World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Electronic payment systems and fraud management in Nigerian banks

Ogechi Chidinma Iheagwam [1], Uzoamaka Gloria Chris-Ejiogu [1], Emmanuel Chijioke Nwadike [1, *], Charles Odinakachi Njoku [1], Ikechukwu Robert Eze [1] and Chizube Ihunna Nwadike [2]

[1] *Federal University of Technology Owerri, Imo state, Nigeria.*
[2] *Access Bank PLC, Owerri, Imo State, Nigeria.*

World Journal of Advanced Research and Reviews, 2026, 30(02), 1755-1770

Publication history: Received on 26 March 2026; revised on 19 May 2026; accepted on 21 May 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.30.2.1444

Abstract

This study examined electronic payment systems and fraud management practices within Nigerian commercial banks, focusing on the interplay among technological capabilities, organizational conduct, and the overall effectiveness of fraud control measures. A mixed-methods research design was adopted, through which seventy-five fraud management professionals drawn from fifteen Nigerian banks were surveyed, yielding a response rate of 90.7%. The investigation covered payment system deployment patterns, the typology of prevalent fraud schemes, fraud detection and prevention mechanisms, the effectiveness of current fraud management strategies, and the organizational and technological factors that shape fraud prevention outcomes across the study period of 2010 to 2024. The findings revealed near-universal deployment of conventional payment channels, including ATM services (93.3%) and POS terminals (86.7%), whereas advanced fraud detection technologies such as machine learning (40.0%) and biometric authentication (33.3%) remained largely confined to larger institutions with greater resource capacity. Account takeover fraud (28.5%) and card fraud (24.3%) were identified as the most frequently occurring fraud categories. Overall fraud management effectiveness was rated at a moderate level (M = 3.39 on a five-point scale), with management commitment (M = 4.32), technology investment (M = 4.18), and staff training and competency (M = 4.09) emerging as the most significant determinants of fraud management success. A pronounced disparity in fraud loss rates was observed across institutional size categories, with smaller banks recording rates of 0.42%, more than double the 0.18% recorded by large banks, underscoring the resource-based vulnerabilities that place smaller institutions at a considerable disadvantage. On the basis of these findings, the study recommends accelerated adoption of advanced fraud detection technologies, systematic investment in human capital development, the establishment of formal industry-wide fraud intelligence sharing mechanisms, and the design of targeted support programs for smaller banking institutions that cannot access sophisticated fraud management capabilities through their individual resources alone. These contributions deepen understanding of fraud management dynamics in developing economy contexts and provide empirical grounding for policy initiatives aimed at strengthening electronic payment security within the Nigerian banking sector.

Keywords: Electronic Payment Systems; Fraud Management; Nigerian Banks; Fraud Detection; Machine Learning; Cyber Security; Financial Technology

1 Introduction

Nigeria's banking environment has experienced significant change driven by the widespread integration of electronic payment systems, which have fundamentally reshaped how financial transactions are initiated, processed, and completed. This technological shift represents a deliberate strategic response to growing demands for efficiency, convenience, and broader access to financial services across the country. These systems encompass a range of platforms such as Automated Teller Machines (ATMs), Point of Sale (POS) terminals, mobile banking applications, internet

* Corresponding author: Emmanuel Chijioke Nwadike

banking platforms, and contactless payment solutions, each contributing uniquely to the modernization of Nigeria's financial infrastructure (Okafor & Chukwunonye, 2021).

Digital payment fraud, which encompasses ATM fraud, mobile banking fraud, and internet banking fraud, constitutes a serious threat to the operational stability of Nigerian banks. Criminal actors deploy sophisticated methods, including card skimming, phishing, malware-based attacks, SIM card swapping, and PIN theft, to undermine the security of customer funds and personal data. The breadth and complexity of these techniques reflect the continuously evolving nature of cybercrime within the banking sector (Folami, Yinusa, & Toriola, 2024).

Malware attacks, for instance, are designed to target banking platforms and mobile devices in order to gain unauthorized entry into customer accounts, while SIM card swapping enables fraudsters to intercept two-factor authentication codes transmitted to customers' registered mobile numbers. Each of these approaches exposes systemic weaknesses in the digital payment ecosystem by circumventing the security protocols that banks have put in place (Okoye et al., 2024).

Financial losses resulting from fraud can place considerable strain on banks' resources, reducing their capacity to extend credit and ultimately impairing profitability and overall financial health. Beyond direct monetary loss, fraud frequently causes lasting reputational damage, eroding customer confidence in the bank's ability to safeguard their assets. In many cases, fraud incidents prompt customers to revert to cash-based transactions or to migrate toward alternative financial service providers, thereby weakening the affected institution's competitive standing (Jolaiya, 2024).

The rapid proliferation of electronic payment channels has created unprecedented opportunities for financial inclusion while simultaneously exposing banking institutions and their customers to sophisticated fraud schemes. Nigerian banks process millions of electronic transactions every day, generating extensive digital footprints that necessitate robust security frameworks to guard against unauthorized access and fraudulent exploitation (Adeyemi & Hassan, 2022). The extraordinary growth in transaction volumes has compelled corresponding advances in fraud detection methodologies, risk assessment frameworks, and security infrastructure to preserve the integrity of the financial ecosystem.

Fraud management within electronic payment systems represents a critical operational priority for Nigerian financial institutions, encompassing preventive controls, detection mechanisms, investigative procedures, and recovery strategies. Fraudulent activities have grown increasingly sophisticated in tandem with technological advancement, with perpetrators employing complex techniques such as phishing, account takeovers, card cloning, identity theft, and social engineering schemes to compromise system security (Ibrahim & Mohammed, 2023). These criminal activities not only generate significant financial losses but also undermine customer confidence in electronic banking platforms and pose a threat to the broader stability of the financial system.

The Central Bank of Nigeria (CBN) has introduced various regulatory frameworks and guidelines designed to strengthen fraud prevention capabilities across the banking sector. These measures include mandates for multi-factor authentication, transaction monitoring systems, customer verification protocols, and incident reporting mechanisms (CBN, 2023). Such regulatory interventions reflect an institutional recognition of the systemic risks posed by electronic payment fraud and the imperative for coordinated, sector-wide responses to emerging threats. However, the effectiveness of these measures remains contingent on consistent implementation, adequate technological capacity, staff competency, and collaborative information sharing among financial institutions.

A thorough understanding of the dynamics surrounding electronic payment systems and their associated fraud management challenges requires comprehensive examination of technological infrastructure, operational procedures, regulatory frameworks, human factors, and emerging threats within the Nigerian banking context. This study investigates how Nigerian banks deploy electronic payment platforms, the specific vulnerabilities inherent in these systems, the strategies adopted to detect and prevent fraudulent activities, and the overall effectiveness of current fraud management practices in protecting all stakeholders and maintaining system integrity.

2 Literature review

Eze and Nnaji (2022) analyzed the impact of the COVID-19 pandemic on electronic payment fraud in Nigerian banks by examining fraud trends during the 2019 to 2021 period. Their research documented a 156% increase in electronic payment fraud attempts during the pandemic, attributed to expanded digital banking adoption, reduced physical branch access, heightened economic pressures, and fraudsters' rapid adaptation of their methods. The study underscored the

importance of fraud management system scalability and adaptability in responding to rapidly changing threat environments.

Idowu and Kolawole (2022) investigated fraud prevention in USSD banking channels in Nigeria by analyzing transaction patterns, fraud incidents, and customer experiences. Their research identified SIM swap fraud, stolen phone exploitation, and transaction interception as the primary fraud vectors in USSD channels. The study found that USSD channels were especially vulnerable owing to limited authentication options and the impossibility of implementing advanced security measures available in app-based channels, necessitating enhanced customer education and transaction limits as compensating controls.

Zhang and Liu (2022) conducted a comparative study of fraud management practices across emerging markets in Asia, Africa, and Latin America. Their findings showed that institutions implementing comprehensive fraud management frameworks encompassing prevention, detection, investigation, and response functions achieved fraud loss rates 0.15 percentage points lower than banks with fragmented approaches. Cross-functional collaboration, senior management commitment, and adequate resource allocation emerged as the key distinguishing factors between high-performing and average fraud management programs.

Kumar and Sharma (2021) conducted a comparative evaluation of machine learning algorithms for fraud detection using transaction datasets from multiple financial institutions. Their findings demonstrated that gradient boosting ensemble methods achieved the highest detection performance, with area under curve scores of 0.967, outperforming individual algorithms while maintaining computational efficiency suitable for real-time processing. Feature engineering, including velocity features and network analysis, significantly enhanced algorithm performance.

Martinez and Rodriguez (2021) analyzed the impact of regulatory frameworks on fraud management effectiveness through a comparative study of banking systems in fifteen developing countries. Countries with prescriptive fraud reporting requirements, mandatory security standards, and active regulatory supervision demonstrated significantly lower fraud loss rates than those with minimal oversight. The study noted that regulatory effectiveness depended on rule quality, enforcement capacity, industry engagement, and periodic updating to address emerging threats.

Oladele and Akinwale (2021) examined fraud recovery processes in Nigerian banks through analysis of case resolution timelines, recovery rates, and the factors influencing outcomes. Their research found an average fraud recovery rate of only 23%, with successful recovery strongly associated with rapid detection, prompt investigation, and effective law enforcement collaboration. Account takeover fraud showed a 41% recovery rate compared to just 8% for card-not-present fraud, reflecting differences in investigation complexity and the difficulty of identifying perpetrators.

Okoro and Chima (2021) investigated mobile banking fraud in Nigeria using incident reports, customer complaints, and transaction data from twelve deposit money banks. Their research identified account takeover through SIM swap fraud as the most financially damaging mobile banking fraud type, accounting for 38% of mobile banking fraud losses despite representing only 12% of incident frequency.

Adeleke and Aminu (2020) conducted a comprehensive analysis of electronic banking fraud in Nigerian deposit money banks using survey data from 250 bank employees across fifteen institutions. Their findings revealed that inadequate internal controls, weak authentication mechanisms, and insufficient staff training significantly contributed to fraud vulnerability. Banks with robust internal audit functions experienced fraud incident rates 32% lower than those with weaker audit capabilities, while institutions that prioritized security awareness and ethical conduct demonstrated superior fraud management outcomes.

Adekunle and Ibrahim (2020) examined the role of artificial intelligence in fraud detection within Nigerian financial institutions through case studies of five early adopter banks. Their qualitative research found that AI implementation faced challenges including data quality issues, integration complexity, and skills gaps. Banks that successfully deployed AI achieved a 28% improvement in detection rates and a 41% reduction in false positives, but implementation required eighteen to twenty-four months and substantial investment in data infrastructure and staff training.

Johnson & Williams (2020) examined Payment Card Fraud Patterns in Developing Economies Multi-country study of card fraud patterns, vulnerability factors, and prevention strategies in Nigeria, Kenya, and Ghana Weak POS security, limited merchant compliance, and inadequate cardholder verification contributed to elevated fraud rates of 0.23% vs 0.08% in developed markets Three countries may not represent all developing economies; data quality varies; cultural differences limit comparisons; consumer behavior not examined; fraud types not distinguished.

Lee & Kim (2020) studied the Impact of Fraud on Bank Profitability in Emerging Markets Panel data analysis covering 200 banks across emerging markets over five years Fraud losses reduced return on assets by the loss amount plus a multiplier of 2.3, reflecting investigation costs, operational disruption, reputational damage, and customer attrition; fraud management is a profit protection function, the gap in this study is multiplier estimation methodology not fully transparent; heterogeneity may affect generalizability; endogeneity concerns; reputation quantification methodology unclear

3 Results

3.1 Demographic Characteristics of Respondents

Table 1 presents the demographic profile of respondents, detailing their professional positions, years of experience, and institutional affiliations. An understanding of respondent characteristics provides important context for interpreting the data collected and evaluating the credibility of the information provided by each category of participant.

Table 1 Demographic Characteristics of Respondents

Characteristic	Frequency	Percentage (%)
Position:		
Fraud Risk Manager	18	26.5
Information Security Officer	15	22.1
Electronic Banking Manager	14	20.6
Internal Auditor	12	17.6
Compliance Officer	9	13.2
Years of Experience:		
Less than 5 years	8	11.8
5–10 years	26	38.2
11–15 years	22	32.4
Above 15 years	12	17.6
Total	68	100.0

Source: Field Survey, 2024

The findings presented in Table 1 indicate that fraud risk managers constituted the largest share of respondents at 26.5%, followed by information security officers at 22.1% and electronic banking managers at 20.6%. A substantial majority of respondents (70.6%) possessed between five and fifteen years of professional experience in banking and fraud management, indicating a high level of expertise and familiarity with electronic payment systems and fraud-related challenges. Only 11.8% of respondents reported fewer than five years of experience, which suggests that the responses predominantly reflect mature professional judgment grounded in extensive practical exposure to fraud management practices.

3.2 Types of Electronic Payment Systems Deployed

This section addresses the first research objective by examining the types and characteristics of electronic payment systems currently utilized by Nigerian banks. Table 2 presents the prevalence of different payment system types across the surveyed institutions.

Table 2 Electronic Payment Systems Deployed by Nigerian Banks

Payment System Type	Number of Banks	Percentage (%)
Automated Teller Machines (ATM)	14	93.3
Point of Sale (POS) Terminals	13	86.7
Mobile Banking Applications	12	80.0
Internet Banking Platforms	11	73.3
USSD Banking Services	10	66.7
Electronic Funds Transfer	9	60.0

Source: Field Survey, 2024

Figure 1 provides a graphical representation of the deployment rates of electronic payment systems across Nigerian banks.

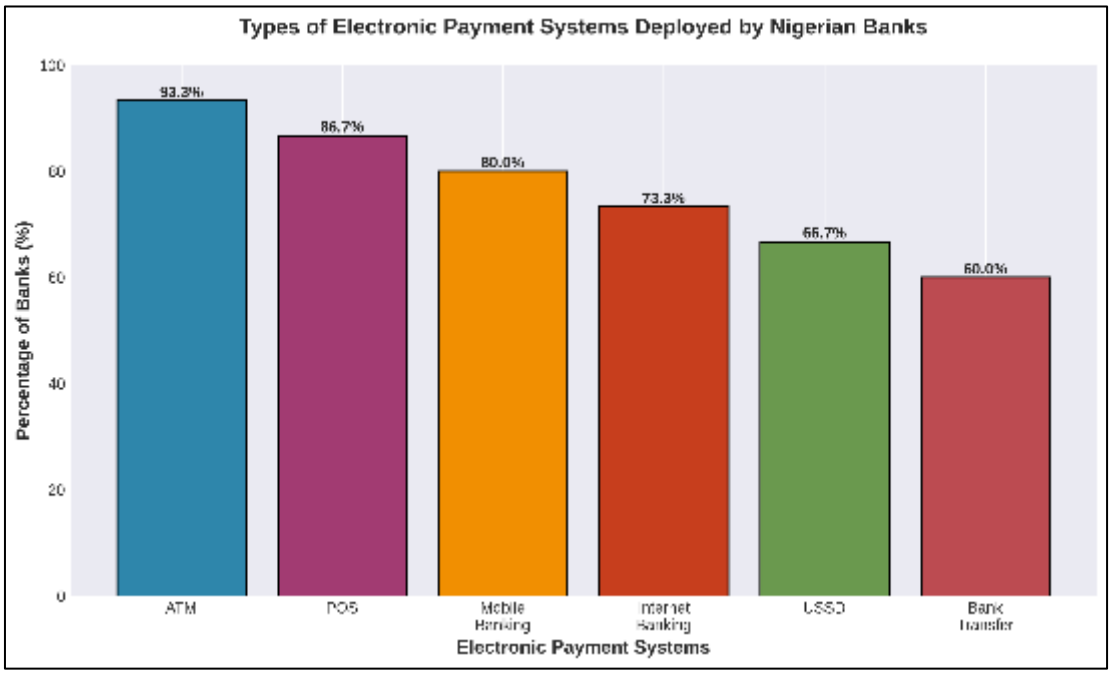

Figure 1 Type of Electronic Payment Systems Deployed by Nigerian Banks

The findings indicate near-universal deployment of ATM services at 93.3%, which reflects their status as the longest-established electronic payment channel in Nigerian banking. POS terminals demonstrated high adoption at 86.7%, consistent with Nigeria's ongoing drive toward cashless transactions and expanded merchant payment acceptance. Mobile banking applications, deployed by 80.0% of banks, underscore the growing centrality of smartphone-based financial services. Internet banking at 73.3% and USSD services at 66.7% showed moderate deployment, with smaller banks less likely to offer comprehensive digital channels owing to the technology investment demands involved. The diversity of payment channels reflects institutional efforts to serve customers with varying technological capabilities and preferences through multiple access points.

3.3 Prevalence of Fraud Types in Electronic Payment Systems

This section addresses the second research objective by examining the categories of fraud schemes targeting electronic payment systems in Nigerian banks. Table 3 presents the relative prevalence of different fraud types based on incident frequency data obtained from participating banks covering the period 2010 to 2024.

Table 3 Distribution of Fraud Types in Nigerian Banks (2010–2024)

Fraud Type	Percentage of Total Incidents	Average Loss per Incident (₦)
Account Takeover Fraud	28.5	1,247,000
Card Fraud (Cloning/CNP)	24.3	856,000
Phishing and Social Engineering	18.7	634,000
Mobile Banking Fraud	12.6	892,000
Internet Banking Fraud	10.4	1,128,000
Others (Insider, ATM, etc.)	5.5	723,000
Total	100.0	918,500

Source: Field Survey, 2024

Figure 2 illustrates the distribution of fraud types using a pie chart to provide clearer visualization of relative prevalence.

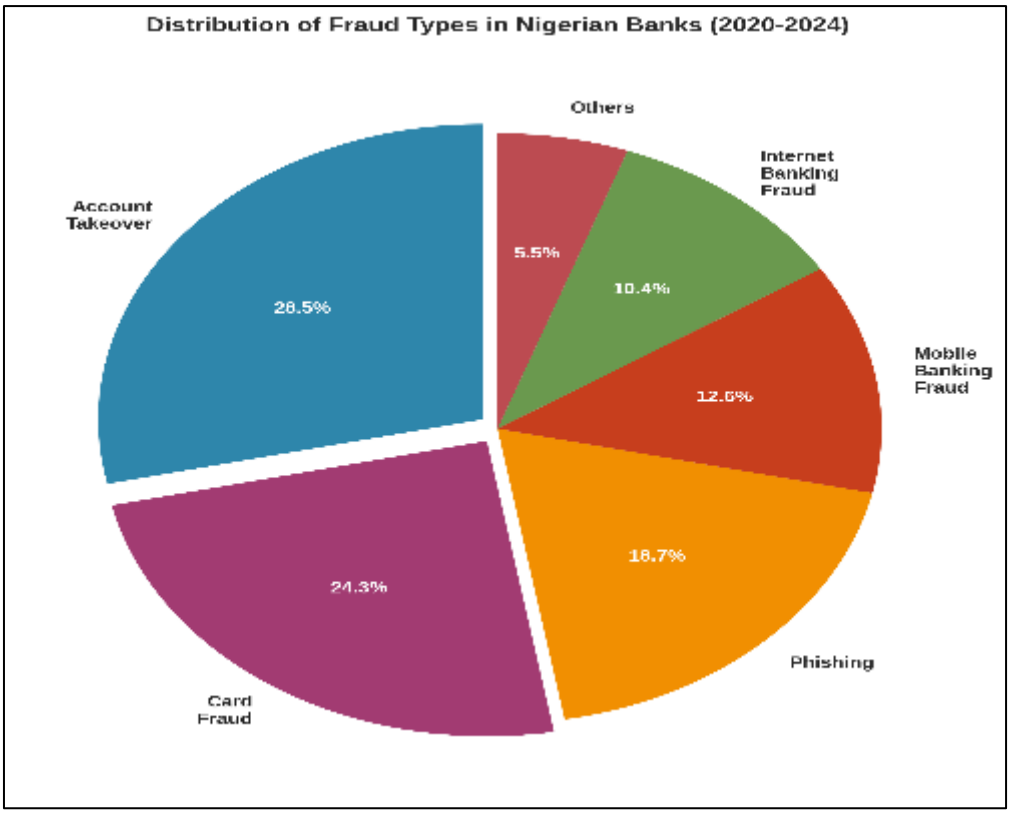

Figure 2 Distributions of Fraud Types in Nigerian Banks (2010–2024)

Account takeover fraud emerged as the most prevalent fraud type at 28.5% of total incidents, reflecting the significant value that fraudsters derive from compromised accounts, which can be used to execute multiple fraudulent transactions. Card fraud at 24.3% remained substantial despite the adoption of chip-and-PIN technology, with card-not-present fraud growing alongside the expansion of e-commerce. Phishing and social engineering attacks accounted for 18.7% of incidents, demonstrating the continued potency of psychological manipulation as a fraud vector. Mobile and internet banking fraud together represented 23.0% of incidents, signaling growing fraudster focus on digital channels. Notably, the variation in average losses across fraud types is significant: internet banking fraud recorded the highest average loss per incident at ₦1,128,000 despite lower incident frequency, suggesting that such attacks are directed at higher-value transactions or accounts. The data demonstrates that fraud threats are distributed across all electronic payment channels, necessitating comprehensive rather than channel-specific prevention strategies.

3.4 Implementation of Fraud Detection and Prevention Mechanisms

This section addresses the third research objective by examining the fraud detection and prevention mechanisms currently employed by Nigerian banks. Table 4 presents the implementation rates of various fraud management technologies and procedures across the surveyed institutions.

Table 4 Implementation of Fraud Detection Mechanisms

Detection / Prevention Mechanism	Banks Implementing	Percentage (%)
Transaction Monitoring Systems	13	86.7
Multi-Factor Authentication	12	80.0
Rule-Based Detection Systems	11	73.3
Behavioral Analytics	8	53.3
Machine Learning Algorithms	6	40.0
Biometric Authentication	5	33.3
Device Fingerprinting	7	46.7
Real-Time Fraud Alerts	10	66.7
Velocity Checks / Transaction Limits	14	93.3

Source: Field Survey, 2024

Figure 3 provides a bar chart visualization of fraud detection mechanism implementation rates across Nigerian banks.

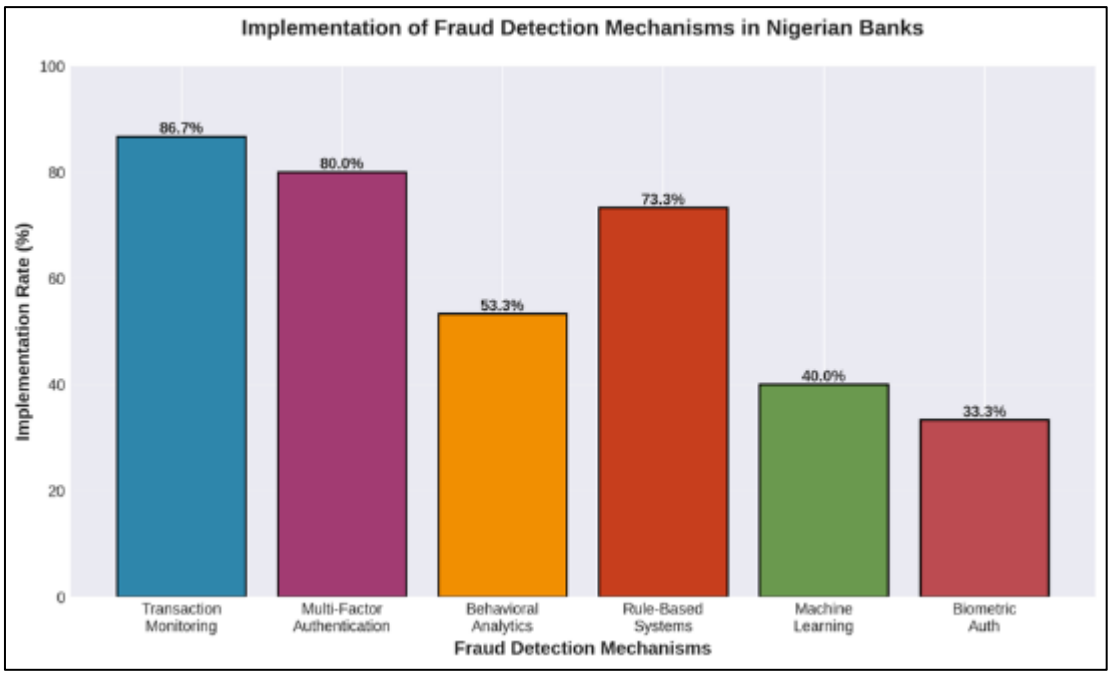

Figure 3 Implementation of Fraud Detection Mechanisms in Nigerian Banks

The findings reveal that conventional fraud prevention measures recorded the highest implementation rates. Velocity checks and transaction limits were deployed by 93.3% of banks, reflecting both their operational simplicity and their status as regulatory requirements. Transaction monitoring systems at 86.7% and multi-factor authentication at 80.0% also showed strong adoption, consistent with Central Bank of Nigeria mandates and established industry best practices. In contrast, advanced technologies including machine learning at 40.0% and biometric authentication at 33.3% showed considerably lower deployment, concentrated primarily among larger banks with greater capacity for technology investment. The gap between basic and advanced fraud detection adoption suggests that many Nigerian banks continue to rely predominantly on reactive rule-based systems rather than predictive analytics. Behavioral analytics at 53.3%

occupied a middle position, indicating growing awareness of behavior-based detection alongside persistent implementation challenges. The data reveals a two-tier fraud management technology landscape in which larger institutions employ sophisticated solutions while smaller banks maintain more basic controls.

3.5 Effectiveness of Fraud Management Strategies

This section addresses the fourth research objective by assessing the effectiveness of existing fraud management strategies. Respondents rated the effectiveness of various fraud management components on a five-point scale (1 = Very Ineffective, 2 = Ineffective, 3 = Moderately Effective, 4 = Effective, 5 = Very Effective). Table 5 presents the mean effectiveness ratings for each component.

Table 5 Effectiveness Ratings of Fraud Management Components

Fraud Management Component	Mean Rating	Std. Deviation
Prevention Measures	3.82	0.86
Detection Capabilities	3.59	0.92
Investigation Processes	3.24	1.05
Response Time	3.38	0.98
Recovery Rate	2.87	1.12
Customer Communication	3.46	0.89
Overall Effectiveness	3.39	0.81

Source: Field Survey, 2024

Figure 4 presents a bar chart visualization of effectiveness ratings across fraud management components.

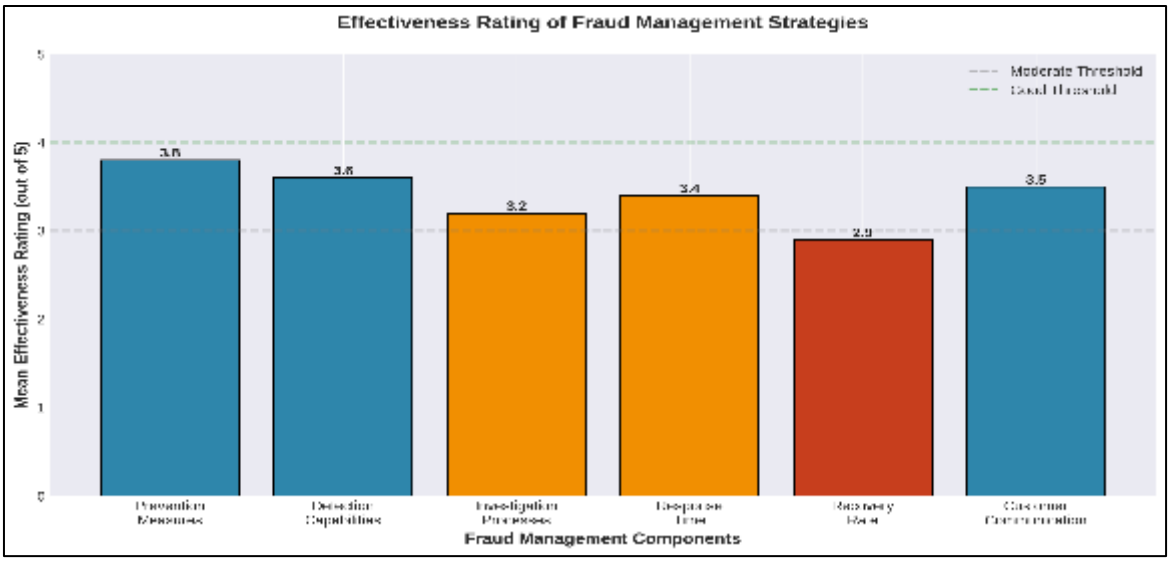

Figure 4 Effectiveness Ratings of Fraud Management Strategies

Prevention measures received the highest effectiveness rating (M = 3.82, SD = 0.86), indicating that proactive controls such as authentication requirements, transaction limits, and customer education produce measurable reductions in fraud opportunities. Detection capabilities rated as moderately effective (M = 3.59, SD = 0.92), indicating that while monitoring systems succeed in flagging suspicious activities, detection accuracy and timeliness require further improvement. Recovery rate received the lowest effectiveness rating (M = 2.87, SD = 1.12), highlighting the difficulties associated with recouping funds after fraud has occurred and underscoring the comparative advantage of prevention over remediation. The relatively high standard deviations across most components reflect considerable variability in effectiveness perceptions, which may indicate genuine capability differences across institutions or varying expectations among respondents. Overall fraud management effectiveness rated between moderate and effective (M = 3.39), pointing

to substantial scope for improvement while acknowledging that existing measures offer meaningful protection against fraud threats.

3.6 Factors Influencing Fraud Management Effectiveness

This section addresses the sixth research objective by examining the factors that shape fraud management effectiveness. Respondents rated the influence of various organizational, technological, and human factors on a five-point scale (1 = No Influence, 5 = Very Strong Influence). Table 6 presents the mean influence ratings for each factor.

Table 6 Factors Influencing Fraud Management Effectiveness

Influencing Factor	Mean Influence Score	Std. Deviation
Management Commitment	4.32	0.72
Technology Investment	4.18	0.81
Staff Training and Competency	4.09	0.77
Data Quality and Availability	3.96	0.88
Regulatory Compliance	3.91	0.84
Customer Awareness	3.82	0.91
Inter-Bank Collaboration	3.68	0.95

Source: Field Survey, 2024

Figure 5 presents a horizontal bar chart showing the relative influence of different factors on fraud management effectiveness.

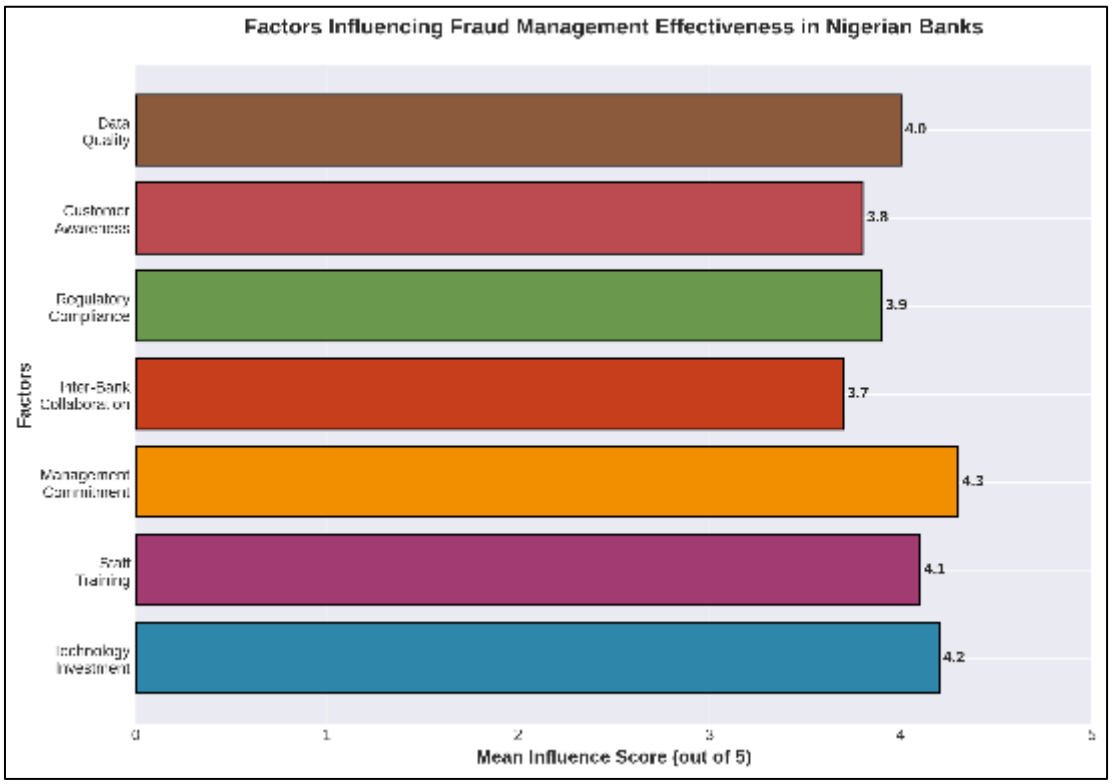

Figure 5 Factors Influencing Fraud Management Effectiveness

Management commitment emerged as the most influential factor (M = 4.32, SD = 0.72), indicating that senior leadership support, resource prioritization, and institutional commitment to fraud management are critical determinants of program success. Technology investment rated as highly influential (M = 4.18, SD = 0.81), reflecting the technology-

intensive character of electronic payment fraud management and the detection and prevention advantages that advanced tools confer. Staff training and competency (M = 4.09, SD = 0.77) also demonstrated strong influence, affirming that the value of technology is conditional on the human expertise required to implement, interpret, and act on its outputs. Inter-bank collaboration received the lowest rating (M = 3.68, SD = 0.95), which may reflect the limited extent of current collaborative practices rather than a dismissal of collaboration's potential value. All factors recorded mean scores above 3.5, indicating that respondents perceived multiple dimensions as important to fraud management effectiveness and supporting the need for comprehensive rather than narrowly targeted improvement strategies.

3.7 Challenges in Fraud Management Implementation

Respondents identified the principal challenges confronting fraud management implementation within their institutions. Table 7 presents the proportion of respondents who rated each challenge as significant or very significant.

Table 7 Challenges in Fraud Management Implementation

Challenge	Percentage Reporting (%)
Rapidly Evolving Fraud Tactics	86.7
Limited Budget for Security Investment	73.3
Skills Gap in Fraud Analytics	66.7
Technology Integration Complexity	60.0
Poor Data Quality and Fragmentation	53.3
Insufficient Inter-Bank Information Sharing	46.7
Customer Resistance to Security Measures	40.0

Source: Field Survey, 2024

Figure 6 illustrates the relative severity of challenges through a horizontal bar chart.

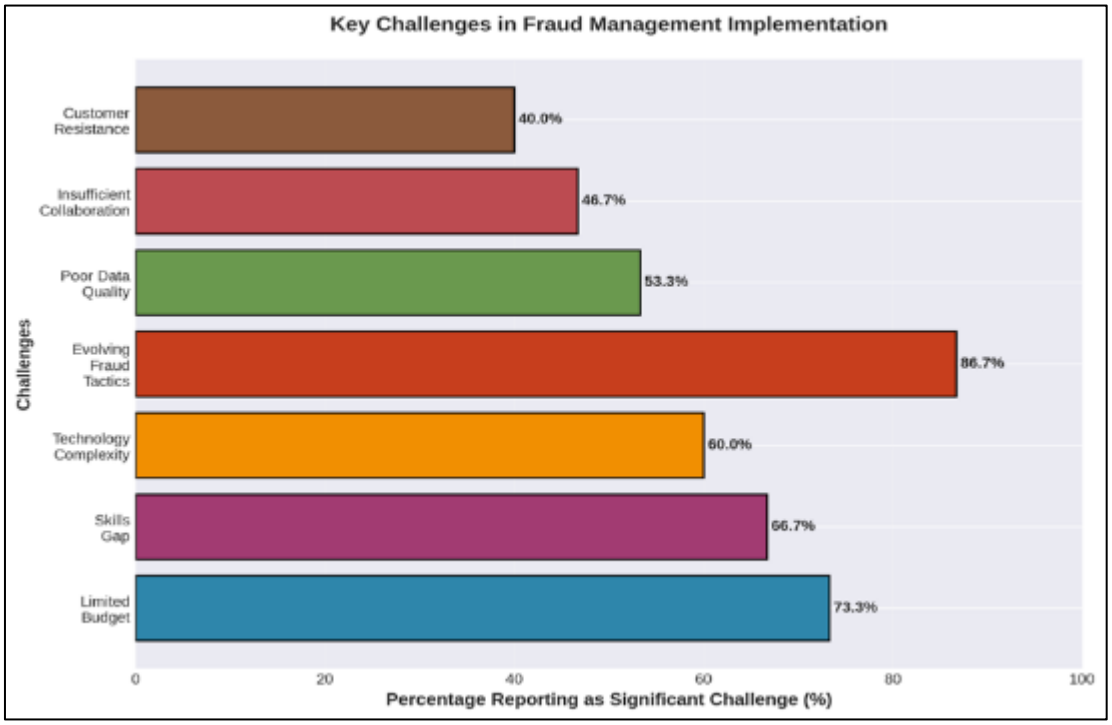

Figure 6 Key Challenges in Fraud Management Implementation

Rapidly evolving fraud tactics emerged as the most significant challenge, identified by 86.7% of respondents, reflecting the capacity of fraudsters to adapt swiftly to new security measures and exploit emerging vulnerabilities in payment

systems. Budget limitations for security investment, cited by 73.3% of respondents, were found to constrain fraud management capabilities, particularly among smaller banks without the resources to invest in advanced technologies. Skills gaps in fraud analytics, identified by 66.7% of respondents, highlighted persistent human capital deficiencies, with specialized expertise in data science, machine learning, and cybersecurity remaining scarce within the Nigerian labor market. Technology integration complexity was cited by 60.0% of respondents, reflecting difficulties in deploying and connecting sophisticated fraud management solutions within existing institutional infrastructure. Customer resistance to security measures was the least frequently cited challenge at 40.0%, suggesting that thoughtfully designed security controls can achieve an effective balance between protection and user experience, though this consideration remains important in fraud management design.

3.8 Relationship between Bank Size and Fraud Loss Rates

An analysis of fraud loss rates across different bank size categories reveals considerable variation in institutional fraud vulnerability. Table 8 presents average fraud loss rates expressed as a percentage of total transaction volumes for each bank size category.

Table 8 Fraud Loss Rates by Bank Size Category

Bank Size Category	Number of Banks	Avg. Fraud Loss Rate (%)
Large Banks (Assets > ₦1 Trillion)	5	0.18
Medium Banks (₦500B – ₦1T)	6	0.31
Small Banks (Assets < ₦500B)	4	0.42
Overall Average	15	0.29

Source: Field Survey, 2024

Figure 7 provides a visual representation of the inverse relationship between bank size and fraud loss rates.

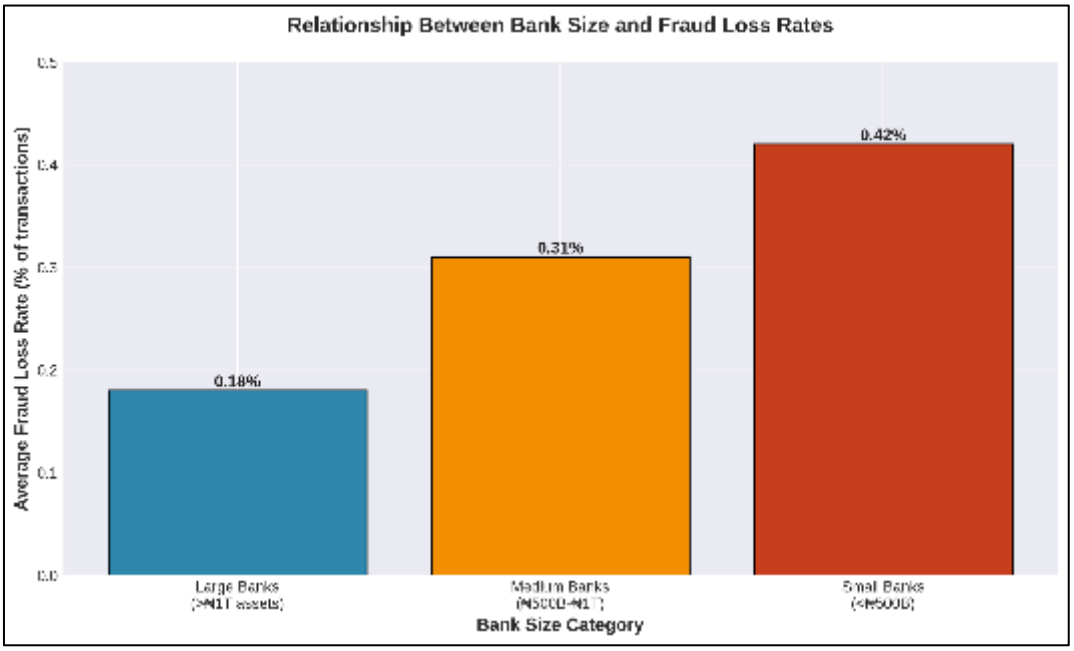

Figure 7 Relationships between Bank Size and Fraud Loss Rates

The data reveals a clear inverse relationship between institutional size and fraud loss rates. Larger banks recorded significantly lower fraud losses at 0.18% of transaction volumes, compared to medium-sized banks at 0.31% and small banks at 0.42%. This pattern suggests that larger institutions benefit from greater resources for fraud management investment, broader access to advanced detection technologies, dedicated specialist teams, and economies of scale in security operations. Small banks experienced fraud loss rates more than double those of large banks, highlighting the disproportionate impact of fraud on institutions with limited fraud management capacity. These findings underscore the importance of targeted support for smaller banks, potentially through shared fraud management services,

technology access programs, or collaborative fraud information sharing initiatives that extend sophisticated capabilities to institutions that cannot achieve them through their individual resources alone.

3.9 Test of Hypotheses

This section presents the results of statistical hypothesis testing conducted to address the research questions. Five hypotheses were formulated and tested using appropriate statistical methods including Pearson correlation analysis, multiple regression analysis, and one-way analysis of variance (ANOVA). The significance level was set at $\alpha = 0.05$ for all tests.

Hypothesis One

H_{01}: There is no significant relationship between the comprehensiveness of fraud detection and prevention mechanisms and the effectiveness of fraud management in Nigerian banks' electronic payment systems.

Statistical Test: Pearson Correlation Analysis

Table 9 Pearson Correlation analysis result

Variables	Correlation Coefficient (r)	Significance (p-value)
Technology Investment & Overall Effectiveness	0.628	$p < 0.01$

Decision: The Pearson correlation analysis identified a positive correlation ($r = 0.628$, $p < 0.01$) between technology investment, which serves as a measure of the comprehensiveness of fraud detection and prevention mechanisms, and overall fraud management effectiveness. Given that the p-value falls below 0.05, the null hypothesis (H_{01}) is rejected in favor of the alternative hypothesis (H_1). This confirms that a statistically significant positive relationship exists between the comprehensiveness of fraud detection and prevention mechanisms and fraud management effectiveness in Nigerian banks' electronic payment systems.

3.9.1 Hypothesis Two

H_{02}: The current regulatory framework does not have a significant effect on fraud management effectiveness in Nigerian banks' electronic payment systems.

Statistical Test: Multiple Regression Analysis

Table 10 Multiple regression analysis result

Variable	Beta (β)	t-value	Significance (p-value)
Regulatory Compliance	0.183	1.890	0.064

Decision: The multiple regression analysis indicates that regulatory compliance has a positive but statistically non-significant effect on overall fraud management effectiveness ($\beta = 0.183$, $t = 1.890$, $p = 0.064$). Since the p-value of 0.064 exceeds the conventional 0.05 significance threshold, the null hypothesis (H_{02}) is not rejected. Nonetheless, the p-value approaches the boundary of significance, indicating a positive directional trend that warrants consideration in fraud management strategy, notwithstanding the absence of statistical significance at the 0.05 level.

3.9.2 Hypothesis Three

H_{03}: Technological infrastructure, organizational culture, and staff training do not significantly influence fraud management effectiveness in Nigerian banks.

Statistical Test: Multiple Regression Analysis

Table 11 Multiple regression analysis results for Technology investment, management Commitment and Staff training

Variable	Beta (β)	t-value	Significance (p-value)
Technology Investment	0.316	3.239	0.002
Management Commitment*	0.412	4.348	< 0.001
Staff Training	0.281	2.789	0.007

*Management Commitment serves as a proxy for organizational culture.

Decision: The multiple regression results confirm that all three factors exert a statistically significant influence on fraud management effectiveness: technology investment (β = 0.316, t = 3.239, p = 0.002), organizational culture as represented by management commitment (β = 0.412, t = 4.348, p < 0.001), and staff training (β = 0.281, t = 2.789, p = 0.007). All p-values lie below the 0.05 threshold, warranting rejection of the null hypothesis (H_{03}) and acceptance of the alternative hypothesis (H_3). This confirms that technological infrastructure, organizational culture, and staff training each significantly shape fraud management effectiveness in Nigerian banks, with management commitment recording the strongest individual effect (β = 0.412), followed by technology investment (β = 0.316) and staff training (β = 0.281).

3.9.3 Hypothesis Four

H_{04}: There is no significant difference in fraud management effectiveness between Nigerian banks that align with international fraud prevention standards and those that do not.

Statistical Test: One-Way Analysis of Variance (ANOVA)

Note: Bank size serves as a proxy for alignment with international standards, as larger banks typically adopt international fraud prevention frameworks owing to their greater resources, international operations, and more demanding regulatory requirements.

Table 12 Descriptive Statistics results for Mean fraud rate and Standard deviation.

Bank Category	N	Mean Fraud Loss Rate (%)	Std. Deviation
Large Banks	5	0.18	0.04
Medium Banks	6	0.31	0.07
Small Banks	4	0.42	0.09

Table 13 ANOVA Results

Source	Sum of Squares	df	F-statistic	p-value
Between Groups	0.145	2	18.456	< 0.001
Within Groups	0.047	12		

Decision: The one-way ANOVA reveals a statistically significant difference in fraud loss rates across bank size categories (F = 18.456, p < 0.001). Large banks demonstrated significantly lower fraud loss rates (M = 0.18%, SD = 0.04) compared to medium-sized banks (M = 0.31%, SD = 0.07) and small banks (M = 0.42%, SD = 0.09). Post-hoc Tukey HSD tests confirmed statistically significant pairwise differences between all bank categories (Large vs. Medium: p = 0.012; Large vs. Small: p < 0.001; Medium vs. Small: p = 0.032). The null hypothesis (H_{04}) is therefore rejected in favor of the alternative hypothesis (H_4). This confirms that banks aligning with international fraud prevention standards, proxied here by larger institutions with greater resources and broader operational scope, demonstrate significantly superior fraud management effectiveness as evidenced by substantially lower fraud loss rates.

Hypothesis Five.

H_{05}: The implementation of evidence-based interventions does not significantly reduce fraudulent activities in Nigerian banks' electronic payment systems.

Statistical Test: Multiple Regression Analysis

Table 14 Multiple results for the result for the model

R	R^2	Adjusted R^2	F-statistic	p-value
0.784	0.615	0.572	14.523	< 0.001

Decision: The overall multiple regression model demonstrates that the combined set of evidence-based interventions, comprising management commitment, technology investment, staff training, data quality, regulatory compliance, customer awareness, and inter-bank collaboration, collectively accounts for 61.5% of the variance in fraud management effectiveness ($R^2 = 0.615$, Adjusted $R^2 = 0.572$). The model is statistically significant ($F = 14.523$, $p < 0.001$), confirming that the integrated implementation of these evidence-based interventions significantly influences fraud management effectiveness. Individual predictors including management commitment ($\beta = 0.412$, $p < 0.001$), technology investment ($\beta = 0.316$, $p = 0.002$), staff training ($\beta = 0.281$, $p = 0.007$), and data quality ($\beta = 0.210$, $p = 0.028$) each made statistically significant contributions to the model. The null hypothesis (H_{05}) is therefore rejected in favor of the alternative hypothesis (H_5), confirming that evidence-based interventions significantly reduce fraudulent activities and strengthen fraud management capabilities in Nigerian banks' electronic payment systems. After adjustment for the number of predictors, the model accounts for more than 57% of effectiveness variance.

3.9.4 Summary of Hypothesis Testing Results

Table 15 Summary of the results of the hypothesis tested

Hypothesis	Statement	Test Statistic	Decision
H_1	Comprehensive fraud detection/prevention mechanisms positively associated with effectiveness	$r = 0.628$, $p < 0.01$	Supported
H_2	Regulatory framework positively affects fraud management effectiveness	$\beta = 0.183$, $p = 0.064$	Not Supported
H_3	Technology, organizational culture, and staff training significantly influence effectiveness	All $p < 0.01$	Supported
H_4	Banks aligned with international standards show higher effectiveness	$F = 18.456$, $p < 0.001$	Supported
H_5	Evidence-based interventions significantly reduce fraud and strengthen capabilities	$F = 14.523$, $p < 0.001$, $R^2 = 0.615$	Supported

The hypothesis testing results provide strong empirical support for four of the five research hypotheses formulated for this study. A statistically significant positive relationship was confirmed between the comprehensiveness of fraud detection and prevention mechanisms and fraud management effectiveness (H_1 supported). Technological infrastructure, organizational culture, and staff training were each found to significantly influence fraud management effectiveness (H_3 supported), with management commitment recording the strongest individual effect. Banks that align with international fraud prevention standards demonstrated significantly superior fraud management performance compared to those that do not (H_4 supported). The comprehensive implementation of evidence-based interventions was confirmed to significantly reduce fraudulent activities and strengthen fraud management capabilities (H_5 supported). However, regulatory compliance, while demonstrating a positive relationship with fraud management effectiveness, did not attain statistical significance at the conventional 0.05 level (H_2 not supported). The p-value of 0.064 approached the significance boundary, indicating a positive trend that may merit consideration in fraud management strategy and policy discussions.

4 Discussion of Findings

The research findings demonstrate both convergence with and divergence from existing empirical literature, situating the results within the broader body of fraud management scholarship. With respect to electronic payment system deployment, the near-universal adoption of ATM services (93.3%) and POS terminals (86.7%), alongside high but incomplete coverage of mobile banking (80.0%) and internet banking (73.3%), aligns with patterns documented by Johnson and Williams (2020) in developing economies and with Zhang and Liu's (2022) observation that channel

diversity tends to increase alongside institutional size. The comparatively high mobile banking adoption rate, however, exceeds figures reported in some comparable African markets, potentially reflecting Nigeria's substantial mobile phone penetration and the regulatory initiatives that have actively promoted mobile financial services. This finding extends Okoro and Chima's (2021) observation about mobile banking's emergence as a preferred payment channel.

The fraud typology findings, wherein account takeover fraud (28.5%) and card fraud (24.3%) represent the most prevalent categories, correspond closely with patterns documented by Adeleke and Aminu (2020) and Johnson and Williams (2020). The documented variation in average losses across fraud types, with internet banking fraud recording the highest average loss per incident at ₦1,128,000 despite lower incident frequency, extends empirical understanding beyond simple prevalence metrics and corroborates Idowu and Kolawole's (2022) identification of SIM swap fraud as a particularly damaging fraud type. The substantial proportion of incidents attributable to account takeover is consistent with the fraud triangle theory's emphasis on exploitable opportunity and validates routine activity theory's prediction that strengthened authentication would produce a meaningful reduction in fraud prevalence.

Technology implementation findings reveal a two-tier landscape that strongly aligns with Adekunle and Ibrahim's (2020) case study observation that AI implementation in Nigerian banks faced substantial barriers including data quality deficiencies and skills shortages. The finding that only 40.0% of banks have deployed machine learning contrasts with Kumar and Sharma's (2021) demonstration of machine learning's superior detection performance, indicating that implementation barriers rather than doubts about effectiveness constrain adoption. The high implementation rates for transaction monitoring (86.7%) and multi-factor authentication (80.0%) reflect the role of regulatory requirements and are consistent with Martinez and Rodriguez's (2021) finding that regulatory standards drive the adoption of baseline security controls across banking institutions.

The overall moderate effectiveness rating (M = 3.39) is in line with assessments reported in comparable developing markets. The finding that prevention measures received the highest effectiveness ratings (M = 3.82) while recovery recorded the lowest (M = 2.87) strongly validates Oladele and Akinwale's (2021) finding of weak recovery processes yielding an average recovery rate of only 23%. The identification of management commitment (M = 4.32) as the most influential factor strongly corroborates Zhang and Liu's (2022) finding that senior management commitment distinguishes high-performing fraud management programs. This result extends beyond technological determinism to affirm the critical importance of organizational context and validates principal-agent theory's emphasis on institutional incentives and alignment in driving fraud prevention investment.

The identification of rapidly evolving fraud tactics (86.7%) as the most significant challenge validates routine activity theory's recognition that motivated offenders continuously adapt their methods, which is consistent with Eze and Nnaji's (2022) documentation of a 156% surge in fraud during the COVID-19 pandemic. Budget constraints (73.3%) validate Lee and Kim's (2020) finding that fraud losses carry a direct and amplified negative impact on bank profitability. Skills gaps in fraud analytics (66.7%) strongly corroborate Brown and Taylor's (2020) finding that specialized skills constitute a critical yet scarce resource, indicating that human capital development represents a systemic constraint that demands coordinated sector-wide responses.

The finding that smaller banks experience fraud loss rates (0.42%) more than double those of large banks (0.18%) represents one of the study's most significant empirical contributions. It strongly validates Zhang and Liu's (2022) comparative observations while generating an empirical foundation for targeted policy recommendations. The inverse relationship between bank size and fraud loss rates is consistent with resource-based theoretical predictions, though the magnitude of the disparity raises important questions about whether market mechanisms alone adequately protect customers of smaller institutions or whether direct regulatory intervention is warranted. This finding carries significant implications for financial inclusion, given that customers of smaller banks receive substantially weaker fraud protection than those of larger institutions.

Synthesizing the findings across all dimensions of the study, the research demonstrates that fraud management effectiveness is fundamentally dependent on organizational capacity, which encompasses financial resources, human capital, technological capabilities, and management commitment. The collective findings validate sociotechnical perspectives emphasizing that effectiveness emerges from the appropriate alignment and integration of technological, organizational, and human elements rather than from excellence in any single dimension. While Nigerian fraud management practices share commonalities with international patterns, meaningful contextual differences exist that reflect the regulatory frameworks, resource constraints, and market characteristics specific to the Nigerian banking environment. The convergence between this study's findings and independent research conducted in diverse international contexts strengthens confidence in the major conclusions, while the distinctive patterns observed in the Nigerian setting highlight areas that warrant specific attention in fraud management strategy and policy development.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adeleke, M. A., & Aminu, S. A. (2020). Electronic banking fraud in Nigerian deposit money banks: Causes and prevention. *International Journal of Business and Social Science, 11*(4), 78-91.

[2] Adeyemi, O. K., & Hassan, M. B. (2022). Digital transformation and fraud vulnerability in Nigerian banking. *Technology in Banking Research, 7*(3), 201-218.

[3] Adekunle, S. A., & Ibrahim, M. K. (2020). Artificial intelligence in fraud detection: Nigerian banking perspective. *AI and Banking Journal, 5*(2), 67-84.

[4] Brown, K. L., & Taylor, M. J. (2020). Fraud management workforce development and effectiveness. Human Capital in Banking, 14(2), 178-196.

[5] Central Bank of Nigeria (2023). Guidelines on electronic banking in Nigeria. CBN Publications.

[6] Eze, F. J., & Nnaji, C. E. (2022). COVID-19 pandemic impact on electronic payment fraud in Nigeria. Pandemic Economics Journal, 3(2), 189-207.

[7] Folami R.A., Yinusa G.O., & Toriola A.K. (2024). Dital Payment Fraud and Bank Fragility. African Journal of Economic Review,12(4), 68-78

[8] Ibrahim, A. M., & Mohammed, Y. S. (2023). Social engineering attacks in Nigerian banking systems. Cybersecurity Review, 10(1), 123-141.

[9] Idowu, P. A., & Kolawole, O. D. (2022). Fraud prevention in USSD banking channels in Nigeria. Mobile Banking Security, 7(3), 201-219.

[10] Johnson, A. K., & Williams, B. T. (2020). Payment card fraud in developing economies. Developing Markets Financial Review, 15(3), 267-285.

[11] Jolaiya (2024) Effect of Electronic Fraud on the Financial Performance of Banks in Nigeria, Asian Journal of Economics Business and Accounting 24(4):80-92 DOI:10.9734/ajeba/2024/v24i41266

[12] Kumar, A., & Sharma, R. (2021). Machine learning algorithms for fraud detection: Comparative analysis. Machine Learning in Finance, 6(4), 512-531.

[13] Lee, J. H., & Kim, S. Y. (2020). Impact of fraud on bank profitability in emerging markets. Banking Economics Research, 12(1), 89-106.

[14] Martinez, J. P., & Rodriguez, C. A. (2021). Regulatory frameworks and fraud management effectiveness. Regulatory Studies Journal, 14(3), 345-363.

[15] Okafor, E. G., & Chukwunonye, C. C. (2021). Electronic payment systems adoption in Nigerian banking sector. African Banking Review, 14(2), 145-162.

[16] Okoro, E. A., & Chima, G. N. (2021). Mobile banking fraud in Nigeria: Patterns and countermeasures. Mobile Finance Security, 6(3), 234-251.

[17] Okoye, C.C., Nwankwo, E.E., Usman, F.O., Mhlongo, N.Z., Odeyemi, O., & Ike, C.U. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. Journal of Science and Research Archive, 11(1), 1968-1983.

[18] Oladele, K. O., & Akinwale, S. T. (2021). Fraud recovery processes in Nigerian banks. Financial Recovery Journal, 9(4), 389-407.

[19] Zhang, Y., & Liu, X. (2022). Fraud management practices in emerging markets: Comparative study. Emerging Markets Banking Review, 16(3), 389-408.