Innovations

Effect of Fraudulent Transactions on the Performance of Mobile Money Operators in Nigeria

[1] **Fidelis Idajor Efenji & [2] Aidi Paul Aidi**
[1] Department of Business Administration, University of Cross River State Calabar
[2] Department of Business Management, Benue State University, Makurdi

Abstract: *This study investigates the impact of fraudulent transactions on the performance of mobile money operators in Nigeria, with specific focus on phishing and social engineering, SIM swap and identity theft, and account takeover fraud. The study targets agents of Opay and MTN MoMo in Nigeria, with a population of 933. Using the Taro Yamane formula, a sample size of 308 respondents was determined to ensure representativeness at a 95% confidence level. Employing a quantitative research design and regression analysis, the study reveals a statistically significant and positive relationship between all three fraud dimensions and organizational performance. Specifically, phishing and social engineering (β = 0.3457), SIM swap and identity theft (β = 0.1562), and account takeover fraud (β = 0.2531) were found to enhance performance. Contrary to conventional expectations, these forms of fraud appear to stimulate mobile money operators to adopt advanced identity verification systems, improve internal controls, strengthen compliance with anti-fraud regulations, and invest in technological upgradesall of which contribute to improved operational efficiency, customer trust, and system resilience. The study concludes that while fraudulent transactions pose serious risks, the proactive and regulatory-driven responses by mobile money operators in Nigeria have transformed these threats into catalysts for performance improvement. It recommends the continued enhancement of identity authentication systems, reinforcement of SIM and card security, and upgrading of anti-money laundering (AML) frameworks to ensure sustained growth and customer protection in the mobile financial services sector.*

Keywords*: Fraudulent Transactions, Mobile Money Operators, Phishing, SIM Swap, Account Takeover, Performance, Nigeria*

1. Introduction

The rapid proliferation of digital financial services in Nigeriaparticularly mobile money operations—has revolutionized the way individuals and businesses conduct financial transactions. Mobile money platforms operated by fintech firms and telecommunication companies such as Opay and MTN MoMo have become instrumental in promoting financial inclusion, especially among the unbanked and

underbanked populations (Ayo et al., 2019; GSMA, 2023). These platforms offer fast, accessible, and affordable financial services, thus bridging significant gaps in Nigeria's financial ecosystem. However, the rise of digital financial services has been accompanied by an alarming increase in fraudulent transactions, threatening the trust, profitability, and sustainability of mobile money operators (Onaolapo & Odetayo, 2021).

Due to the digital and virtual nature of mobile money, these platforms are highly susceptible to cybercrime, including phishing and social engineering , phishing, social engineering, SIM swaps, and unauthorized access (Adesina & Ayo, 2020). These fraudulent activities not only erode customer trust but also result in substantial financial losses, reputational damage, and increased operational costs for service providers (CBN, 2022). The growing sophistication of fraud has made it imperative for mobile money operators to enhance their fraud detection and prevention mechanisms. The core concern is not merely the occurrence of fraudulent activities but the extent to which they affect the overall performance of mobile money operators in Nigeria (Adeoye & Emmanuel, 2022).

Understanding the nature, dimensions, and implications of fraudulent transactions is crucial, given the increasing role of mobile money in driving Nigeria's digital economy. Such an understanding enables operators, regulators, and policymakers to devise and implement robust fraud prevention frameworks while ensuring optimal organizational performance (Ibrahim et al., 2023). Fraudulent transactions in this context serve as the independent variable and are defined as unauthorized, deceptive, or illegal activities executed through mobile money platforms, often involving the manipulation of digital systems or user data for financial gain. These can be perpetrated by both external actors such as cybercriminals and internal actors like dishonest employees or agents (Onaolapo & Odetayo, 2021).

Key manifestations of fraudulent transactions include phishing and social engineering, where fraudsters manipulate users into revealing sensitive information such as PINs and OTPs; SIM swap and Identity Theft , where attackers take over users' mobile lines to access their wallets; and account takeovers, where hackers gain unauthorized access to digital accounts for illegal transfers (Adesina & Ayo, 2020). Transaction reversal fraud also poses significant threats, with fraudsters exploiting refund mechanisms for personal gain. Furthermore, internal collusion—involving collaboration between insiders and external fraudsters—remains a critical risk area for mobile money operators (CBN, 2022).

The performance of mobile money operators, the dependent variable, refers to the degree to which these institutions achieve their financial, strategic, and operational goals. In Nigeria's competitive and evolving fintech landscape, organizational performance is measured not just by profitability but also by customer satisfaction, operational efficiency, market expansion, and brand strength (Ibrahim et al., 2023; Adeoye & Emmanuel, 2022). Specific performance dimensions include financial performance (e.g., revenue growth, profit margins), customer retention and trust (e.g., user loyalty and service satisfaction),

operational efficiency (e.g., system uptime, fraud resolution speed), and brand reputation, which reflects public perception, especially during or after fraud-related incidents (GSMA, 2023).

There is growing empirical evidence to support the notion that fraudulent transactions negatively influence the performance of mobile money operators. Frequent fraud incidents typically lead to a decline in user trust, reduced transaction volumes, increased customer attrition, and reduced revenue (Onaolapo & Odetayo, 2021). Financially, fraud results in direct monetary losses as well as rising expenditures on fraud mitigation, compliance, and legal enforcement. Reputationally, it weakens public confidence and attracts negative media attention, eroding competitive advantage. In response, organizations must allocate resources to cybersecurity, staff training, and awareness campaigns, further straining operational budgets (Adeoye & Emmanuel, 2022).

In focusing on Opay and MTN MoMo as case studies, both organizations operate in high-risk, high-volume transaction environments. Their expansive customer bases and agent networks make them particularly vulnerable to fraud. For instance, in Opay's case, fraudulent activities among agents can result in massive fund losses, prompting agent attrition and reduced service coverage. Similarly, repeated fraud incidents on the MTN MoMo platform could undermine customer trust, driving users back to traditional banking systems or informal cash-based methods (CBN, 2022; Ibrahim et al., 2023). Consequently, both firms are compelled to make significant investments in fraud prevention technologies, compliance systems, and customer education initiatives costs that impact profitability and service delivery.

Ultimately, the performance of these operators measured through growth in user base, revenue generation, operational reliability, and customer satisfaction is directly impacted by how effectively they manage and reduce fraudulent activities. Tackling fraud is, therefore, not only a matter of security but a strategic imperative for long-term survival and competitive positioning in Nigeria's digital financial services ecosystem (GSMA, 2023).

1.2 Statement of the Problem

The expansion of mobile money services in Nigeria has significantly improved access to financial services, especially among the unbanked and underbanked populations (CBN, 2020; Enhancing Financial Innovation & Access [EFInA], 2022). Platforms like Opay and MTN MoMo have revolutionized financial inclusion by offering fast, affordable, and convenient digital transactions. However, this rapid digital transformation has also introduced new vulnerabilities, particularly in the form of fraudulent transactions, which are now a growing concern for both operators and users.

Fraudulent transactionsranging from phishing and SIM swap to phishing and social engineering and internal collusionpose a severe threat to the mobile money ecosystem. Studies have shown that the increasing sophistication of

cybercriminals, coupled with weak digital literacy and inadequate security measures, has led to a surge in digital financial fraud across Sub-Saharan Africa, with Nigeria being one of the most affected (GSMA, 2021; Agwu & Ogu, 2019). These activities not only result in financial losses but also damage customer trust and brand reputation, directly affecting the performance of mobile money operators.

Evidence suggests that a rise in fraudulent incidents leads to reduced user trust, increased customer churn, higher operational costs, and reputational damage (Ayo et al., 2020). Operators such as Opay and MTN MoMo, who operate in high-risk, high-transaction environments, are particularly susceptible. For instance, persistent fraud in Opay's agent network can drive away agents and customers, leading to reduced coverage and transaction volumes. Similarly, repeated fraud incidents within MTN MoMo's ecosystem can discourage users and shift them back to traditional banking options. This negatively impacts performance indicators such as revenue, customer retention, and service delivery (Oni & Ayo, 2021).

Despite the growing threat, there is a limited body of empirical research that comprehensively investigates how the different dimensions of fraudulent transactionssuch as phishing, SIM swaps, transaction reversal fraud, and internal collusionimpact the strategic, financial, and operational performance of mobile money operators in Nigeria. Furthermore, existing security and fraud prevention strategies often lag behind the evolving tactics of fraudsters, raising questions about the effectiveness and responsiveness of mobile money platforms to these challenges.

Therefore, the problem this study seeks to address is the persistent and escalating impact of fraudulent transactions on the performance of mobile money operators in Nigeria, with a focus on understanding the specific dimensions of fraud and how they undermine financial performance, customer trust, operational efficiency, and brand reputation. Without targeted research and strategic responses, mobile money operators risk eroding the gains achieved in financial inclusion and digital innovation.

1.3 Objectives of the Study

The primary objective of this study is to investigate the impact of fraudulent transactions on the performance of mobile money operators in Nigeria, the specific objectives are:

- To investigate the effect of phishing and social engineering on performance of mobile money operators in Nigeria.
- To examine the impact of SIM swap and Identity Theft on performance of mobile money operators in Nigeria.
- To assess how account takeover fraud influences the performance of mobile money operators in Nigeria.

1.4. Research Hypotheses

Based on the objectives, the following hypotheses are proposed in null form:

- H_{01}: Phishing and social engineering have no significant effect on performance of mobile money operators in Nigeria.
- H_{02}: SIM swap and Identity Theft have no significant impact on performance of mobile money operators in Nigeria.
- H_{03}: Account takeover fraud does not significantly influence the performance of mobile money operators in Nigeria.

2.0. Review of Related Literature

2.1. Conceptual Framework

This subsection explores the key concepts central to the study. The research is structured around two primary constructs: performance and fraudulent transactions. Fraudulent transactions, which serve as the independent variable, are examined through three major dimensions: phishing and social engineering, SIM swap and Identity Theft, and account takeover fraud. The performance of mobile money operators constitutes the dependent variable in the study..
Figure 2.1 shows the diagrammatical representation of the study variables.

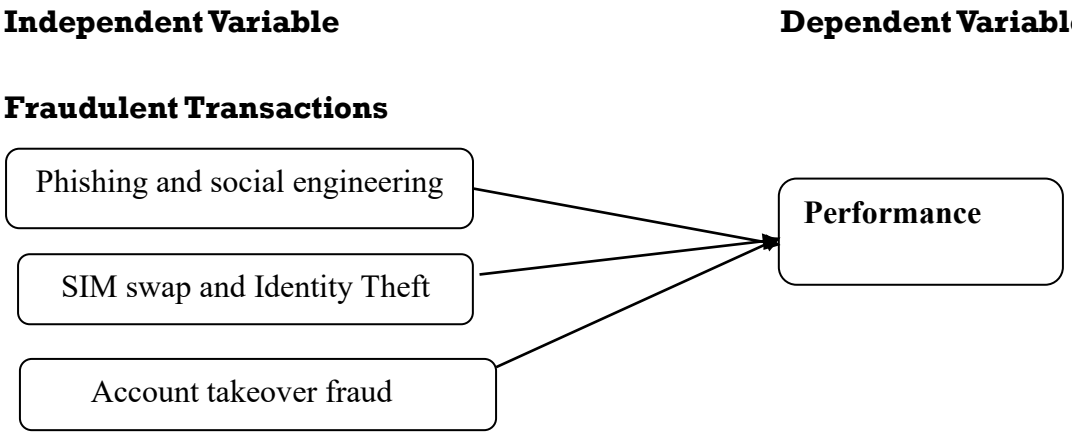

Fig. 2.1: Conceptual Model of the Study
Source: Researcher concept 2025

2.1.1 Concept of Fraudulent Transactions

Fraud is generally defined by the Oxford English Dictionary as a wrongful or criminal deception intended to result in financial or personal gain. In the context of financial services, fraud can manifest in various forms, including bank fraud, insurance fraud, and securities and commodities fraud. Understanding the classifications and definitions within these categories is essential for the detection and prevention of fraud. From an accounting and auditing perspective, fraud is a critical issue. According to the Association of Certified Fraud Examiners (ACFE), financial fraud involves the deliberate misrepresentation of an entity's financial condition through intentional misstatements or omissions in financial statements

with the aim of misleading users. The primary objectives of financial fraud are typically to overstate profits, assets, and revenues while understating expenses, liabilities, and losses.

The acceptance and continued usage of new payment systems by consumers and service providers depend heavily on strong operational and security practices. This is especially true in financial services where both financial and non-financial risks are present. Detecting fraudulent activities—preferably before transactions are completed—is crucial to preventing financial loss. If fraudulent attempts are intercepted before a transaction is processed, the transaction can be invalidated and blocked. However, if detected post-transaction, action must still be taken to block the offending user or provider from further activity and initiate legal or regulatory measures. Fraud generally includes a wide range of actions such as theft, conspiracy, corruption, embezzlement, bribery, account takeover, and extortion. While legal definitions of fraud may vary across jurisdictions, fraud is commonly viewed as an intentional act carried out by management, employees, or external parties to manipulate financial records or systems for personal or unlawful benefit.

There is no universally accepted definition of "fraudulent transactions," particularly in the digital context. However, the Nigeria Electronic Fraud Forum (NEFF, 2011) defines electronic fraud (e-fraud) as a deceptive behavior involving the use of computerized systems intended to secure an illegitimate advantage. Similarly, Legal Practitioner (2013) describes it as any wrongful or criminal deception that results in financial or personal gain. Electronic fraud typically involves the unauthorized use of digital technologies to access or remove funds from a bank account or transfer funds illegally. Common forms include phishing scams, social engineering, identity theft, and other cybercrimes targeting users of digital financial platforms. Although there is limited consensus on a single definition of fraudulent transactions, most definitions highlight two key elements: the involvement of an electronic platform and a resulting loss. These losses may be financial or non-financial, such as reputational damage or loss of competitive edge—making it difficult to quantify the full impact of fraudulent transactions.

In practice, fraudulent transactions refer to financial losses arising from deceptive or unauthorized activities conducted through electronic payment platforms or digital products. The increasing adoption of electronic payment channels has made them both attractive to new users and vulnerable to fraudulent exploitation. The convenience and accessibility of these channels, such as mobile apps, ATMs, and Point of Sale (POS) devices, have accelerated their popularity, especially in Nigeria's banking industry.

Driven by advancements in technology, cost-efficiency goals, customer service expectations, and global banking trends, Nigerian banks and fintechs have embraced electronic settlement systems. These systems rely heavily on electronic gadgets including Automated Teller Machines (ATMs), POS terminals, mobile phones, and web-based applications. Collectively known as Alternative

Banking Channels (ABCs), these platforms now handle a wide array of financial transactions, such as cash withdrawals, funds transfers, bill payments, airtime top-ups, insurance payments, and account inquiries. Most ABCs require a bank card or card information for operation, while others allow for cardless transactions. According to Agboola (2006), the emergence of these digital channels marks a significant evolution in the concept of money, often referred to as "e-money" due to their ability to perform the traditional functions of physical currency. As Khan (2018) noted, these platforms have become preferred channels for customers due to their speed, convenience, and round-the-clock availability.

However, the rise of ABCs has also created new opportunities for fraud. In 2023, actual fraud losses as a percentage of attempted fraud in Nigeria soared to 80%, up from just 3% in 2013, with the bulk of these losses attributed to e-fraud. This alarming increase highlighted the growing risks in the digital payment ecosystem. The Nigerian Inter-Bank Settlement System (NIBSS) in its 2017 fraud report further projected the likelihood of continued growth in e-fraud, due to increasing dependence on digital payments. This trend is being fueled by factors such as the rapid advancement in payment technologies, government policies like the cashless economy initiative, and the implementation of the Financial System Strategy (FSS 2020). Additionally, a growing population of tech-savvy young Nigerians continues to drive demand for electronic financial services.

Fraudulent transactions—especially those committed electronically—pose a significant threat to the stability and integrity of Nigeria's financial system. As digital transactions become more widespread, so does the complexity and frequency of fraud. This necessitates the urgent need for stronger regulatory frameworks, better fraud detection systems, and increased user awareness to safeguard the growth and performance of digital financial services in Nigeria.

2.1.2 Dimensions of Fraudulent Transactions

Fraudulent transactions in mobile money operations can be understood through three key dimensions: phishing and social engineering, SIM swap and identity theft, and account takeover fraud. Each of these represents a serious threat to the integrity and performance of mobile money services in Nigeria.

Phishing and Social Engineering: Phishing and social engineering involve the illicit use of an individual's personal information—such as their name, National Identity Number (NIN), bank account details, or mobile money login credentials—to impersonate them for fraudulent purposes, typically to gain financial advantage (Smith, 2018). In mobile money operations, fraudsters may use these tactics to gain access to user accounts and conduct unauthorized withdrawals or fund transfers. This form of fraud undermines customer trust, leads to business losses, and compels operators to invest heavily in cybersecurity

infrastructure. Additionally, it exposes mobile money operators to legal, regulatory, and reputational risks.

SIM Swap and Identity Theft: SIM swap and identity theft is another prevalent form of fraud in which criminals manipulate telecom systems or exploit third-party agents to gain control over a user's mobile number. This form of fraud is sometimes confused with card skimming, where fraudsters clone data from a debit or credit card. In the mobile money context, the fraudster gains access to a user's linked accounts by assuming control of their mobile line, often without the user's knowledge (Barker & D'Amico, 2023). This enables unauthorized transactions that may go undetected until significant financial losses occur. For mobile money operators, such fraud leads to chargebacks, system downtimes, and customer dissatisfaction, all of which impact their financial and operational performance.

Account Takeover Fraud: Account takeover fraud occurs when fraudsters gain unauthorized control of a user's financial account and use it to conduct illicit transactions. Although Levi and Reuter (2006) originally described it in the context of money laundering, this concept has evolved with mobile money platforms becoming convenient channels for such criminal activity. Due to their fast, relatively anonymous, and often cross-border nature, mobile money systems are increasingly exploited to move and conceal illegally obtained funds. Operators involved in such activities, even unintentionally, may face regulatory sanctions, suspension of operating licenses, and severe damage to their public image.

2.2 Fraudulent Transactions and Financial Performance

Several studies have explored the link between fraud and financial performance, particularly within the Nigerian banking and financial services sector. Idowu (2019) examined the causes of fraud in Nigerian banks and found that poor management practices, inadequate working conditions, prolonged job assignments, and low staff remuneration were major contributors to fraud incidents. These conditions created frustration among staff, which in turn, increased the likelihood of fraudulent behavior.

Similarly, Adepoju and Alhassan (2018) noted that while bank customers had grown to rely on Automated Teller Machines (ATMs) for convenience, a significant rise in ATM-related fraud had undermined this trust. They emphasized the importance of risk management strategies in curbing such fraud, especially given that fraudulent tactics had become more sophisticated over time.

Akindele (2018), in his study on the challenges associated with ATM usage in Nigeria, argued that lack of proper training, communication gaps, and poor leadership were central to the occurrence of fraud in banks. He recommended

robust internal control systems and measures to improve employee welfare as necessary strategies for fraud reduction.

Further, Abdulrasheed, Babaitu, and Yinusa (2012) investigated the impact of fraud on bank profitability. Their findings revealed a significant negative relationship between the amount of money lost to fraud and bank profits, indicating that fraud directly impairs financial performance. Kanu and Okorafor (2013) also examined the economic implications of fraud on bank deposits in Nigeria using descriptive and inferential statistics. Their analysis of data from 1993 to 2018 showed a strong positive relationship between fraudulent activities and the depletion of deposit funds, with fraudulent withdrawals constituting a large portion of losses.

In another study, Aruomoaghe and Ikyume (2013) focused on how fraud undermines the accuracy of financial reporting. They found that failure to report fraudulent activities in financial statements results in misleading reports, which can distort stakeholders' decision-making. Uchenna and Agbo (2013) also assessed the impact of fraud on banking performance between 2001 and 2011, using 24 deposit money banks as case studies. Employing Pearson correlation and multiple regression analysis, they observed that fraud had a measurable negative effect on bank operations, with the highest percentage of mobilized funds lost to fraud occurring between 2001 and 2005, although this reduced significantly between 2006 and 2011.

Outside Nigeria, DeYoung (2001a, 2001b, 2001c, and 2005) systematically analyzed the performance of Internet-only banks in the U.S. Compared to traditional banks with physical branches, these digital institutions initially experienced lower profitability due to high labor costs and lower fee-based revenues. However, the study also found that Internet banks grew faster and had greater potential to achieve scale economies over time, which could lead to improved financial competitiveness. This insight is relevant for Nigerian mobile money operators, many of which operate largely through digital platforms and face similar risks of digital fraud.

2.4 Theoretical Frameworks

Thanasak (2013) states that before making any efforts to reduce fraud and manage the risks proactively, it is important for the business organizations to identify the factors leading to fraudulent behaviour by understanding who are the fraudsters, when and why frauds are committed. Various theories have attempted to explain the causes of fraud and the most cited theories are the Fraud Triangle Theory (FTT) of Cressey (1950) , Fraud scale theory by Albrecht(1983) , Hollinger-Clark theory (1984) and Fraud Diamond Theory (FDT) of Wolfe and Hermanson (2004). Both of these identify the elements that lead perpetrators to commit fraud.

2.4.1 Fraud Triangle Theory (FTT)

The Fraud Triangle Theory (FTT) was developed by Donald Cressey in 1950, building on Edwin Sutherland's earlier concept of white-collar crime introduced in 1939. Cressey, a criminologist, examined the behavior of convicted fraudsters and discovered that three key conditions must coexist for fraud to occur: perceived pressure, opportunity, and rationalization. Perceived pressure refers to the financial or personal burdens that compel an individual toward unethical behavior. Opportunity represents the circumstances that make fraudulent actions feasible—often stemming from weak internal controls. Rationalization involves the mental justification that allows the individual to regard the dishonest act as acceptable. The theory operates under the assumption that individuals are generally moral but may deviate under pressure if given the chance and a way to justify their actions. Additionally, it assumes that fraud is a deliberate, calculated behavior and that strong internal control systems can deter it by limiting opportunities.

Despite its contributions to understanding fraudulent behavior, the Fraud Triangle Theory has been criticized for its oversimplification of the fraud phenomenon. Critics argue that it fails to account for other influential factors such as greed, entitlement, organizational culture, and collusion. It also tends to generalize all fraudulent acts as the result of situational pressure, ignoring cases involving malicious intent or repeat offenders. Nonetheless, this theory remains highly relevant to the present study, offering a foundational framework for identifying fraud risks by examining psychological and environmental conditions within an organization. It provides useful insights for management in preventing fraud by addressing employee pressures, monitoring opportunities within systems, and recognizing rationalizations. However, the limited scope of the theory necessitates a more comprehensive model that accounts for broader behavioral and systemic complexities in fraud detection and prevention.

A major gap in the Fraud Triangle Theory is its narrow focus on only three elements, which limits its effectiveness in addressing the full spectrum of fraudulent behaviors. The theory overlooks key psychological and contextual dimensions such as individual greed, toxic organizational culture, and habitual unethical tendencies. As a result, while the model provides a foundational understanding of fraud, it must be extended to encompass additional variables. In this study, the Fraud Triangle Theory is adapted but enhanced to provide a broader and more effective framework for detecting and preventing fraud, especially within complex organizational settings.

2.4.3 Hollinger-Clark Fraud Study

The Hollinger-Clark Fraud Study, conducted by Hollinger and Clark in 1983, provides an empirical perspective on employee theft. Surveying over 10,000 workers, the study identified job dissatisfaction—not financial need—as the primary driver of theft in the workplace. The research highlighted that

environmental factors such as poor management practices and unsatisfactory job conditions significantly influence employee behavior. Younger employees were observed to have a higher propensity for theft, especially when they had easier access to company assets. Importantly, the study concluded that formal organizational controls alone are insufficient deterrents; rather, increasing the perception of detection has a stronger deterrent effect.

The study operates on the assumption that most employees, when dissatisfied or under certain pressures, may resort to dishonest acts. It suggests that self-interest often overrides ethical considerations if environmental conditions permit. It also assumes that managerial behavior and workplace morale significantly shape employee integrity. However, a major critique of the study is its overreliance on the employer's role in addressing employee needs—even when dealing with inherently dishonest or greedy individuals. The research fails to probe deeply into the root causes of dissatisfaction or recognize the diversity of employee motivations and ethical orientations.

Although the Hollinger-Clark study makes significant contributions by linking workplace conditions to theft, it places disproportionate emphasis on the employer's responsibility to prevent fraud through job satisfaction. The study does not fully investigate the underlying reasons behind dissatisfaction, especially among employees who may be dishonest regardless of working conditions. This limits the explanatory power of the model for understanding fraud driven by greed or deliberate intent. Nevertheless, this study is incorporated into the present research to support a broader assessment of how management practices, employee engagement, and ethical leadership can contribute to effective fraud detection and prevention strategies.

2.5 Empirical Literature Review

Several investigations into fraud in the public and private banking sectors have been conducted around the world. According to Swain & Pani (2016), who published a report titled Frauds in Indian Banking: Aspects, Reasons, Trend Analysis, and Suggestive Measures, frauds in the Indian banking sector have been on the rise in India over the previous several years. Negligence by responsible officers, a lack of seriousness, lack of understanding among bank employees, non-compliance with Reserve Bank of India (RBI) KYC rules, and rising pressure on personnel about the same are some of the key causes of bank fraud.

According to (Kanu, S. I., & Okoroafor, 2013), the factors of fraud are classified according to the environment, including technological, legal, human, social, and management factors. Technological causes, according to his research, are those that have been made conceivable by technological innovation. Legal reasons of fraud are those that make fraud more likely as a result of an ineffective legal system. The actions or omissions of an organization's management that lead to fraud are known as management causes of fraud. Individuals who commit fraud owing to a lack of character development as a result of a poor upbringing are

known as personal reasons of fraud. The social causes of fraud are those that are reinforced by bad societal values, such as when the society idolizes a wealthy individual without questioning his or her sources of money.In a Study to Investigate the Reasons for Bank Frauds and the Implementation of Preventive Security Controls in the Indian Banking Industry, Khanna, A., & Arora (2019) found that workers' level of awareness is insufficient to avoid various frauds. There is a lack of training, overworked workers, competitiveness, and a low degree of employee compliance.

According to OgudaNdege, Odhiambo Albert and John Byaruhanga (2024) investigated the Effect of Internal control on Fraud Prevention and Detection in District treasuries of Kakamega Country. The study propose hypothesis to test the relationship between internal control systems and Fraud Detection and Prevention. The study sampled 31 key respondents out of 122 populations with the acceptance range of 20% sample determination, the sample include district accountant, district internal auditors and head department, and used close ended questionnaire.The response analyzed by using Pearson Correlation. The study result shows there is a significant positive relationship between internal control systems and fraud detection and prevention.

Yalew (2021) as cited in Olongo, did a study on the influence of fraud risk management practices in commercial banks and their effect on fraud risk exposure. The objective of the study was to hunt out the effect of fraud risk management practices on fraud prevention and fraud detection in commercial banks in Kenya, the researcher used descriptive research design and the sample size was 30 commercial banks. The results of the study establish that loans fraud, cheque related fraud, account opening fraud, computer fraud and credit card fraud are the most common in Kenya banking industry.

In the Nigerian banking industry, Abdulrasheed & Yinusa (2012) investigated the impact of fraud on bank performance. The study employed a vector error correction model using quarterly data from 2002 to 2013. It also focused on the fraud triangle theory. According to the study, the number of employees participating in fraud has a large positive influence on return on assets, however the quantity of fraud perpetrated and the number of employees involved in fraud both have a negative impact on bank performance.

Within the period 2001-2011, Beatrice (2023), conducted a study on the influence of fraud and fraudulent behaviors on bank performance in Nigeria. The research design was evaluated, and multiple regression analysis was employed to investigate the impact of fraud on bank performance. According to the survey, weak controls are the leading source of fraud and fraudulent activity.

According to Yego & John (2016), in their paper ‘‘The Impact of Fraud in the Banking Industry: A Case of Standard Chartered Bank’’, fraud has become one of the most serious problems in the world today, and it is unlikely to go away very soon, Because of the scams, it is impacting the profitability of enterprises as well as the firm's solvency. However, continual monitoring and verification can help to

reduce the risk of fraud to some level. According to Kundu, S., &Rao (2023), in their paper Reasons of Banking Fraud – A Case of Indian Public Sector Banks. Customers want banks to provide them with openness, accountability, fairness, and effective intermediation. One of the most difficult tasks facing modern bankers is safeguarding public funds and people's trust.

Khanna, A., & Arora (2019), conducted research into the causes of bank fraud in the Indian banking sector. The study's goal was to determine the factors that contribute to bank fraud. Through cluster sampling, 253 employees from various banks were chosen for the study. Lack of training, overburdened staff, competition, and inadequate compliance (the extent to which procedures and prudential policies defined by the Federal Reserve Bank of India to prevent frauds are followed) are the key causes of bank frauds, according to the study.

Fikru (2018) the banks and regulatory authorities have proposed and allowed internal control measures to check the practice of bank fraud. But the effectiveness of any internal control system is dependent on how fluid the system interacts with itself and how embedded it is into the organization ‘s business processes. This paper examines the issues of effective internal control vs. fraud Detection and prevention in the Ethiopian banking industry by adopting primary data. Using a survey method, this work examined how the internal control systems in the Ethiopian banks have aided in combating or preventing fraud in the banking industry. To do this the study examines the effectiveness of internal control in Ethiopian banking industry and based on that effectiveness the researcher test the effectiveness of ICs in preventing and detection of fraud in Ethiopian banking industry. Among the findings were those internal control techniques employed by banks in checking fraud have been effective but put marks on some improvements and the final conclusion of this study is that there is a significant relationship between internal control system (control environment, risk assessment, control activity, information and communication and monitoring) and fraud.

Kalkidan (2017) this study focused on assessment of fraud control practice in the case of Dashen Bank. The research has applied descriptive statistics by using questionnaires and document review. To undertake the research simple random sampling is used to select respondents from branches and purposive type of sampling was used to select 27 branches out of 109 branches found in Addis Ababa. 185 questionnaires were distributed in which 183 of them returned. Data were analyzed using descriptive statistics using SPSS software. The result indicates that there are fraud cases but the rate is low and internal control in the bank is 21 not effective. There is a deficiency in controlling component mainly the risk assessment and information and communication component. Comparing to risk and information communication control environment, control activities and monitoring practice are good. Employees do not have adequate awareness about anti-fraud policy, and the controlling mechanisms used by the bank are not enough to prevent fraudulent activities.

As mentioned in the previous studies, bank fraud is on the rise in various countries on a daily basis. However, those studies do not particularly address bank fraud in Nigeria, which is why the researcher wishes to investigate bank fraud in Nigeria.

3. Research Methodology

This study population consisted of all agents of Opay and MTN MoMo of the Mobile money operators in Nigeria to avoid bias representation, the study has 933 populations, Sample size determination, to avoid the problem of response biases and to increase the response rate for the study, the researcher uses Taro Yemane formula to determine a sample size at a 95% confidence level and P = 0.5 are assumed for Equation. 308 sample size of respondents with a buffer margin of 10% was derived from a total population of 933 employees of Mobile money operators in Nigeria

3.1 Reliability and validity

To ensure the reliability of the instrument, a pilot study was carried out on in some of the departments.

The pilot test enables the researcher to ascertain the degree of clarity of the questions and also to remove bias and ambiguity in the data questionnaire.

Summary - KMO and Bartlett's Test		
Overall Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		**0.814**
Bartlett's Test of Sphericity	Approx. Chi-Square	**2089.69**
	TVE	**0.704**
	Df	**10**
	Sig.	**0.000**
Overall Reliability Statistics: Cronbach's Alpha		**0.825**

3.2 Data Analysis Technique

The hypotheses formulated in Chapter One is tested using Regression analysis with the help of STATA Version 13.0 because of the fitness and robustness of the model. First, reliability analysis and Confirmatory Factor Analysis (CFA) were conducted to ensure that all the measurement items are robust and reliable. Factor loadings for, dimensions and performance assessed using This technique is considered appropriate because it can be used to assess complex and multiple relationships between more variables in this case (fraudulent transactions and performance) all at the same time. Structural equation modeling as indicated by current research is the most reliable instrument used in measuring the relationship between. fraudulent transactions variables and performance.

Model Specification

The general model of the study is expressed as:

$Y = f(X)$ ---------- (1)

Where Y = performance

X = fraudulent transactions

But X = F (IT, CS and ML) - - - - - - - - (2)

Where: PSE = Phishing and social engineering ,SIT = SIM swap and Identity Theft, ATF = Account takeover fraud

Y and X are as defined above

α = Constant

β = Coefficient of X

e = error term

$OP = \alpha_1 + \beta_1 PSE + \beta_2 SIT + \beta_3 ATF + e_1$ - - - - - - - - - - - (3)

Where:

β_1-β_2= coefficients of X_1 respectively.

4. Data Presentation and Analysis

To gather the needed data for this study, 308 survey questionnaires of the mobile money operators in Nigeria were sent out, and 294 were filled out and returned. Out of the 294 returned questionnaires, 12 were incomplete and were accordingly discarded. Thus, the valid returned questionnaires are 282, representing 95.9%, and the valid returned questionnaires discarded are 12, representing 4.1%.

The mean values of the variables (performance) are 3.655 and 3.778, respectively, which approximate 2, suggesting that respondents agreed with workers in the Mobile money operators in Nigeria under study's fraudulent transactions.

4.1 Correlation Matrix of Dependent and Independent Variables

Variables	P	PSE	SIT	ATF
P	1.000	0.2854	0.2344	0.2385
PSE		1.000	0.2222	0.2134
SIT			1.000	0.2156
ATF				1.000

Source: STATA Output 2025

The **positive correlations** among the variables indicate that increases in fraudulent transaction incidents (PSE, SIT, ATF) are **positively related** to changes in performance. Though this seems counterintuitive, the regression model helps to clarify the interpretation.

4.2 Regression Results

Multiple regression method:

The summary of the regression results for each model is shown in the Tables below

Table: Summary of regression result for model (performance)

Variable	Coefficient (β)	Std. Error	t-value	p-value	95% Confidence Interval
Constant (α)	1.3381	0.0277	4.03	0.000	[1.0057, 2.6992]
Phishing and social engineering (PSE)	0.3457	0.0328	2.51	0.000	[0.2794, 0.4211]
SIM swap and Identity Theft (SIT)	0.1562	0.0175	6.99	0.000	[0.1177, 0.2599]
Account takeover fraud (ATF)	0.2531	0.0154	7.52	0.000	[0.2578, 0.4265]

Source: STATA Output

Model Fitness (R-squared and F-statistic)

R^2 = 0.600: This means that 60% of the variation in **Performance (P)** can be explained by the three predictors (PSE, SIT, ATF). This is a fairly strong explanatory power for a social science model.

F-statistic p-value = 0.000: This indicates that the overall regression model is statistically significant. In other words, at least one of the independent variables has a significant effect on performance.

4.3 Discussion of Findings

a. Phishing and Social Engineering (PSE): The regression coefficient for phishing and social engineering (0.3457) indicates a significant and positive effect on the performance of mobile money operators. This result suggests that, in response to increasing phishing threats, operators may have invested in stronger identity management systems such as Know Your Customer (KYC) protocols and biometric verification. These measures, although initially implemented to counter fraud, have likely contributed to improved operational efficiency and user trust. Additionally, heightened awareness and improved internal fraud detection may have led to enhanced organizational responsiveness and resilience.

b. SIM Swap and Identity Theft (SIT):he positive coefficient (0.1562) for SIM swap and identity theft also suggests a statistically significant association with improved performance. This may be attributed to the fact that incidents involving SIM swaps and identity theft often prompt system upgrades, increased employee training, and implementation of more advanced monitoring tools. Over time, these efforts may enhance the adaptability and robustness of mobile money operators, leading to better service delivery and risk preparedness.

c. Account Takeover Fraud (ATF): Account takeover fraud shows a significant and positive impact on performance, as reflected in its coefficient of 0.2531. This could be due to increasing regulatory pressure compelling mobile money operators to adopt more rigorous anti-account takeover frameworks, including Anti-Money Laundering (AML) measures. Compliance with these regulations often requires streamlining internal processes, improving reporting structures, and enhancing due diligence practices—all of which contribute to better operational discipline and governance.

5. Conclusion

This study investigated the impact of various forms of fraudulent transactions—phishing and social engineering (PSE), SIM swap and identity theft (SIT), and account takeover fraud (ATF)—on the performance of mobile money operators in Nigeria. Interestingly, the results deviate from conventional expectations, revealing that these fraud risks, rather than negatively affecting performance, are positively and significantly related to it.

The significant positive relationship between phishing and social engineering (coefficient = 0.3457) and performance implies that the threat of fraud has compelled operators to invest in sophisticated identity verification systems, including biometric authentication and real-time fraud monitoring. These initiatives, while designed to combat fraud, have also improved operational workflows and customer confidence.

Similarly, the positive influence of SIM swap and identity theft (coefficient = 0.1562) suggests that operators are responding proactively with infrastructure upgrades, capacity-building initiatives, and smart monitoring solutions, which in turn enhance system resilience and adaptability.

Account takeover fraud (coefficient = 0.2531) has also shown a positive performance impact, likely driven by regulatory demands from bodies such as the Financial Action Task Force (FATF) and the Central Bank of Nigeria (CBN). These pressures have led operators to introduce stricter internal controls, transparent governance structures, and enhanced due diligence mechanisms. As a result, organizations have improved in terms of compliance, stakeholder trust, and sustainable operations.

In essence, while fraudulent transactions present significant risks, the responsive actions taken by mobile money operators—ranging from technological investments to regulatory compliance—appear to enhance performance outcomes. These responses transform challenges into opportunities for innovation, system strengthening, and long-term competitiveness.

5.1 Recommendations

Based on the study's findings, the following recommendations are proposed to strengthen the performance of mobile money operators in the face of fraudulent transactions:

Enhance Identity Verification Systems: Operators should invest in multi-layered identity authentication technologies such as biometric verification, artificial intelligence-powered fraud detection, and behavioral analytics. These tools are crucial not only for mitigating phishing and social engineering but also for improving system reliability and user trust.

Strengthen Card and SIM Security Infrastructure: To combat SIM swap and identity theft, it is recommended that mobile money operators adopt secure payment technologies such as EMV-compliant terminals, promote the use of virtual cards, and implement periodic training for agents and staff on card data protection and cybersecurity best practices.

Upgrade Anti-Account Takeover (AML) Frameworks: Operators should refine their AML strategies by automating suspicious activity reporting (SARs), integrating intelligent transaction monitoring systems, and maintaining close collaboration with regulatory agencies to ensure compliance and real-time oversight.

References

1. *Abdulrasheed, A., & Yinusa, D. O. (2012). The impact of fraud on bank performance in Nigeria. [Study employed a vector error correction model using quarterly data from 2002 to 2013].*
2. *Abdulrasheed, A., Babaitu, I., & Yinusa, S. (2012). Fraud and profitability in Nigerian banks. International Journal of Business and Social Science, 3(3), 53–59.*
3. *Adepoju, A., & Alhassan, A. (2018). The impact of ATM fraud on customer trust in Nigerian banks. African Journal of Banking and Finance, 10(1), 22–35.*
4. *Agboola, A. A. (2006). Electronic payment systems and tele-banking services in Nigeria. Journal of Internet Banking and Commerce, 11(3), 1–10.*
5. *Akindele, R. I. (2018). Challenges of ATM usage in Nigerian banking sector. Journal of Banking Operations, 3(2), 55–67.*
6. *Albrecht, W. S. (1983). Fraud and the accounting profession. Journal of Accountancy, 156(6), 77–84.*
7. *Aruomoaghe, A., &Ikyume, A. N. (2013). Fraud and financial reporting accuracy in Nigeria. Journal of Accounting and Auditing Research, 8(2), 41–50.*
8. *Association of Certified Fraud Examiners (ACFE). (n.d.). Report to the nations on occupational fraud and abuse. ACFE.*
9. *Barker, R., & D'Amico, L. (2023). Digital identity theft and mobile fraud in developing economies. Journal of Financial Crime, 30(2), 156–174.*
10. *Beatrice, O. O. (2023). The influence of fraud and fraudulent behaviors on bank performance in Nigeria (2001–2011). [Unpublished study using multiple regression analysis].*

11. *Cressey, D. R. (1950). Other people's money: A study in the social psychology of embezzlement. Free Press.*
12. *DeYoung, R. (2005). The financial performance of Internet banks. Journal of Financial Services Research, 27(3), 273–291.*
13. *Fikru, M. G. (2018). Internal control and fraud prevention in Ethiopian banking industry: Evidence from primary data. [Unpublished manuscript].*
14. *Hollinger, R. C., & Clark, J. P. (1983). Theft by employees. Lexington Books.*
15. *Idowu, A. (2019). Causes of fraud in Nigerian banks and its effects on banking operations. Journal of Accounting and Financial Management, 5(1), 43–56.*
16. *Kalkidan, M. (2017). Assessment of fraud control practice: A case study of Dashen Bank. [Unpublished master's thesis].*
17. *Kanu, C., &Okorafor, G. (2013). The economic implications of bank fraud in Nigeria. International Journal of Financial Research, 4(3), 43–51.*
18. *Kanu, S. I., & Okoroafor, G. C. (2013). The nature, extent and economic impact of fraud on bank performance in Nigeria. Interdisciplinary Journal of Contemporary Research in Business, 4(9), 253–265.*
19. *Khan, M. (2018). Electronic banking and customer satisfaction in Nigeria. International Journal of Banking and Finance, 7(4), 112–125.*
20. *Khanna, A., & Arora, B. (2019). A study to investigate the reasons for bank frauds and the implementation of preventive security controls in the Indian banking industry. International Journal of Advanced Research in Computer Science, 10(1), 1–6.*
21. *Kundu, S., & Rao, P. (2023). Reasons of banking fraud – A case of Indian public sector banks. International Journal of Management Studies, 10(2), 45–52.*
22. *Legal Practitioner. (2013). Legal definition and implications of electronic fraud in Nigeria. Nigerian Bar Journal, 9(2), 78–90.*
23. *Levi, M., & Reuter, P. (2006). Money laundering. Crime and Justice, 34(1), 289–375.*
24. *Nigeria Electronic Fraud Forum (NEFF). (2011). Annual report on electronic fraud in Nigeria. Central Bank of Nigeria Publications.*
25. *Nigerian Inter-Bank Settlement System (NIBSS). (2017). Annual fraud report. Retrieved from: nibss-plc.com.ng*
26. *OgudaNdege, O., Odhiambo, A., & Byaruhanga, J. (2024). Effect of internal control on fraud prevention and detection in district treasuries of Kakamega County. International Journal of Finance and Accounting, 13(1), 19–30.*
27. *Smith, J. (2018). Phishing and social engineering in mobile transactions. Cybersecurity and Information Systems Journal, 6(2), 84–99.*
28. *Swain, R. K., & Pani, S. (2016). Frauds in Indian banking: Aspects, reasons, trend analysis and suggestive measures. International Journal of Management and Applied Science, 2(12), 12–18.*
29. *Thanasak, T. (2013). Fraud prevention and detection: A data mining approach. International Journal of Computer Applications, 80(3), 24–31.*

30. *Uchenna, E. A., & Agbo, A. E. (2013). Fraud and banking performance in Nigeria: 2001–2011. Journal of Finance and Banking Research, 6(4), 87–103.*
31. *Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. CPA Journal, 74(12), 38–42.*
32. *Yalew, M. (2021). As cited in Olongo, A. (2021). Fraud risk management practices and their effect on fraud risk exposure in Kenyan commercial banks. Journal of Financial Crime, 28(4), 1212–1225.*
33. *Yego, K., & John, B. (2016). The impact of fraud in the banking industry: A case of Standard Chartered Bank. European Journal of Business and Management, 8(14), 47–56.*