) and independent variables (Fraud type, Fraud Incidents, Perceived Fraud Risk, Fraud Prevention Measures and Customer Awareness). The basic objective of using regression equation was to make the researcher more effective at describing, understanding, predicting and controlling the stated variables. In this investigation, the regression model consists of five independent and dependent variables.

The regression equation model in the study is described as follows:-

$$Y= \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \varepsilon i$$

Where;

Y= dependent variable

β_0 = coefficient (for constant)

B_i = (β_1, β_2, β_3, β_4, and β_5) are constant regression coefficient's representing the condition of the independent variables to the dependent variables.

X_i = (X_1, X_2, X_3, X_4, and X_5) are the independent variables and

εi = error term

Specifically, the model for this study is expressed as follows;

$$SCE = \beta_0 + \beta_1 F_I + \beta_2 PFR + \beta_3 FPM + \beta_4 CA + \beta_5 FT + \varepsilon i.$$

Where;

FI = Fraud Incidents

PFR = Perceived Fraud Risk

FPM = Fraud Prevention Measures

CA = Customer Awareness

FT = Fraud Type

3.8 Reliability and validity of instruments

Reliability

Test Reliability refers to the consistency and stability of measurements or observations throughout the study. It assesses whether the findings can be duplicated or repeated under similar conditions, ensuring consistent and predictable results. According to the Cronbach's alpha guidelines, a reliability coefficient above 0.7 indicates that the data is reliable and acceptable. In this study, the researcher tested the internal consistency of the questionnaire, focusing on variables with Likert scale-style questions, to ensure reliability.

Table 3. 1 Reliability test and summary of Cronbach's alpha values

Variables	Cronbach's Alpha	Number of items
Fraud Type	0.934	9
Fraud Prevention Measure	0.938	9
Customer Awareness	0.948	10
Perceived Fraud	0.944	10
Fraud Incident	0.936	10
Service Utilization	0.912	10

Source: (Survey result of 2025, SPSS V-27)

Validity

The validity of the study decides if the researcher genuinely measures what is supposed to be measured and how accurate the research results are (Thatcher, 2010). To ensure the research's validity, credible sources such as published books and recent papers authored by highly regarded authors was used The questionnaire was adopted from (Yihunie, H. A., & Sharma, D, 2024) paper on an Overview of Digital Payment Frauds: Causes, Consequences, And Countermeasures, and (Hirnissa, M. T., Zariyawati, M. A., & Ying-Ying, T., 2019) paper on, Perceived Risk towards Continual Usage Intention of Online Banking. In order to make the questionnaire more pertinent and useful for obtaining precise data, the researcher eliminated items that were biased and inappropriate.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.1 Introduction

Data gathered via questionnaires is analyzed, interpreted, and discussed in this chapter. Tables are used to show and summarize responses to the questionnaire's measures. These research topics were addressed through the use of a Likert scale-based questionnaire that examined respondents' and users' perceptions of the utilization of digital banking. In addition, research were conducted using these records, which were then utilized for analysis and discussion. A total of 400 questionnaires have been developed and given to the respondents and 336 of the surveys that were sent out were gathered and used for data analysis.

4.2 Response Rate of Survey

Response rate is the quantity of those who responded the survey divided by the total number of subjects in the sample that was chosen or the quantity of qualified people in the sample. It is vital that research studies appropriately provide the denominator for computation of response rates so that readers are able to evaluate any potential prejudice, especially in regards to explanations for an absence of response. There is no predefined threshold to determine high response rate, but 80% or more is considered excellent (Booker, N., Austin, S. F., & Balasubramanian, B. A., 2021). The researcher distributed 400 questionnaires to respondents to meet research goals and 336 respondents completed and returned the questionnaire, with 28 (16%) remaining uncollected. Response rate was 84 per-cents, which is significant in determining the population of the research region based on the sample size of respondents.

4.3. Demographic profile of Respondents

The research examined the demographics of respondents' questionnaire. Respondents' demographics include Gender, Age, education level, occupation and income level of respondents. The study's objectives and intended usage were communicated to participants, which encouraged confident and honest responds. This was considered important to have an extensive comprehension of the targeted population. This summary describes the characteristics of respondents who answered the questionnaire.

Table 4. 1 Demographics profile of Respondents

Description		Frequency	Percentage
Gender	Male	183	54.5
	Female	153	45.5
	Total	336	100.0
Age (in years)	25 and below	138	41.1
	26-35	132	39.3
	36-45	30	8.9
	46-55	28	8.3
	Above 55	8	2.4
	Total	336	100.0
Educational Background	Diploma	58	17.3
	Bachelor's degree	188	56.0
	Master's degree	78	23.2
	Doctorate and above	12	3.6
	Total	336	100.0
Occupation of respondents	Unemployed	38	11.3
	Private Sector employee	140	41.7
	Government employee	48	14.3
	Self Employed	42	12.5
	Student	46	13.7
	NGO's employee	22	6.5
	Total	336	100.0
Income level of respondents	Below 1000	50	14.9
	1000-10000	82	24.4
	10001-30000	110	32.7
	30001-50000	68	20.2
	Above 50000	26	7.7
	Total	336	100.0
How frequently do you use digital banking services?	Daily	146	43.5
	Weekly	134	39.9
	Monthly	28	8.3
	Rarely	28	8.3
	Total	336	100.0

Source: (Survey result of 2025, SPSS V-27)

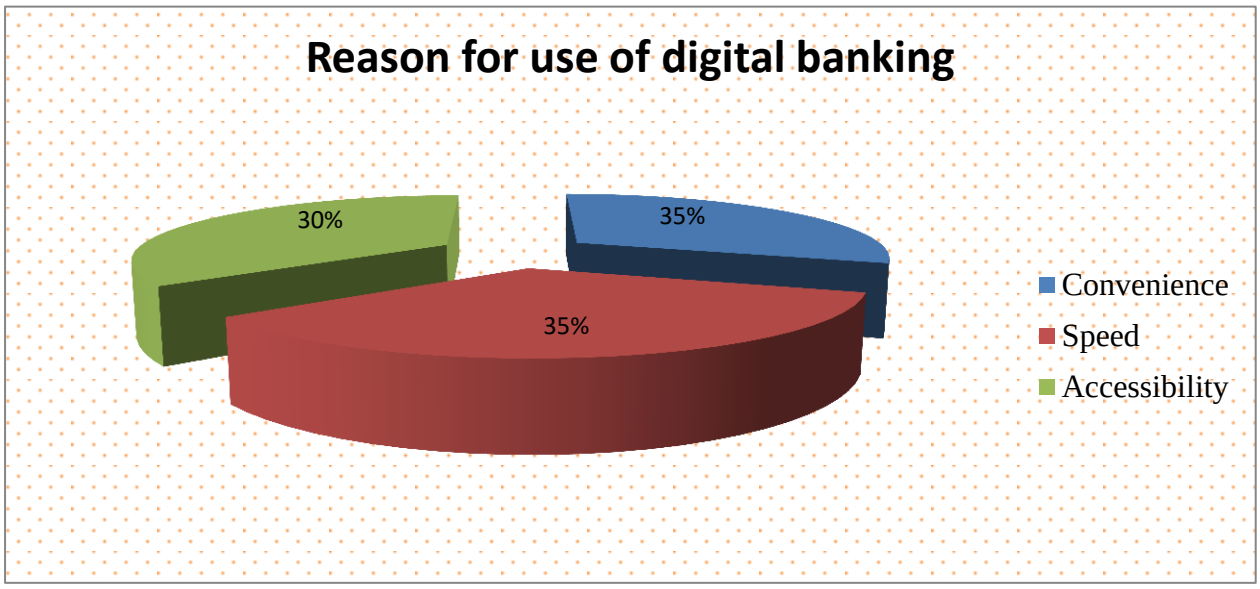
The analysis of the survey data reveals intriguing demographic insights about the respondents. Of the total participants, 54.5% identified as male and 45.5% as female. A notable concentration of respondents, 41.1%, was aged 25 years or younger. The age distribution further includes 39.3% between 26-35 years, 8.9% between 36-45 years, 8.3% between 46-55 years, and a small segment of 2.4% over 55 years. In terms of educational attainment, the majority of respondents hold a Bachelor's degree, comprising 56% of the sample. Additionally, 23.2% possess a Master's degree, while 17.3% have a diploma, and only 3.6% have achieved a Doctorate or higher.

When examining occupational status, 41.7% of respondents are employed in the private sector, making it the most common employment category. Government sector employees account for 14.3%, while students represent 13.7%. Self-employed individuals constitute 12.5%, and 11.3% of the respondents are unemployed. Finally, employees from non-governmental organizations (NGOs) make up 6.5% of the sample. Regarding income levels, a significant portion of respondents, 32.7%, reported earning between 10,001 and 30,000 birr. Those earning between 1,000 and 10,000 birr represent 24.4%. Furthermore, 20.2% of respondents earn between 30,001 and 50,000 birr, while 14.9% have an income below 1,000 birr, and 7.7% earn above 50,000 birr. Overall, this data not only highlights the demographic diversity of the respondents but also underscores the varying educational, occupational, and income backgrounds that shape their experiences and perspectives.

The data also reveals significant insights into respondents' usage of digital banking services. A substantial portion, 43.5% (146 individuals), uses these services daily, indicating a strong reliance for regular transactions and financial management. Close to 40% (134 individuals) engage with digital banking weekly, suggesting it is a valuable tool for many, though not necessarily on a daily basis. In contrast, only 8.3% (28 individuals) use these services monthly, indicating infrequent use, while another 8.3% (28 individuals) report rarely uses, possibly due to a preference for traditional banking methods. Overall, more than 83% of respondents utilize digital banking at least weekly, highlighting a clear trend toward digital financial management in the surveyed population.

4.3.1 Reason for use of mobile banking

Figure 4. 1 The reason for using digital banking

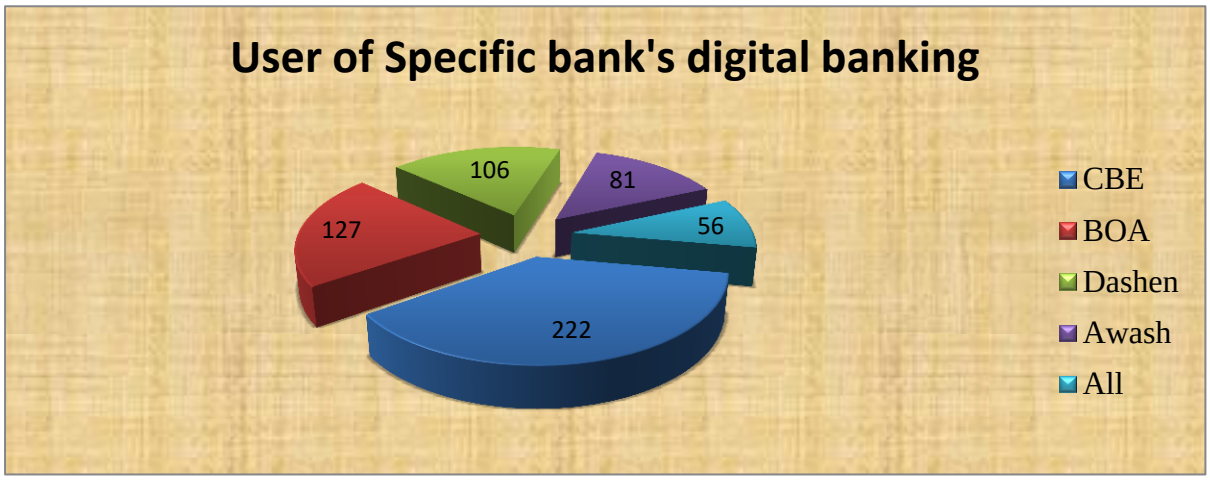


Source: (Survey result of 2025, SPSS V-27)

Mobile banking offers significant convenience by allowing customers to conduct transactions at any time and from any location, thereby enhancing their overall banking experience. Additionally, it improves the efficiency of bank staff by streamlining customer service processes and reducing wait times, leading to a more effective service delivery (Thind, N. S., Gupta, M., & Lakhanpal, S, 2020). According to (Sherlen Tertia and Anny Nurbasari, 2022) research, factors such as perceived ease of use, usefulness, and security play crucial roles in building trust in mobile banking. This trust motivates customers to use the app for checking balances and making transactions online, ultimately improving their banking experience. Similarly, the pie chart illustrates the reasons for using digital banking. Both convenience and speed are tied as the most significant factors, each accounting for 35% of the reasons. Accessibility follows closely, making up 30%. This suggests that users prioritize ease of use and quick transactions when opting for digital banking services.

4.3.2 Users of Specific digital bank

Figure 4.2 Which bank do the users use mostly?



Source: (Survey result of 2025, SPSS V-27)

The pie chart presents the distribution of users among selected commercial banks' digital banking services. CBE leads with 222 users, indicating a significant market share and strong user preference. BOA follows with 127 users, reflecting a robust user base as well. Dashen has 106 users, while Awash has 81 users, both of which show smaller segments of the market according to these sample data. Additionally, the intersection of users among all bank's totals 56, suggesting that some customers utilize digital services from multiple banks

4.3.3 Cross checking of why respondents are using the specific digital banking products of each bank

Table 4. 2 why respondents are using the specific digital banking products of each bank

Banks primary reason Cross tabulation						
			For what reason do use digital banking			
			Convenience	Speed	Accessibility	Total
Which bank do you use?	CBE	Count	148	176	182	222
	BOA	Count	95	105	109	127
	Dashen	Count	88	84	94	106
	Awash	Count	69	69	71	81
	All	Count	50	56	50	56
Total		Count	226	258	264	336

Source: (Survey result of 2025, SPSS V-27)

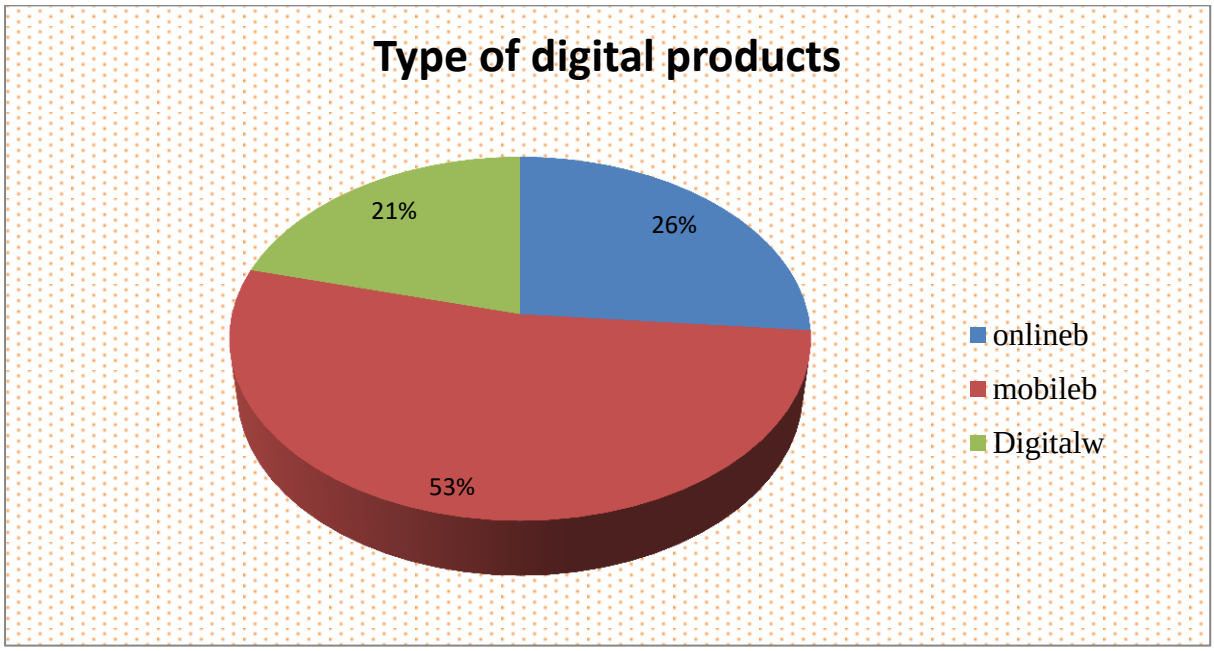
The table provides insights into the reasons respondents use digital banking services at various banks, categorized by convenience, speed, and accessibility. For CBE, convenience is the primary reason for usage, with 148 respondents citing it, followed closely by speed (176) and accessibility (182). This indicates that CBE users highly value both the quick service and ease of access offered by the bank's digital platform, contributing to its total of 222 users. BOA shows a similar trend, with convenience being the most cited reason (95), followed by speed (105) and accessibility (109), leading to a total of 127 users. This suggests that while users appreciate the efficiency of BOA's services, they also seek a balance of convenience and accessibility.

Dashen has 88 respondents indicating convenience, with speed (84) and accessibility (94) being slightly lower. This brings Dashen's total to 106 users, reflecting a need for improvement in user experience, particularly in speed. Awash have the lowest counts across all categories, with convenience at 69, speed at 69, and accessibility at 71, totalling 81 users. This may indicate that Awash has significant room for enhancement in its digital banking offerings to better meet user expectations.

The "All" category, which aggregates responses across all banks, shows that convenience (50), speed (56), and accessibility (50) are common reasons for adopting digital banking, with a total of 56 respondents. Overall, the data underscores that convenience, speed, and accessibility are pivotal factors influencing users' decisions to engage with digital banking services. Notably, accessibility emerges as the most significant consideration, commanding the largest share among the three reasons. This indicates that users prioritize the ease of accessing digital banking platforms, suggesting that banks should focus on enhancing accessibility features to meet customer expectations effectively. By addressing this critical aspect, financial institutions can improve user satisfaction and foster greater adoption of their digital banking services.

4.3.4 Type of digital banking the respondents are using

Figure 4. 3 Type of digital banking do users are using



Source: (Survey result of 2025, SPSS V-27)

As noted by (Chu, H., & Zhan, X., 2024), convenience, security, and personalization in digital banking services are critical factors that enhance customer satisfaction. Improved user experiences and interfaces across online banking, mobile banking, and digital wallets contribute significantly to fostering customer loyalty by effectively addressing these key dimensions. The accompanying pie chart illustrates the distribution of digital products among users, with mobile banking representing the largest segment at 53%, underscoring its strong preference and importance in the digital banking landscape. Online banking follows at 26%, highlighting the value of convenience and accessibility offered by mobile devices. Although digital wallets are gaining traction, they account for the smallest segment at 21%. Overall, this data emphasizes that mobile banking is the most preferred option, with online banking also holding a notable share, while digital wallets remain less commonly utilized. Additionally, (Kumar, 2024) reveals in his study that mobile banking users reported significant improvements in their overall satisfaction with banking services. This enhancement is attributed to the personalized experiences and streamlined services offered through mobile applications.

4.3.5 Which product of digital banking is the respondents are using from each specific Banks

Table 4. 3 product of digital banking customers are using from each specific bank

Banks digital Cross tabulation						
			Which digital banking are you use?			
			Online banking	Mobile banking	Digital wallets	Total
Which bank do you respondents use?	CBE	Count	107	206	80	222
	BOA	Count	86	115	61	127
	Dashen	Count	66	102	53	106
	Awash	Count	60	73	55	81
	All	Count	41	53	38	56
Total		Count	153	305	121	336

Source: (Survey result of 2025, SPSS V-27)

The cross-tabulation data presents the usage of various digital banking services among selected commercial banks. The total number of respondents using each service is as follows: online banking (153), mobile banking (305), and digital wallets (121).

For the Commercial Bank of Ethiopia (CBE), the highest usage is seen in mobile banking, with 206 users, followed by online banking (107) and digital wallets (80). The Bank of Abyssinia (BOA) also shows a strong preference for mobile banking, with 115 users, while online banking and digital wallets have 86 and 61 users, respectively. Dashen Bank has 66 users for online banking, with 102 and 53 users for mobile banking and digital wallets. The Awash Bank shows a similar trend, with 60 users for online banking, 73 for mobile banking, and 55 for digital wallets. Lastly, the "All" category indicates a total of 41 users for online banking, 53 for mobile banking, and 38 for digital wallets.

Overall, the data indicates a strong preference for mobile banking among all selected commercial banks, alongside significant usage of online banking. Although digital wallets are being used, their numbers are considerably lower than those of the other two digital services.

This suggests that while mobile banking is gaining traction, online banking continues to be the preferred option for customers in the surveyed banks.

4.4 Analysing the effect of fraud in digital banking on customer service utilization

(Burns, A. C., & Bush, R. F. , 2006) Defined descriptive analysis as the process of rearranging, organizing, and modifying raw data to present descriptive information that researchers can easily comprehend and analyse. Common calculations used to summarize data include averages, frequencies, mode, mean, and standard deviation. The mean, range, and standard deviation were calculated for the interval-scale independent variables (types of fraud in digital banking, Fraud Prevention Measures, customer awareness, perceived fraud risk and fraud incidents) and the dependent variable (the Effect of Fraud in Digital Banking on customer Service Utilization). Questions related to both independent and dependent variables were developed using a Likert scale and were constructed on an ordinal measurement level for each perspective. According to (Boone, H. N., & Boone, D. A., 2012), accurately analysing Likert data requires understanding the measurement scale provided by each item. Numbers assigned to Likert-type items indicate a "greater than" relationship, but they do not specify the magnitude of the difference. Due to this, Likert-type items are considered to be on an ordinal scale. Descriptive statistics suitable for ordinal data include the mode or median for central tendency and frequencies for variability.

In contrast, Likert scale data formed by combining four or more Likert-type items into a composite score (e.g., through summation or averaging) are treated as interval-level data. For analysing these composite scores, interval-scale methods are appropriate. Therefore, descriptive statistics such as the mean and standard deviation are recommended to measure central tendency and variability. Further analysis of interval-scale data may involve Pearson's correlation (r), t-tests, ANOVA, and regression analysis. To understand how digital banking users perceived each independent variable, the mean and standard deviations were computed. To assist and clarify the interpretation of these values, the scales were rearranged as suggested by (Al-Sayaad, J., Rabea, A., & Samrah, A. , 2006)

Table 4. 4 Scaled Likert Criterion

No.	Mean range	Response Option
1	1 to 1.80	Strongly disagree
2	1.8 to 2.6	Disagree
3	2.6 to 3.4	Neutral
4	3.4 to 4.20	Agree
5	4.2 to 5.00	Strongly Agree

Source: Al-Sayaad et al. (2006, as cited by Bassam, 2013)

4.5 The outcomes of descriptive statistics measures

4.5.1 Types of Fraud in Digital Banking

The following factors provide the findings for descriptive statistics obtained from the sample of respondents.

Table 4. 5 Knowledge of customers about type of digital banking

Descriptive Statistics		
Item List	**Mean**	**Std. Deviation**
I am aware of phishing as a common type of fraud in digital banking	3.93	.950
I know that identity theft can occur through digital banking channels	3.98	.901
I am aware of account takeover fraud in digital banking	3.92	.946
I believe that phishing attacks are a frequent issue for digital banking customers	3.92	.930
I think that identity theft incidents are common among users of digital banking services	3.83	.995
I feel that account takeover fraud poses a significant risk to digital banking users	4.05	.869
I believe that phishing fraud negatively impacts customer trust in digital banking.	4.01	.946
Identity theft incidents have caused customers to be more cautious when using digital banking services	3.93	.928
Account takeover fraud leads to a loss of confidence in the security of digital banking platforms	4.05	.929
Fraud type Grand mean and standard deviation	3.958	.7547

Source: (Survey result of 2025, SPSS V-27)

From the above table, the majority of the respondents feel that account takeover fraud poses a significant risk to digital banking users. This statement has one of the highest mean scores (4.05) suggesting strong agreement among respondents that account takeover fraud is a significant risk. The relatively low standard deviation of 0.869 indicates more consistent views, with a majority of participants recognizing the seriousness of this threat. This highlights growing concern about the impact of account takeover on user security and confidence.

The overall or grand mean of 3.96 reflects strong agreement across all items, suggesting that respondents generally perceive various forms of digital banking fraud: phishing, identity theft, and account takeover as common, impactful, and concerning. The grand standard deviation of 0.7547 is relatively low, indicating that there was consistent agreement among respondents. This reinforces the idea that digital fraud is a well-recognized and significant issue in the eyes of most users.

4.5.2 Fraud Prevention Measures

Table 4. 6 Knowledge of customers about fraud prevention measure taken

Descriptive Statistics		
Questions	Mean	Std. Deviation
I am aware of the fraud prevention measures implemented by my bank.	3.69	1.103
I regularly receive information from my bank about fraud prevention strategies.	3.74	1.066
The two-factor authentication process provided by my bank is effective in preventing fraud.	3.81	1.007
I believe that the security measures taken by my bank are sufficient to protect my personal information.	3.61	1.166
My banks fraud detection notifications are timely and effective.	3.60	1.142
I trust my bank to handle my financial information securely, reducing my concerns about fraud.	3.58	1.148
The fraud prevention measures in place increase my overall satisfaction with my banks services.	3.68	1.099
I believe my bank should enhance its fraud prevention measures even further.	3.93	1.074
I would be willing to participate in educational programs offered by my bank to better understand fraud prevention.	3.77	1.125
Fraud prevention Measure Grand mean and standard deviation	3.713	.9020

Source: (Survey result of 2025, SPSS V-27)

In the above Table, the average mean score of 3.713 (grand mean) suggests a general agreement by the respondents that banks have taken suitable steps in checking fraud, but the standard deviation of 0.902 suggests moderate variability of views. The respondent indicated in all cases that they are informed about fraud prevention measures of their bank, and the mean score is 3.69, and they are provided with regular updates on this issue (3.74). Interestingly, the highest level of agreement was recorded with regard to the effectiveness of two-factor authentication (3.81), which suggests that this is a valued step by the customers.

All in all, whereas customers are generally satisfied with existing anti-fraud controls and consider them effective, there is still an apparent demand for stricter security policies and more proactive involvement by banks. The research also indicates a potential for financial institutions to build trust and engender customer satisfaction through enhancing their anti-fraud controls and involving customers through awareness and education campaigns.

4.5.3 Customer Awareness

Table 4. 7 The customer awareness about fraud

Descriptive Statistics		
Questions	Mean	Std. Deviation
I am aware of the various digital banking services offered by my bank (e.g., mobile banking, online transfers)	3.87	1.063
I understand how to use the digital banking provided by my bank	4.10	.991
I am aware of the fraud prevention measures implemented by my bank	3.79	1.037
I have received information from my bank regarding how to protect myself from fraud.	3.78	1.127
I understand the importance of using strong passwords for my 1 accounts	4.13	1.005
I believe that I have sufficient knowledge to recognize fraudulent activities related to my bank accounts	3.86	1.030
I actively seek information about new digital banking features and security updates from my bank.	3.86	1.087
I feel confident in my ability to use digital banking services safely	3.93	1.068
I am aware of the potential risks associated with using public Wi-Fi for banking transactions	3.68	1.143
I believe that continuous education about digital banking and fraud prevention is necessary for customers.	4.10	1.040
Customer Awareness Grand mean and standard deviation	3.910	.8755

Source: (Survey result of 2025, SPSS V-27)

The grand mean of 3.910 indicates the general high degree of confidence and awareness throughout the respondents, while the standard deviation of 0.8755 indicates moderately consistent responses throughout participants.

Users indicated a very high level of understanding with regard to the importance of using strong passwords (4.13) and were confident that they possessed adequate knowledge to detect fraud (3.86). Strong agreement was also indicated with responses on receiving information about online banking innovations and improvements (3.86) and feeling secure using these services online securely (3.93). However, awareness of risk through the use of public Wi-Fi to access banking facilities was relatively lower (3.68) and perhaps it is an industry where customer education can be enhanced.

Overall, the research shows an informed and engaged customer base for digital banking and online fraud protection. There still exists, however, a need for banks to continue emphasizing some areas of risk such as use of public Wi-Fi and on-going education to keep customers up to speed and secure within a shifting digital landscape.

With regard to open ended question responses of Customers, it suggests that security protocols, transparency and instructional programs all have a significant impact on digital banking trust. Because transparency can greatly increase their trust in the bank's digital services, customers indicate a need for clear information regarding data usage and privacy regulations. It is widely held that their sense of security when utilizing these services is a result of continuous advancements in security protocols. Furthermore, the need for fraud prevention education programs emphasizes how crucial it is to arm consumers with information. Last but not least, establishing trust is seen to require a responsive and transparent customer care channel for reporting fraud events, which shows the bank's dedication to successfully resolving client problems.

4.5.4 Perceived Fraud Risk

Table 4. 8 customers perceived fraud risk

Descriptive Statistics		
Questions	Mean	Std. Deviation
I believe that fraud is a significant risk when using digital banking services	3.93	1.017
I am aware of the different types of fraud that can occur in digital banking transactions (e.g., phishing, identity theft).	3.80	1.083
I feel that my personal information is at risk when I use digital banking services.	3.60	1.163
I am concerned about the security of my financial transactions conducted online	3.74	1.099
I believe that the risk of falling victim to fraud increases when using public Wi-Fi for banking transactions	3.67	1.149
My concerns about fraud risk influence my decision to use digital banking services	3.61	1.171
I take extra precautions (e.g., using strong passwords, monitoring accounts) due to my perceived risk of fraud	3.83	1.052
I would feel more comfortable using digital banking services if my bank provided more information on fraud prevention	3.95	1.003
I believe that my bank effectively communicates the fraud risks associated with digital banking.	3.80	1.096
Overall, I feel that digital banking is safe despite potential fraud risks.	3.82	1.017
Perceived fraud Grand mean and standard deviation	3.774	.8864

Source: (Survey result of 2025, SPSS V-27)

The descriptive statistics of Perceived Fraud Risk provide evident understanding of the customers' perceptions and concerns about the security of digital banking. The respondents rate their perceived level of risk as moderate to high with a grand mean of 3.774, and the standard deviation of 0.8864 shows that responses are almost similar for the sample. The majority of the respondents concur that fraud has a significant risk when dealing with digital banking services (mean = 3.93), and this is supported by awareness of different forms of fraud like phishing and identity theft (3.80

Customers overall see fraud as a genuine danger in digital banking, but that is not necessarily going to discourage use. Instead, it supports an educated and cautious attitude. Banks are able to strengthen this confidence even further by enhancing communication and education on fraud prevention, addressing specific concerns

4.5.5 Fraud Incidents

Table 4. 9 Fraud Incident the customers are experiencing

Descriptive Statistics		
Questions	Mean	Std. Deviation
I have personally experienced a fraud incident while using digital banking services	3.26	1.356
I know someone who has experienced a fraud incident while using digital banking services.	3.64	1.204
I am aware of the common types of fraud incidents that can occur in digital banking (e.g., phishing, account takeover).	3.83	1.031
I believe that fraud incidents in digital banking are becoming more common	3.92	.955
I feel that my financial security is at risk due to potential fraud incidents in digital banking.	3.65	1.177
Fraud incidents have affected my trust in digital banking services.	3.70	1.180
I know how to report a fraud incident to my bank.	3.62	1.124
I believe that my bank responds effectively to reported fraud incidents	3.57	1.165
I feel confident that my bank takes appropriate measures to prevent fraud incidents	3.65	1.071
Overall, I believe that the risk of fraud incidents in digital banking can be effectively managed by my bank.	3.64	1.089
Fraud incident Grand mean and standard deviation	3.648	.9089

Source: (Survey result of 2025, SPSS V-27)

Descriptive statistics for Fraud Incidents in Digital Banking are helpful to know customers' experience, awareness, and confidence regarding their banks' fraud-handling capability. The grand mean of 3.648 reflects that the respondents as a whole somewhat agree with the statements provided, though not strongly, and the standard deviation of 0.9089 reflects the variability level in the responses as moderate.

Overall, while direct personal experience with fraud is less common, indirect experience and increased awareness add strength to a moderate level of customer concern. Nearly all

respondents believe that their banks are in fairly decent condition to handle fraud risk but also see a need for improved response measures and confidence-rebuilding measures. Improved communication, transparency, and support at the time of incidents may further increase customer trust in digital banking products.

4.5.6 The Effect of Fraud in Digital Banking on Service Utilization

Table 4. 10 The Effect of Fraud in Digital Banking on Service Utilization

Descriptive Statistics		
Question	Mean	Std. Deviation
I regularly use my banks digital platforms to conduct financial transactions.	3.92	.995
My experience with fraud affects my use of digital banking services	3.75	1.086
I avoid using some digital banking features due to concerns about fraud.	3.53	1.177
I limit the amount I transact through digital banking because of security concerns.	3.49	1.197
I would stop using digital banking if fraud incidents increased significantly.	3.77	1.103
I will take (took) action after experiencing fraud (Changed passwords, stopped using digital banking and Reported to the bank)	3.95	1.006
I feel secure using digital banking services after experiencing fraud	3.43	1.195
I prefer using digital channels over visiting physical branches.	4.03	1.051
I conduct high-value transactions through digital banking channels.	3.73	1.075
I trust my banks digital platform enough to try new services when they are introduced.	3.84	1.021
Fraud in Digital Banking on Service Utilization Grand mean and standard deviation	3.745	.8155

Source: (Survey result of 2025, SPSS V-27)

The descriptive statistics for The Effect of Fraud in Digital Banking on Service Utilization provide a clear picture of the way fraud experiences and anxieties influence customers' utilization of digital banking services. The grand mean value of 3.745 indicates overall

positive sentiments about the utilization of digital banking despite the existence of fraud anxieties and the generally low standard deviation value of 0.8155, which indicates comparable responses among participants.

Overall, while customers are proactive and assertive in their use of digital banking, fraud occurrence and worry still exert a moderating influence on the level at which they use it. Convenience and trust in the bank's computer systems encourage continued usage, but banks must prioritize transparent communication, prompt response to mishaps, and on-going security improvement to prevent usage erosion due to fraud in the long run.

4.6 The Relationship between Independent variables and Service Utilization

The linear relationship between two variables is measured via correlations. The range of values for a correlation coefficient is -1 to +1. A significant correlation between the variables under studies is shown by values near the absolute value of 1, whereas a weak or non-existent linear connection is indicated by values around the value of 0. It is quite helpful for gaining a sense of the connections between independent and dependent variables as well as for a first look into multi-collinearity (Field, 2009). (Hinkle, D. E., Wiersma, W., & Jurs, S. G., 2003) Provide the following rule of thumb for evaluating correlation coefficient size: see table below.

Table 4. 11 coefficient size of correlation

Size of Correlation	Interpretation
.90 to 1.00 (-.90 to -1.00)	Very high positive (negative) correlation
.70 to .90 (-.70 to -.90)	High positive (negative) correlation
.50 to .70 (-.50 to -.70)	Moderate positive(negative) correlation
.30 to .50 (-.30 to -.50)	Low positive (negative) correlation
.00 to .30 (-.00 to -.30)	Little if any correlation

Source: Hinkle and others, 2003

Therefore, the following results of the independent and dependent variables was be reviewed in depth using the survey's SPSS output and table 4.11 above.

Table 4. 12 the relationship between independent variables and Service Utilization

Correlations		
List of Variables		Service utilization
Fraud type	Pearson Correlation	.682
	Sig. (2-tailed)	.000
	N	336
Fraud prevention M	Pearson Correlation	.775
	Sig. (2-tailed)	.000
	N	336
Customer Awareness	Pearson Correlation	.651
	Sig. (2-tailed)	.000
	N	336
Perceived fraud	Pearson Correlation	.773
	Sig. (2-tailed)	.000
	N	336
Fraud incident	Pearson Correlation	.548
	Sig. (2-tailed)	.000
	N	336
Service utilization	Pearson Correlation	1
	N	336

Source: (Survey result of 2025, SPSS V-27)

The correlation test shows those statistically significant positive correlations between service usage and a number of fraud and customer behaviour-related variables with 336 as the sample size. Among all the variables tested, fraud prevention measures show the highest correlation with service usage ($r = 0.775$, $p < 0.01$), revealing that the more extensive fraud prevention mechanisms are implemented, the more their services are used possibly due to users feeling greater security and trust. Similarly, perceived fraud is also highly correlated with service use

($r = 0.773$, $p < 0.01$), which indicates that if users are better informed about the possibility of fraud; they tend to utilize services more, potentially to monitor or report fraud.

Fraud type is strongly positively correlated with service use ($r = 0.682$, $p < 0.01$), and this may indicate that fraud awareness or exposure to different fraud types impacts contact with services. Customer awareness is also significantly and positively correlated ($r = 0.651$, $p < 0.01$), emphasizing the provision of customer information on fraud issues so that they may use services. Lastly, the correlation between fraud incidents and service utilization, even though weaker ($r = 0.548$, $p < 0.01$), is still positive and moderate. This further suggests that genuine experience in fraud incidents also adds to increased usage of services, possibly because users become more aware or assertive. Overall, the findings underscore that preventive measures as well as user sentiment towards fraud have significant bearing on the use of services.

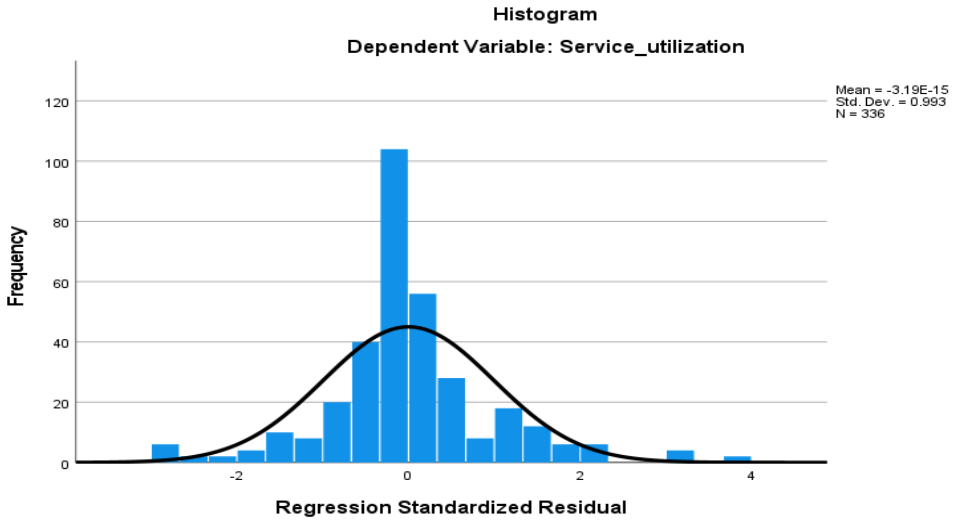
4.7 Results for Assumption of Multiple Regression Analysis

Prior to doing a regression analysis, the fundamental assumption checks for the mode must be completed. This is a necessary requirement for describing the links between dependent and explanatory variables. The key assumptions, including normality, linearity, multi-colinearity, Auto correlation and homo-scedacity must be tested and demonstrated to be reasonable. The tests are outlined below:

4.7.1 Normality Distribution Test

Multiple regression requires that the independent variables be normal distributed. This indicates that mistakes are normally distributed, thus plotting the residual values will resemble a normal curve (Keith, 2006) Frequency distribution has many different forms and sizes. As a result, having a broad definition of popular distribution types is critical. In an ideal scenario, data would be dispersed symmetrically around the center of all scores. Putting a vertical line through the center of the distribution should provide the same results on both sides. This is referred to as a normal distribution and is represented by a bell-shaped curve. This form indicates that the majority of scores are concentrated toward the center.

Figure 4. 4 Test of normality

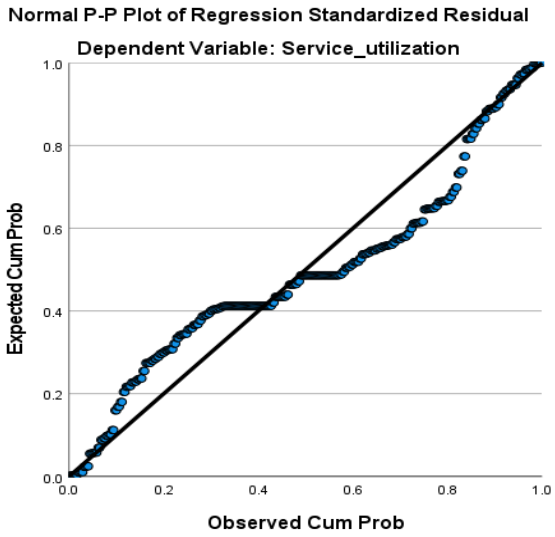


Source: (Survey result of 2025, SPSS V-27)

4.7.2 Linearity Test

The P-P plot may be used to assess the linearity of the relationship between dependent and independent variables in the model. The residuals are distributed more normally as the dots approach the diagonal line. Visual inspection of the p-p plot shows a linear connection between the dependent and independent variables (see graph below).

Figure 4. 5 P-P Plot of Regression Standardized Residual



Source: (Survey result of 2025, SPSS V-27)

4.7.3 Multi-collinearity Test

Multi-collinearity in regression analysis occurs when two or more explanatory variables are highly correlated to each other, such that they do not provide unique or independent information in the regression model. Multi-collinearity occurs when there is a substantial connection between two or more factors in a regression model (Saunders, M., Lewis, P., & Thornhill, A., 2007). There should not be a perfect linear connection between several predictors. High correlation between independent variables can lead to multi-collinearity, as stated by (Kothari, 2004) and (Field, 2009). (Pallant, 2010) Suggests that VIF values above 10 indicate multi collinearity and should be taken seriously. The investigation found that each independent variable had a tolerance value of at least 0.10, indicating that the assumption of multi collinearity was met. The variance-inflation factor (VIF) is significantly lower than the cut-off value of 10, as seen in the table below. The VIF score indicated that multi collinearity is not a concern. The tests found no significant correlation between the predictors, confirming the assumption.

Table 4. 13 test of multicollinearity

Coefficients			
Model		Collinearity Statistics	
		Tolerance	VIF
1	Fraud type	.344	2.905
	Customer Awareness	.260	3.843
	Perceived fraud	.267	3.746
	Fraud incident	.345	2.896
	Fraud prevention M	.434	2.307
a. Dependent Variable: Service utilization			

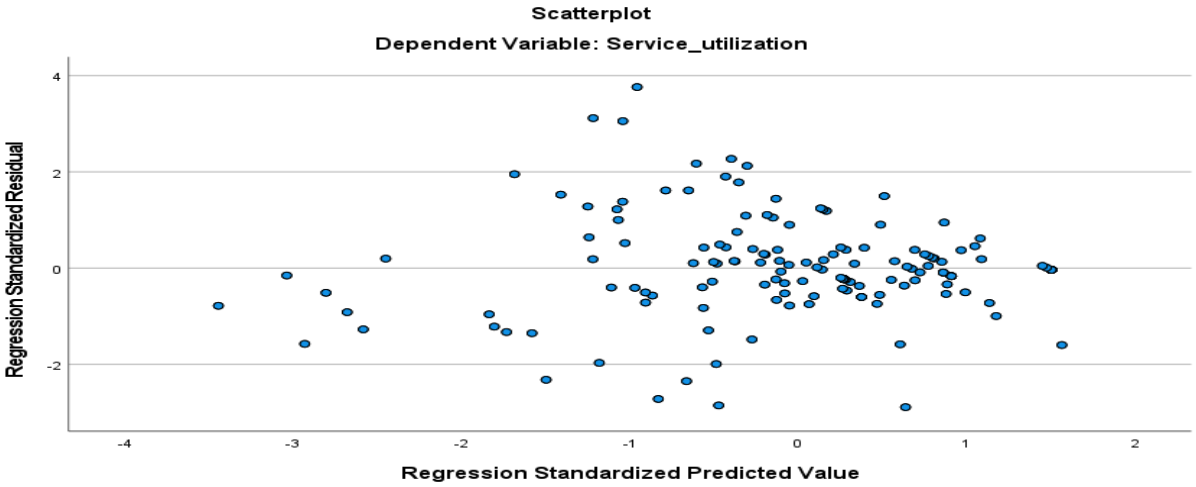
Source: (Survey result of 2025, SPSS V-27)

4.7.4 Homoscedasticity

Homoscedasticity is an assumption that errors have similar variance across all levels of independent variables (Osborne, J. W., & Waters, E., 2002). This indicates a uniform distribution of residual terms or homogeneity of error terms throughout the data. To check for homoscedasticity, check a plot of the standardized residuals against the regression standardized predicted value (Osborne, J. W., & Waters, E., 2002) If error terms are scattered randomly and do not follow a pattern, the issue does not affect analysis. The scatterplot in the

following figure demonstrates that the standardized residuals in this study are distributed uniformly, indicating no violation of homoscedasticity.

Figure 4. 6 Scatterplot of standardized residuals



Source: (Survey result of 2025, SPSS V-27)

4.7.5 Test of Auto-correlation

The theory that errors are unrelated to one another, suggesting that individuals are reacting independently, is known as autocorrelation or independence of errors (Stevens, 2009). The assumption that our residuals are independent (or uncorrelated) may be tested using the Durbin Watson statistic. The range of this statistic is 0 to 4. The Durbin-Watson number must be near 2 in order to satisfy this assumption (Field, 2009). Problematic and concerning values are those that are less than 1 and greater than 3. The researcher must examine the Model Summary box that is shown below in order to verify this assumption.

Table 4. 14 Test of Auto-correlation

Model Summary					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.841[a]	.707	.703	.4771	2.047
a. Predictors: (Constant), Fraud incident, Fraud prevention M, Fraud type, Perceived fraud, Customer Awareness					
b. Dependent Variable: Service utilization					

Source: (Survey result of 2025, SPSS V-27)

4.8 Regressions Analysis

Regression analysis is a statistical method used to estimate the connections between variables. It assesses the strength of the association between variables and the predictive potential of independent factors on the dependent variable. Regression analysis determines how a change in the independent variable affects the dependent variables while other variables remain constant. Regression analysis is a statistical method for identifying impactful factors. Regression analysis aims to determine the impact of independent factors on a dependent variable. A multiple R of 1 represents a situation in which the model perfectly predicts the observed data. (Field, 2009) Adjusted R-square is a measure of the loss of predictive power or shrinkage in regression. The adjusted R-square tells us how much variance in the outcome would be accounted for if the model had been derived from the population from which the sample was taken Adjusted R-squared is always smaller than R-squared, but the difference is usually very small unless you are trying to estimate too many coefficients from too small a sample in the presence of too much noise.

Table 4. 15 model summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.841[a]	.707	.703	.4771
a. Predictors: (Constant), Fraud incident, Fraud prevention M, Fraud type, Perceived fraud, Customer Awareness				
b. Dependent Variable: Service utilization				

Source: (Survey result of 2025, SPSS V-27)

The regression model showed a strong relationship between the independent variables (Fraud incident number, Fraud prevention Measures, Fraud type, Perceived fraud risk and Customer Awareness) and service utilization. The R^2 value of 0.707 indicates that approximately 70.7% of the variance in service utilization is explained by the model. The adjusted R^2 value of 0.703 confirms the model's strength after accounting for the number of predictors. The standard error of the estimate (0.4771) suggests a reasonably accurate model fit.

4.9 ANOVA (Analysis of Variance)

This study employed ANOVA to analyse the effect of independent factors (Fraud incident, Fraud prevention Measure, Fraud type, Perceived fraud and Customer Awareness) on the dependent variable (service utilization). This research evaluates the model's ability to predict fraud factors affecting customer's service utilization.

Table 4. 16 Test of ANOVA

ANOVA						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	181.647	5	36.329	159.588	.000[b]
	Residual	75.123	330	.228		
	Total	256.770	335			
a. Dependent Variable: Service utilization						
b. Predictors: (Constant), Fraud incident, Fraud prevention M, Fraud type, Perceived fraud, Customer Awareness.						

Source: (Survey result of 2025, SPSS V-27)

The ANOVA results show that the regression model is statistically significant, F (5, 330) = 159.588, p < .000. This indicates that the combination Fraud incident, Fraud prevention M, Fraud type, Perceived fraud, Customer Awareness has a significant impact on fraud factors affecting customer's service utilization.

4.10 Coefficients of Regression Analysis

Regression coefficient analysis examines the impact of independent factors on the dependent variable. Fraud incident, Fraud prevention measure, Fraud type, Perceived fraud, Customer Awareness all showed statistical significance at 0.01 and 0.05 levels, supporting the hypothesis.

Table 4. 17 Regression Coefficient Analysis of the model

Coefficients						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.463	.143		3.235	.001
	Fraud type	.109	.059	.094	1.847	.066
	Fraud prevention M	.429	.044	.442	9.769	.000
	Customer Awareness	.137	.063	.128	2.190	.029
	Perceived fraud	.392	.057	.397	6.885	.000
	Fraud incident	-.156	.049	-.162	-3.193	.002
a. Dependent Variable: Service utilization						

Source: (Survey result of 2025, SPSS V-27)

A multiple regression analysis was conducted to determine the relationship between impact of Fraud on Customer Service Utilization of digital banking and five predictor variables: Fraud type, Fraud prevention Measures, Customer Awareness, Perceived fraud and Fraud incident. Based on the SPSS output, the regression equation is:

$$Y=0.463+0.109X1+0.429X2+0.137X3+0.392X4-0.156X5+ \varepsilon$$

Service Utilization=0.463+0.109(fraud type) +0.429(fraud prevention measure) + 0.137(customer service) +0.392(perceived fraud)−0.156(fraud incident) + ε

The regression analysis revealed that among the five predictors, fraud prevention measure has the most substantial impact on customer's service utilization regarding digital banking fraud. Specifically, a 1-unit increase in fraud prevention measure leads to a 0.429 unit increase in digital banking fraud on customer's service utilization, and this effect is statistically significant ($p = 0.000$) with the highest standardized Beta value of 0.442, indicating a strong positive influence. In contrast, a 1-unit increase in knowing about type of fraud (fraud type) results in a 0.109 unit increase, which is not statistically significant ($p = 0.066$). Similarly, a 1-unit increase in customer awareness contributes a 0.137 unit increase of fraud in digital banking service utilization and this effect is statistically significant ($p = 0.029$). Regarding

fraud incident, a 1-unit increase is associated with a decrease of 0.156 units in service utilization of digital banking, suggesting a negative relationship and this is statistically significant (p = 0.002). Finally, a 1-unit increase in perceived fraud leads to a 0.392 unit increase in digital banking service utilization and again this result is statistically significant (p = 0.00). Overall, the five independent variables are such as Fraud Type, Fraud prevention Measures, Customer Awareness, Perceived fraud and Fraud incident demonstrates a meaningful and statistically significant effect of fraud in digital banking on customer service utilization of digital banking in this model.

4.11 Hypotheses Testing

Multiple regressions were employed to test the hypothesis for the independent variables, as correlation analysis alone cannot accurately determine a relationship between variables. In this study, the hypothesis is concerned with the individual effects of the five independent factors. The testing of these hypotheses leads to the accomplishment of the study's aims. This section looks deeply into the study of the data for each independent variable and their impact on how fraud in digital banking affects customer utilization of digital financial services within selected commercial banks.

Hypothesis 1: Different types of fraud reporting positively influences customer service utilization.

The regression table shows that the p value for fraud incidences is 0.066 and the coefficient is 0.109. This implies that different types of fraud reporting have an impact on the use of customer service utilization. There is a statistically insignificant association ($p > 0.05$). Consequently, the hypothesis is rejected by the researcher.

Therefore **Hypothesis 1 is rejected**

Hypothesis 2: Fraud incidents negatively impact customer service utilization.

As indicated in the regression table, the coefficient of Fraud incidents is −0.156, with a p value of 0.002. This suggests that, number of fraud incidents have a negative impact on customer service utilization of digital banking; the correlation is statistically significant ($p < 0.05$). As a result, the researcher accepts the hypothesis and which indicates that number of fraud incidents negatively affects customer service utilization of digital banking.

Therefore **Hypothesis 2 is accepted.**

Hypothesis 3: Higher perceived fraud risk reduces customer service utilization.

The regression table shows that the p value for fraud incidences is 0.000 and the coefficient is 0.392. Because $p < 0.05$, it indicates that the link is statistically significant. A higher perceived risk of fraud lowers the use of customer service. Therefore, a higher perceived risk of fraud results in a lower use of customer service

Therefore **Hypothesis 3 is accepted**

Hypothesis 4: Effective fraud prevention measures increase customer service utilization

The regression table shows that the p value is 0.000 and the coefficient of fraud prevention measures is 0.429. The link was found to be statistically significant ($p < 0.05$). The researcher so agrees with the hypothesis, which informs us the use of digital banking for customer service, is increased by effective fraud protection measures.

Therefore **Hypothesis 4 is accepted**

Hypothesis 5: Greater customer awareness of fraud risks, positively affects customer service utilization.

As indicated in the regression table, the coefficient of customer awareness is 0.137 with a p value of 0.029.The correlation is statistically significant ($p < 0.05$). Greater customer awareness of fraud risks positively affects customer service utilization As a result, the researcher accepts the Hypothesis

Therefore **Hypothesis 5 is accepted**

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter summarizes major results, draws conclusion from the study, and offers suggestions or recommendation for parties engaged in delivering a digital banking service and in general. The conclusion and recommendations reflect the research aims and serve as a starting point for further research on the effect of fraud on digital banking services in Ethiopia. On the other hand, it also offers suggestions based on the finding about the best ways that Banks may enhance usage of digital banking and how to minimize a risk.

5.2 Summary

This chapter presents the analysis and interpretation of survey responses collected through structured questionnaires that achieved an 84% response rate (336 out of 400). The study explores the habit of using digital banking, demographics, service selection, and perceptions about fraud. Most were male (54.5%), under the age of 35, and had a bachelor's degree or above. Mobile banking emerged as the most prevalent service, used by 53% of the respondents, followed by internet banking (26%) and e-wallets (21%). Usage is particularly high at the Commercial Bank of Ethiopia (CBE), which also ranked first in convenience perceived, speed, and accessibility. Convenience (35%), speed (35%), and accessibility (30%) were the primary reasons for digital banking use. Mobile banking was the most embraced service in all banks, but CBE embraced it the most. Digital wallets had the least adoption. Cross-tabulation and regression tests revealed that ease of use, usefulness, and security had a huge impact on adoption, and accessibility was reported as being the top concern among users. The study also researched fraud perceptions using descriptive and inferential statistics. Respondents reported high perception of common cyber fraud types, including account takeover (mean = 4.05), phishing (mean > 4.0), and identity theft (mean = 3.93). While banks were seen to be actively engaged in combating fraud (mean = 3.713), problems still existed with regard to security alert dependability and data protection from loss. Collectively, the findings suggest that improving fraud prevention, improving accessibility, and upholding user trust are the most critical means of boosting digital banking adoption and satisfaction with that it has a positive impact in decreasing fraud In digital banking.

The findings indicate that respondents have high confidence and know well about digital banking and fraud dangers. They are most likely to strongly agree that banks can prevent fraud better (mean = 3.93) and agree to take training in relation to it (mean = 3.77). Overall perceived competence in online services and using them effectively is very high (grand mean = 3.91), particularly in the mode of mobile banking and internet transfer (mean = 3.87), using strong passwords (mean = 4.13), and staying abreast of innovations (mean = 3.86). While customers as a whole are secure (mean = 3.93) and believe in online banking websites (mean = 3.82), there is still a marginal level of unawareness of dangers like the use of public Wi-Fi (mean = 3.68), indicating areas for more education. The majority believe on-going rising of awareness is required (mean = 4.10), and they like banks to provide them with even greater fraud protection details (mean = 3.95). Perceived fraud risk is moderate in size (grand mean = 3.77), and phishing, identity theft, and account takeovers are considered serious threats.

Users are cautious partly, some do know how to protect themselves and how to report fraud, but banks' response and protection of data is mid-range. Even though actual personal experiences of fraud are lower (mean = 3.26), being a friend/family member who has been victimized by fraud (mean = 3.64) does have an effect on users' attitudes. Most customers are still employing digital banking for convenience (mean = 4.03), making frequent transactions (mean = 3.92), and reporting ease for large-value transactions (mean = 3.73). Fraud, however, has an effect on behaviour: some limit usage or avoid features, and many would stop using digital banking if fraud increases (mean = 3.77). Even though customers are engaged in reaction to instances of fraud (mean = 3.95), post-fraud security awareness is relatively low (mean = 3.43). Statistical correlation analysis gives evidence in this regard and finds significant positive correlation among fraud avoidance behaviour and Internet banking use ($r = 0.775$, $p < 0.01$) and between awareness of fraud knowledge and usage of services ($r = 0.773$, $p < 0.01$). This implies that security and informed users enhance participation, despite the presence of fraud threats. The study showed that use of digital banking services by various components of fraud is greatly affected.

Such consumers who are better aware of fraud types and have a broader know-how on fraud, uses digital banking services more frequently. While a less significant effect was found with genuine fraud occurrences, they nevertheless had a significant effect on usage, having a tendency to make users cautious. Regression analysis supported these findings since all the key assumptions on statistical needs were met. The model demonstrated that about 70.7% of the variance in service use could be accounted for using the variables in question. Of these,

fraud countermeasures exerted the greatest positive effect, followed by perceived fraud and customer awareness. However, occurrences of fraud adversely affected usage, and type of fraud had a positive though statistically insignificant effect.

5.3 Conclusion

Users particularly those in the age range between 25–34, showed higher levels of utilization, likely due to their greater digital literacy and familiarity with technology. Customers with higher education were more aware of fraud risks and more active in using digital platforms. Gender differences were observed but not as pronounced indicating that both male and female users are increasingly adopting digital financial services. The findings of this study conclusively determine that fraud-related factors play a foundational role in shaping the utilization of digital banking services. The regression analysis confirmed that fraud type, fraud prevention measures, fraud incidents, customer awareness, and perceived fraud are positive significant predictors of service utilization. Among them, fraud prevention measures had the greatest impact, suggesting that customers will be more inclined to utilize digital banking channels if they believe there are effective security features in place. Customer awareness also positively and significantly impacted, highlighting the importance of alerting users to potential threats and how they can protect themselves. Perceived fraud was positively related to usage, surprisingly, maybe pointing to greater user awareness and the perception that fraud threats can be managed with knowledge and the right tools.

On the other hand, actual fraud experiences were negatively associated with service usage. This may be taken to imply that actual exposure to fraud can undermine trust in digital banking, and customers will reduce their use. Fraud type was positively associated with service use, but its association was not significant, implying that knowledge of fraud types as such may not be enough to impact digital banking utilization. Moreover, all the key assumptions of regression analysis were fulfilled, in support of the validity and reliability of the findings. The overall model explained a large proportion (70.7%) of the variance in the use of digital banking, which suggests that these fraud-related factors are indeed strong predictors of customer utilization in the digital financial sector.

5.4 Recommendation

This is the researcher recommendation that Banks should continue to strengthen their digital security systems, including multi-factor authentication, encryption, and fraud detection technologies.

- The researcher recommended that regular awareness campaigns should be launched to educate users about common and emerging fraud types, safe banking practices, and how to recognize suspicious activity by Banks.
- Banks should support users (customers) after Fraud Incidents which includes swift incident response, compensation policies and emotional reassurance.
- The recommendation to Banks is to promote best practices such as using strong passwords, avoiding public Wi-Fi for transactions and regularly monitoring customer accounts.
- It is the researcher recommendation that Banks should conduct regular surveys or feedback collection to understand customer concerns and adjust digital strategies.
- The researcher recommended that banks should create a responsive and transparent customer service channel for reporting fraud instances to enhance customer trust in banking institutions.
- The researcher recommended that Ethiopian Cyber Security and Information Assurance Center (ECSIAC) should implement advanced algorithms to detect and prevent fraudulent transactions in real-time, create a centralized platform for reporting and analysing fraud incidents across all banks and develop systems to gather customer feedback on security experiences, improving trust and service utilization.

5.5 Limitation of the study

The results might not be representative of the larger national environment or the experiences of clients in other parts of Ethiopia; it only applied to the chosen commercial banks in Addis Ababa. Furthermore, using consumer self-reported data could add biases since people might underreport their interactions with banking services or their encounters with fraud. Finally, as new technology and fraud strategies continue to emerge, the findings may become less relevant over time due to the quickly changing nature of digital banking and fraud.

5.6 Suggestion for further research

- ✓ The Effect of Fraud in Digital Banking on Service Utilization in Ethiopia.
- ✓ How does cyber security literacy affect users' trust in digital banking services?
- ✓ What role does perceived risk play in influencing digital banking behaviour?

Bibliography

Adegboyega, J. E. (2018). Card Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria.

Adeyemo, J. (2012). Fraud and its impact on financial performance. *Journal of Business Mangement*, 5(2), 62–77.

AFJOC. (2024, 2 13). *AFJOC-African Joint Operation against Cybercrime, 2023,*. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation-against-Cybercrime

Agnew. (2001). Timothy Bergsma Walden University College of Management and Technology.

Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: unmasking online threats and fortifying e-banking security, a systematic review. *Journal of Financial Crime*.

Akande, F. I., Egwakhe, A. J., Benjamin, R., & Umukoro, E. J. (2024). Fraud And Financial Performance Of Banks In Nigeria. .

Albrecht, W. S.Albrecht, C. C., Albrecht, C. O. & Zimbelman, M. F. (2009). Fraud Examination. *Natorp Boulevard, USA: South-western Cengage Learning.*

Al-Sayaad, J., Rabea, A., & Samrah, A. . (2006). *Statistics for economics and administration studies.* Dar Hafez, Jeddah, Kingdom of Saudi Arabia. . .

Amoh, J. K., Awunyo-Vitor, D., & Ofori-Boateng, K. (2021). Customers' awareness and knowledge level of fraudulent acts in electronic banking in Ghana. *Journal of Financial Crime*, 28(3), 870–882.

Betts, M. J., Eshelby, L., & Whitehouse-Hayes, D. (2024). Preventing Fraud. . 107–132. .

Birnbrich, H. C. (2012). "The impact of fraud prevention on bank-customer relationshipsAn empirical investigation in retail banking". *International Journal of Bank Marketing*, Vol. 30 Iss 5 pp. 390 - 407.

Booker, N., Austin, S. F., & Balasubramanian, B. A. (2021). Survey response rates and the impact on validity of research findings. *Journal of Health Services Research & Policy*, 26(6), 697–703.

Boone, H. N., & Boone, D. A. (2012). Analyzing Likert Data. . *The Journal of Extension,*, 50(2) Article 48. .

Brooks, C. (2008). *Introductory econometrics for finance (2nd ed.).* Cambridge University Press.

Bryman, A. (2004). *Social research methods (2nd ed.).* Oxford University Press.

Burns, A. C., & Bush, R. F. . (2006). *Marketing research (5th ed.).* Upper Saddle River, : Pearson/Prentice Hall.

Chauhan, S., Akhtar, A., & Gupta, A. (2022). Customer experience in digital banking. *International Journal of Quality and Service Sciences.*

Chu, H., & Zhan, X. (2024). The Impact of Digital Banking Services on Customer Satisfaction. *Frontiers in business, economics and management*.

Cressey, D. (1973). Other People's Money: A study in the social psychology of embezzlement. *Other People's Money: A study in the social psychology of embezzlement.* Patterson Smith Publishing Corporation.

De Vaus, D. A. (2002). *Research design in social research.* Sage Publications.

Diamantopoulos, A., & Schlegelmilch, B. B. (2006). *Taking the fear out of data analysis: A step-by-step approach. .* Sage Publications.

Field, A. (2009). *Discovering statistics using SPSS (3rd ed.).* SAGE Publications. .

Gbadebo, A. D., Akande, J. O., & Adekunle, A. O. (2023). Financial Statements Fraud of Banks and other Financial Institutions in Nigeria. *International Journal of Professional Business Review.*

Gitonga, T. m. (2018). Factors affecting customer confidence in financial service institutions in kenya: a case of minet insurance brokers limited.

Global banking fraud . (2019). Retrieved from (https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf)

Gupta, V., & Shukla, S. (2024). Consumer Trust in Digital Banking: A Qualitative Study of Legal and Regulatory Impacts. *Interdisciplinary Studies in Society, Law, and Politics*, 18-24.

Hinkle, D. E., Wiersma, W., & Jurs, S. G. (2003). *Applied statistics for the behavioral sciences (5th ed.).* . Houghton Mifflin.

Hirnissa, M. T., Zariyawati, M. A., & Ying-Ying, T. (2019). Perceived risk towards continual usage intention of online banking. *Advanced Journal of Accounting and Finance,*, 10-18.

Holloway, I., & Wheeler, S. (2002). *Qualitative research in nursing. .*

(2023). Identity theft and financial loss. Edward Elgar Publishing eBooks.

IIA's. (2017). *The IIA's International Standards for the Professional Practice of Internal Auditing (Standards).* The Institute of Internal Auditors.

Jamtgaard, M., & Nair, A. (2018). *Point-of-sale fraud detection using video data and statistical evaluations of human behavior.*

Jurjen, Jansen., Rutger, Leukfeldt. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, 10(1):79.

K., V., Ryzhenkova. (2024). Definition of the concept of fraud in the field of banking. 3(84):368-373.

Keith, T. Z. (2006). *Multiple regression and beyond.* Pearson Education. .

Kelvin, O. (2012). Mobile money for financial inclusion. *Journal of Macro Finance, Africa*, 4, 14.

Kim, G., & Shim, M. . (2016). Study on the Mobile FinTech Vacant Technology using Patent Analysis. 32(4), 185-211.

Kothari, C. R. (2004). *Research methodology: Methods and techniques .* New Age International (P) Ltd., Publishers.

KUMAR, B. (2022). Identification of scams of cheques. *Indian Scientific Journal Of Research In Engineering And Management*, 06(05).

Kumar, J. (2024). The Transformative Role of Mobile Applications in Digital Banking: A Comprehensive Analysis of Customer Engagement and Service Evolution. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), 1675–1684.

Lien, N., Doan, T., & Bui, T. N. (2020). Fintech and Banking: Evidence from Vietnam. *Journal of Asian Finance Economics and Business*, 45(9), 54-80.

Longley, R. (2022, 12 1). *Definition and Examples of Fraud.* Retrieved from https://www.thoughtco.com/fraud-definition-and-examples-4175237

Mark Button, Branislav Hock, David Shepherd. (2022). *"Economic Crime".* ImprintRoutledge .

Mbama, C., Ezepue, P., Alboul, L., & Beer, M. (2018). Digital banking, customer experience and financial performance. . *Journal of Research in Interactive Marketing.* .

Milosevic, Đ. (2022). Frequent occurring forms of internet frauds. 56, 209–227.

Mohari, M. (2024). INTERNET BANKING: FRAUDS AND PREVENTION. *Gurukul International Multidisciplinary Research Journal*.

Neuman, W. L. (2000). *Social research methods: Qualitative and quantitative approaches (4th ed.).* Allyn and Bacon.

Orodho, A. J., & Kombo, D. K. (2002). *Research methods.* Kenyatta University.

Osborne, J. W., & Waters, E. (2002). Four Assumptions of Multiple Regression That Researchers Should Always Test. *American Journal of Industrial and Business Management*, 8, 1-15.

Osuala, E. C. (2007). *Introduction to research methodology. .* African First Publishers Limited.

Oumlil and Wilian. (2000). Customer satisfaction with online banking. *International Journal of Marketing*, vol.11 pp 567-70.

Owiti, S., Ogara, S., & Rodrigues, A. (2022). A fraud management framework for mobile financial services within kenya. *EPRA International Journal of Economics, Business and Management*, 60–67.

Pallant, J. (2010). *SPSS survival manual: A step by step guide to data analysis using SPSS (4th ed.). .* Open University Press/McGraw-Hill.

Papazoglou, M. P. (2003). Service-oriented computing: Concepts, characteristics and directions. *In Proceedings of the Fourth International Conference on Web Information Systems Engineering.*, (pp. (pp. 3–12). IEEE. 10.1109/WISE.2003.12).

Rabsan. (2000). service quality insight and managerial implication from the fortier. *Journal of American marketing*, vol 9 pp 9-13.

Rafles, Ginting., Ibnu, Aswat., Helma, Malini. (2023). Keandalan validity verification system. v6.i1.19462.

Ramamoorti, S., Morrison, D., & Koletar, J. W. (2009). Bringing Freud to Fraud: Understanding the state-of-mind of the C-level suite/white collar offender through "ABC" analysis. *https://ecommons.udayton.edu/acc_fac_pub/71.* Institute for Fraud Prevention (IFP) at West Virginia University.

Reynolds, D. (2023). Identity Theft. .

Rezaee, Z. (2004). Causes, consequences and deterrence of financial statement fraud,. *Critical Perspective on Accounting.*

Rossouw, G. J., Mulder, L., & Barkhuysen, B. (2000). Defining and Understanding Fraud: A South African Case Study. *Business Ethics Quarterly*, 10(4), 885–895.

Salant, P., & Dillman, D. A. (202). *How to conduct your own survey. .* John Wiley & Sons,.

Sandal, Azhar., Manisha, Shahi., Vikas, Chhapola. (2020). E-Banking Frauds: The Current Scenario and Security Techniques. 905-918.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business students (4th ed.).* Pearson Education Limited.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students (5th ed.).* Pearson Education.

Shelton, A. M. (2014). "Analysis of Capabilities Attributed to the Fraud Diamond" . 213.

Sherlen Tertia and Anny Nurbasari. (2022). Perceived Ease of Utilization, Usefulness, Security, and Trust in Mobile Banking.

Singh, K., Mistrean, L., Singh, Y., Barak, D., & Abhishek, P. (2024). Fraud Prevention in Digital Payment Systems and Cybersecurity Education for Customers of Nationalized Financial Institutions. .

Stevens, J. P. (2009). *Applied multivariate statistics for the social sciences (5th ed.).*

Tamiru, G. (2017). Impact of E-banking service on customer satisfaction commercial bank of Ethiopia in Jimma city. *Impact of E-banking service on customer satisfaction commercial bank of Ethiopia in Jimma city.*

Tangmanee, C., & Sritadawut, N. (2021). Effects Of Perceived Risk And Bank Reputation Through Online Trust On The Use Of Internet Banking Services. *International Journal of Electronic Commerce Studies*, 12(2), 229–244.

Thatcher, R. W. (2010). Validity and reliability of quantitative electroencephalography. *Journal of Neurotherapy,* , 122-152.

Thind, N. S., Gupta, M., & Lakhanpal, S. (2020). Increasing Acceptability Of Mobile Banking: An Indian Perspective. 7(7).

Tijani, J. A., & Ilugbemi, A. O. (2015, Asian Economic and Financial Review, 5(3), 521-531.). *Asian Economic and Financial Review, 5(3), 521-531.* Retrieved from Electronic payment channels in the Nigeria banking sector and its impacts on national development.: http://www.aessweb.com/journals/5002

Todorović, Z., Tomaš, D., & Todorović, B. (2020). Anti-Fraud Strategy. *ECONOMICS*, 8, 69 - 78.

Trisolvena, M. N., & Saputra, N. H. (2024). Phishing Cyber Security Threats. 2(1) 38–48.

Webalem, M. (2021). The effectiveness of internal control system for detection and prevention of fraud the case of selected banks in Ethiopia. *St.mary's university school of graduate studies.* St.mary's university school of graduate studies.

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond : Considering the Four Elements of Fraud. pp. 12, 38–42.

Yalew, T. (2021). Effects of Fraud on Bank Performance in Ethiopian. College of Business & Economics Department of Accounting and Finance.

Yamane, T. (1967). *Statistics: An introductory analysis. (2nd ed.).* Harper and Row.

Yihunie, H. A., & Sharma, D. (2024). Combating digital bank fraud in Ethiopia.

Yonas, W. (2020). Fraud in three Ethiopian banks follow on technology driven banking services. *Addis Ababa University Faculty of Business and Economics.*

Appendix A

Dear Respondents:

My name is Feben Wondimu, and I am conducting research for my MSc in Corporate Finance Department: Specialty in investment management at Addis Ababa University. My research title is "The Effect of Digital Banking Fraud on Customer Service Utilization." This survey aims to gather information that will be used only for academic purposes. Your participation is voluntary and all responses will be kept confidential, and no personal information will be disclosed. As a result, you are politely encouraged to respond to each question in accordance with its requirements. I appreciate your cooperation in advance. If you have any question please contact me through my:

Gmail: feb3669@gmail.com Phone number: 0936690938

Section 1: Demographic Information

1. Gender:

☐ Male ☐ Female

2. Level of Education:

☐ Diploma ☐ Master's Degree

☐ Bachelor's Degree ☐ Doctorate and above

Other _____

3. In which age group are you?

☐ 25 and below ☐ 26-35 ☐ 36-45 ☐ 46-55 ☐ Above 55

4. Occupation:

☐ Unemployed

☐ Private sector employee

☐ Government employ

☐ Student

☐ NGO's employee

Other _____

5. Monthly Income:

☐ Below 1,000 ☐ 30,001 – 50,000

☐ 1,000 - 10,000 ☐ Above 50,000

☐ 10,001 - 30,000

Section 2: Digital Banking Usage

7) Which bank's digital products do you use frequently?

☐ CBE (commercial bank of Ethiopia) ☐ Bank of Abyssinia

☐ Dashen Bank ☐ Awash Bank ☐ All of the above banks

6. How frequently do you use digital banking services?

☐ Daily ☐ Monthly

☐ Weekly ☐ Rarely

Other_____

7. Which digital banking services do you use? (Select all that apply)

☐ Online banking ☐ Mobile banking app

☐ Digital wallets

Other (please specify): _____

8. What is your primary reason for using digital banking?

☐ Convenience

☐ Speed

☐ Accessibility

Other (please specify): _____

Section 3: Questions related with specific objectives

Types of Fraud in Digital Banking	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am aware of phishing as a common type of fraud in digital banking					
I know that identity theft can occur through digital banking channels					
I am aware of account takeover fraud in digital banking					

I believe that phishing attacks are a frequent issue for digital banking customers					
I think that identity theft incidents are common among users of digital banking services					
I feel that account takeover fraud poses a significant risk to digital banking users					
I believe that phishing fraud negatively impacts customer trust in digital banking.					
Identity theft incidents have caused customers to be more cautious when using digital banking services					
Account takeover fraud leads to a loss of confidence in the security of digital banking platforms					
Overall, I believe that the types of fraud prevalent in digital banking are adequately addressed by commercial banks					

Fraud Prevention Measures	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am aware of the fraud prevention measures implemented by my bank.					
I regularly receive information from my bank about fraud prevention strategies.					
The two-factor authentication process provided by my bank is effective in preventing fraud.					
I believe that the security measures taken by my bank are sufficient to protect my personal information.					
My bank's fraud detection notifications are timely and effective.					
I trust my bank to handle my financial information securely, reducing my concerns about fraud.					
The fraud prevention measures in place increase my overall satisfaction with my bank's services.					
I believe my bank should enhance its fraud prevention measures even further					
I would be willing to participate in educational programs offered by my bank to better understand fraud prevention.					

Customer Awareness	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I am aware of the various digital banking services offered by my bank (e.g., mobile banking, online					

transfers)					
I understand how to use the mobile banking app provided by my bank					
I am aware of the fraud prevention measures implemented by my bank					
I have received information from my bank regarding how to protect myself from fraud.					
I understand the importance of using strong passwords for my online banking accounts					
I believe that I have sufficient knowledge to recognize fraudulent activities related to my bank accounts					
I actively seek information about new digital banking features and security updates from my bank.					
I feel confident in my ability to use digital banking services safely					
I am aware of the potential risks associated with using public Wi-Fi for banking transactions					
I believe that continuous education about digital banking and fraud prevention is necessary for customers.					

Perceived Fraud Risk	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I believe that fraud is a significant risk when using digital banking services					
I am aware of the different types of fraud that can occur in digital banking transactions (e.g., phishing, identity theft).					
I feel that my personal information is at risk when I use digital banking services.					
I am concerned about the security of my financial transactions conducted online					
I believe that the risk of falling victim to fraud increases when using public Wi-Fi for banking transactions					
My concerns about fraud risk influence my decision to use digital banking services					
I take extra precautions (e.g., using strong passwords, monitoring accounts) due to my perceived risk of fraud					
I would feel more comfortable using digital banking services if my bank provided more information on fraud prevention					

I believe that my bank effectively communicates the fraud risks associated with digital banking.					
Overall, I feel that digital banking is safe despite potential fraud risks.					

Fraud Incidents	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I have personally experienced a fraud incident while using digital banking services					
I know someone who has experienced a fraud incident while using digital banking services.					
I am aware of the common types of fraud incidents that can occur in digital banking (e.g., phishing, account takeover).					
I believe that fraud incidents in digital banking are becoming more common					
I feel that my financial security is at risk due to potential fraud incidents in digital banking.					
Fraud incidents have affected my trust in digital banking services.					
I know how to report a fraud incident to my bank.					
I believe that my bank responds effectively to reported fraud incidents					
I feel confident that my bank takes appropriate measures to prevent fraud incidents					
Overall, I believe that the risk of fraud incidents in digital banking can be effectively managed by my bank.					

The Effect of Fraud in Digital Banking on Service Utilization	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I regularly use my bank's digital platforms to conduct financial transactions.					
My experience with fraud affect your use of digital banking services					
I avoid using some digital banking features due to concerns about fraud.					
I limit the amount I transact through digital banking because of security concerns.					
I would stop using digital banking if fraud incidents increased significantly.					
I will take (took) action after experiencing fraud (Changed passwords, Stopped using digital banking and Reported to the bank)					

I feel secure using digital banking services after experiencing fraud					
I prefer using digital channels over visiting physical branches.					
I conduct high-value transactions through digital banking channels.					
I trust my bank's digital platform enough to try new services when they are introduced.					

What kind of suggestion do you have for Improving Trust?

If you have any additional comment or suggestion, please add in the given space below.