Examining the Role of Digital Platforms in Mitigating Financial Fraud in Nigeria

Onyegbule, Kenneth C.[1], Ejem, Chukwu A.[2], Ogbulu, Onyemachi M.[3] Effe-Nnamdi, Ann C.[4]
Department of Banking and Finance,
Abia State University, Uturu, Nigeria
*Corresponding Author's email:
chukwu.ejem@abiastateuniversity.edu.ng
https://doi.org/10.56201/wjfir.v10.no10.2026.pg.73.94

Abstract
This study examined the role of digital platforms in mitigating financial fraud in Nigeria. The study was motivated by the increasing adoption of digital financial services, as well as the growing incidence of technology-enabled financial fraud. The study specifically examined the extent to which digital platforms contribute to the prevention and detection of financial fraud, identified the security mechanisms used in mitigating fraudulent activities, and examined the challenges affecting the effectiveness of digital platforms in fraud control. Data for this study were obtained from Central Bank of Nigeria (CBN), Nigeria Inter-Bank Settlement System (NIBSS), Nigeria Deposit Insurance Corporation (NDIC), and National Bureau of Statistics (NBS)The study adopted ARDL to evaluate the relationship between digital platform variables and financial fraud in Nigeria. The findings revealed that digital platforms play significant roles in mitigating financial fraud. The study concluded that digital platforms are essential instruments for preventing and detecting financial fraud; however, technology alone cannot completely eliminate fraudulent activities. Effective fraud mitigation requires a combination of advanced technology, strong internal controls, customer education, effective regulatory oversight, and collaboration among banks, fintech companies, telecommunications operators, and law-enforcement agencies. The study therefore recommended continuous investment in advanced fraud-detection technologies, stronger cybersecurity measures, improved customer awareness, enhanced authentication mechanisms, and greater cooperation among relevant stakeholders to reduce financial fraud and strengthen confidence in Nigeria's digital financial system.

Keywords: *Digital platforms, financial fraud, fraud mitigation, electronic banking, ARDL, Nigeria.*

1.1 Introduction

The rapid growth of digital technology has fundamentally transformed the Nigerian financial system. Digital platforms such as mobile banking applications, internet banking, automated teller machines (ATMs), point-of-sale (POS) terminals, USSD services, electronic wallets, fintech applications, and instant payment systems have improved the speed, accessibility, and convenience of financial transactions. Digital financial services have also contributed to financial inclusion by bringing formal financial services closer to previously underserved populations (Nkechika, 2022).

However, the increasing dependence on digital platforms has simultaneously created new opportunities for financial fraud and other technology-enabled crimes.

Financial fraud in Nigeria has evolved alongside developments in the banking and payment ecosystem. The movement from predominantly cash-based transactions to electronic and digital payments has shifted many fraudulent activities to technology-mediated channels. Tade (2022), for example, found that technology-mediated transactions, particularly ATM and internet-based transactions, were among the payment channels that experienced significant exposure to fraud. The study also noted that fraud attacks on Nigerian deposit money banks increased over the period examined, demonstrating the persistent nature of the problem.

The Central Bank of Nigeria (CBN, 2025) has recognized the importance of technology in both the development of the financial system and the fight against financial fraud. Through initiatives such as the Nigeria Electronic Fraud Forum (NeFF), the CBN has promoted collaboration among banks, payment service providers, regulators, and law-enforcement agencies to strengthen the security of electronic payment channels. The CBN notes that the growing adoption of electronic payment channels has also increased exposure to electronic fraud, thereby necessitating coordinated measures to protect the integrity of the payments system.

Digital platforms, however, are not only channels through which fraud can occur; they can also provide important tools for detecting, preventing, and mitigating fraudulent transactions. Technologies such as biometric identification, Bank Verification Number (BVN), transaction monitoring systems, artificial intelligence, machine-learning algorithms, multi-factor authentication, data analytics, and automated alerts can help financial institutions identify suspicious activities and intervene before losses occur. The CBN's payment-system supervision framework emphasizes real-time monitoring, stronger internal controls, authentication mechanisms, and collaboration among relevant institutions as important components of payment-system security.The emergence of more sophisticated forms of fraud makes the role of these technologies even more important. Social engineering, phishing, identity theft, account takeover, SIM-swap fraud, insider abuse, and authorized push payment (APP) fraud can exploit both technological vulnerabilities and weaknesses in users' decision-making. The CBN has identified APP fraud as an increasing concern because victims may be manipulated into voluntarily authorizing fraudulent transactions, making conventional fraud-detection mechanisms more difficult to apply. Similarly, recent research on digital payment systems in Nigeria identifies weak authentication, inadequate cybersecurity infrastructure, insider abuse, identity theft, phishing, malware, and SIM-swap fraud as important sources of digital financial crime (Aladejubelo, 2026). Consequently, the effectiveness of digital platforms in mitigating financial fraud cannot be assumed merely from their availability. Digitalization can improve fraud detection and control while simultaneously creating new vulnerabilities. Bello (2022) observes that financial digitalization has introduced substantial benefits but also creates risks that require appropriate regulatory and supervisory responses. Therefore, there is a need to examine whether the technological tools and digital platforms currently employed by Nigerian financial institutions are sufficiently effective in preventing, detecting, and responding to financial fraud. This study, therefore, examines the role of digital platforms in mitigating financial fraud in Nigeria, with particular attention to the technologies, mechanisms, challenges, and institutional measures associated with digital fraud prevention.

1.2 Statement of the Problem

Financial fraud remains a significant challenge to the integrity, efficiency, and public confidence of Nigeria's financial system despite the increasing adoption of digital technologies and the implementation of regulatory measures aimed at strengthening fraud prevention. The rapid expansion of mobile banking, internet banking, POS transactions, USSD payments, fintech services, and instant electronic transfers has increased the volume and speed of financial transactions. While these developments have improved financial accessibility and convenience, they have also expanded the attack surface available to fraudsters. Research on Nigeria's banking ecosystem indicates that technology-mediated transactions have been particularly vulnerable to fraudulent activities (Tade, 2022;). A major problem is that fraudsters are continuously adapting their methods to developments in digital financial services. Rather than relying solely on traditional forms of fraud, perpetrators increasingly employ social engineering, phishing, identity theft, account compromise, SIM swaps, cryptocurrency schemes, and other technology-enabled techniques. Recent evidence on cryptocurrency-related fraud in Nigeria demonstrates the evolving sophistication of digitally enabled financial crimes and the need for stronger scrutiny of digital financial ecosystems (Garbaa et al., 2026). The problem is further complicated by the fact that digital financial platforms can simultaneously function as tools for fraud mitigation and channels for fraud perpetration. Technologies such as automated transaction monitoring, biometric verification, BVN, multi-factor authentication, artificial intelligence, and data analytics have the potential to identify suspicious transactions and prevent unauthorized access. Nevertheless, their effectiveness may be constrained by inadequate cybersecurity infrastructure, weak implementation, insufficient customer awareness, insider involvement, poor information sharing, and the ability of fraudsters to exploit gaps between financial institutions, telecommunications companies, fintech providers, and regulatory agencies.

Another concern is the persistence of a gap between technological innovation and fraud-control capacity. The financial sector continues to introduce new digital products and payment channels at a rapid rate, while regulatory and institutional mechanisms must constantly adapt to emerging threats. The CBN has consequently emphasized the need for stronger monitoring, authentication, identity verification, and collaboration among stakeholders in protecting Nigeria's payments system. The challenge, therefore, is not simply whether digital platforms are available, but whether they are being effectively deployed and integrated into comprehensive fraud-management systems (CBN, 2025). Furthermore, the increasing incidence of social-engineering fraud raises questions about the adequacy of technology alone as a solution. Where fraudsters manipulate legitimate account holders into authorizing transactions themselves, conventional security controls may be insufficient. This creates a need for more sophisticated fraud-detection mechanisms, real-time transaction analysis, customer education, stronger authentication, and effective cooperation between financial institutions and relevant government agencies. The CBN's proposed framework for handling authorized push payment fraud illustrates the growing institutional recognition of this problem. The central problem addressed by this study, therefore, is the uncertainty regarding the extent to which digital platforms have effectively mitigated financial fraud in Nigeria despite their growing adoption and the introduction of various technological and regulatory safeguards. It is necessary to determine whether digital platforms have significantly improved fraud detection and prevention, what specific technologies contribute most to fraud mitigation, what challenges limit their effectiveness, and how financial institutions and regulatory agencies can strengthen the use of digital platforms to reduce financial fraud. Addressing these issues is important for protecting

customers, improving confidence in digital financial services, strengthening financial inclusion, and promoting the stability and integrity of Nigeria's financial system.

2. Review of Related Literature

2.1 Conceptual Review

2.1.1 Concept of Digital Platforms

Digital platforms are technology-enabled systems that facilitate interactions, transactions, communication, and the exchange of information between different users through electronic networks. In the financial sector, digital platforms provide the technological infrastructure through which individuals, businesses, financial institutions, and other organisations can access and exchange financial services electronically. Examples include mobile banking applications, internet banking, automated teller machines (ATMs), point-of-sale (POS) terminals, USSD banking, electronic wallets, fintech applications, and electronic payment platforms.

The increasing adoption of digital platforms has significantly transformed the Nigerian financial system. Traditional banking activities that previously required physical interaction can now be performed remotely and in real time. Customers can transfer funds, pay bills, purchase goods and services, check account balances, and access other financial services through mobile devices and internet-enabled platforms. According to the Central Bank of Nigeria (CBN, 2022), the development of electronic payment infrastructure has been central to the transformation of Nigeria's payment system and the expansion of digital financial services.

Digital platforms can therefore be understood from two perspectives. First, they are service-delivery mechanisms that improve the accessibility, speed, convenience, and efficiency of financial services. Second, they are information and transaction-processing systems capable of collecting, processing, and analysing large volumes of transaction data. The second function is particularly relevant to fraud mitigation because transaction data can be monitored to identify unusual patterns and suspicious activities. However, digitalisation also introduces new vulnerabilities. As financial transactions increasingly move online, fraudsters have opportunities to exploit weaknesses in authentication systems, customer behaviour, software, networks, and institutional controls. Thus, the effectiveness of digital platforms depends not only on their availability but also on the security technologies and controls incorporated into them.

2.1.2 Digital Financial Platforms in Nigeria

Digital financial platforms in Nigeria encompass a broad range of technologies and services. These include mobile banking, internet banking, POS terminals, ATMs, USSD, electronic funds transfer, mobile wallets, fintech platforms, and other electronic payment systems.

Mobile banking allows customers to access banking services through mobile devices. It provides convenience and enables transactions to be conducted without visiting a physical branch. However, mobile banking can be exposed to risks such as SIM-swap fraud, stolen credentials, malware, phishing, and unauthorized access. Internet banking enables customers to conduct banking activities through websites and online portals. Although it provides extensive functionality, it can be vulnerable to phishing, password theft, malware, identity theft, and account takeover. Tade (2022) found that technology-mediated transactions were important channels through which fraud occurred in Nigeria's banking ecosystem. Automated teller machines (ATMs) allow customers to withdraw cash and perform other banking activities without direct interaction with bank employees. Although the use of PINs, cards, biometrics, and other security mechanisms provides protection, ATM-related fraud remains a concern.

Point-of-sale (POS) platforms have become particularly important to Nigeria's cashless economy. They enable customers to make payments electronically at retail outlets and other locations. However, POS-related fraud may arise from card theft, fraudulent transactions, manipulation of terminals, identity theft, and compromise of payment credentials.

USSD banking provides access to financial services through mobile-network codes without requiring internet connectivity. It has contributed significantly to financial inclusion, particularly for customers with limited access to smartphones or reliable internet services. Nevertheless, SIM-related vulnerabilities and social engineering can expose users to fraud.

Fintech platforms have further expanded the digital financial ecosystem by providing payment, lending, savings, investment, and other financial services. Their rapid growth creates opportunities for innovation but also requires effective cybersecurity, identity verification, data protection, and regulatory oversight.

2.1.3 Concept of Financial Fraud

Financial fraud refers to the deliberate use of deception, misrepresentation, concealment, or other dishonest means to obtain money, property, financial advantage, or other benefits unlawfully. In the banking and financial sector, fraud may involve customers, employees, external criminals, or combinations of these actors. Financial fraud can occur through both traditional and digital channels. Traditional forms may include forgery, fraudulent withdrawals, manipulation of financial records, and unauthorised conversion of funds. Digital financial fraud includes phishing, identity theft, account takeover, card fraud, internet banking fraud, mobile banking fraud, SIM-swap fraud, social engineering, and fraudulent electronic transfers. Tade and Adeniyi (2020) observed that electronic fraud in Nigeria's cashless ecosystem has internal, external, and collaborative dimensions. This suggests that financial fraud cannot be attributed exclusively to external criminals. Employees, customers, third-party service providers, and other actors may contribute to the occurrence of fraud. The increasing sophistication of digital financial fraud has made conventional fraud-control mechanisms less sufficient. Fraudsters can use stolen credentials, social engineering, malware, and other techniques to circumvent traditional security controls. Consequently, financial institutions increasingly require technology-based mechanisms capable of detecting unusual behaviour and identifying fraudulent transactions in real time.

2.1.4 Concept of Fraud Mitigation

Fraud mitigation refers to the policies, procedures, technologies, controls, and practices designed to prevent, detect, investigate, respond to, and minimise the effects of fraudulent activities.

Fraud mitigation differs from fraud prevention in that mitigation encompasses measures implemented before, during, and after a fraudulent event. Prevention seeks to stop fraud from occurring, while detection seeks to identify fraudulent activities when they occur or shortly afterwards. Response and recovery mechanisms seek to limit financial losses and restore affected accounts or systems. In the context of digital financial services, fraud mitigation may involve: biometric authentication; multi-factor authentication; transaction monitoring; artificial intelligence and machine learning; real-time fraud alerts; Bank Verification Number (BVN); Know Your Customer (KYC) procedures; device and behavioural analysis; encryption; transaction limits; anomaly detection; digital forensics; customer education; cybersecurity monitoring; and cooperation between banks, fintech firms, telecommunications operators, regulators, and law-enforcement agencies.

Digital platforms can therefore serve as important instruments for fraud mitigation when these mechanisms are properly integrated into the financial system.

2.1.5 Digital Platforms and Fraud Detection

Fraud detection involves identifying transactions, behaviours, or activities that indicate possible fraudulent conduct. Traditional fraud-detection approaches often rely on predetermined rules. For example, a bank may flag a transaction because it exceeds a particular amount or originates from an unusual location. Modern digital platforms increasingly use data analytics, artificial intelligence, and machine-learning techniques to detect more complex patterns. These systems can analyse large volumes of transactions and identify deviations from a customer's normal behaviour.
Osa et al. (2025), for example, examined the application of artificial intelligence to predicting fraud and forgery in the Nigerian banking industry. Their findings demonstrated the potential of machine-learning models to predict fraud-related outcomes and provide information useful for fraud management. The major advantage of technology-driven detection is speed. A fraudulent transaction can potentially be identified within seconds rather than after substantial financial loss has occurred. However, the effectiveness of such systems depends on the quality of data, the sophistication of the algorithms, system integration, and the capacity of financial institutions to respond to alerts.

2.1.6 Digital Platforms and Fraud Prevention

Fraud prevention involves measures designed to prevent fraudulent activities before they occur. Digital platforms can support prevention through strong customer authentication, biometric verification, transaction limits, device recognition, encryption, and real-time risk assessment.
Identity-management technologies are particularly important. In Nigeria, the Bank Verification Number (BVN) initiative was introduced to strengthen customer identification and reduce identity-related financial crimes. Similarly, Know Your Customer procedures enable financial institutions to verify customer identities and monitor account activities.
Prevention also depends on customer behaviour. Fraudsters frequently exploit customers through phishing, impersonation, fake investment schemes, and other social-engineering techniques. Consequently, customer awareness and financial literacy remain important complements to technological controls.

2.1.7 Digital Platforms and Fraud Investigation

Digital platforms also facilitate the investigation of financial fraud. Electronic transactions generate digital records that can provide information about transaction amounts, timestamps, account numbers, devices, locations, and transaction histories.
Digital forensics can be used to examine electronic evidence associated with fraudulent transactions. Sanusi et al. (2026) found that integrating digital forensics with machine learning could strengthen fraud detection in Nigerian deposit money banks.
Therefore, digitalisation provides not only preventive and detective capabilities but also an evidentiary trail that can support fraud investigation, prosecution, and recovery of illicitly obtained funds.

2.1.8 Challenges Associated with Digital Fraud Mitigation in Nigeria

Despite the benefits of digital platforms, several challenges may limit their effectiveness in mitigating financial fraud in Nigeria.

Cybersecurity vulnerabilities: Digital platforms may be compromised through malware, phishing, credential theft, and other cyberattacks.
Insider fraud: Employees with legitimate access to financial systems may abuse their privileges.
Social engineering: Fraudsters may manipulate customers into voluntarily providing confidential information or authorizing fraudulent transactions.
Limited digital literacy: Customers who lack sufficient knowledge of digital security may be more vulnerable to fraudulent schemes.

Technological limitations: Poor network infrastructure, system downtime, and inadequate cybersecurity infrastructure can affect the reliability of digital fraud-control mechanisms.
Data privacy concerns: The collection and processing of large amounts of customer information create privacy and data-protection risks.
Fragmentation among stakeholders: Effective fraud mitigation requires collaboration between banks, fintech companies, telecommunications companies, regulators, and law-enforcement agencies. These challenges demonstrate that technology alone cannot completely eliminate financial fraud. Rather, digital technologies need to operate within an effective institutional, regulatory, and behavioural framework.

2.1.9 Financial Fraud and Digital Platforms

2.1.9.1 Financial Fraud

Financial fraud refers to illegal or unethical actions aimed at obtaining financial gains through deception or manipulation (Albrecht, 2018). In Nigeria, common types include ATM fraud, identity theft, cybercrime, embezzlement, and card fraud (Adeyemi & Agboola, 2020). Fraud thrives where internal controls are weak, monitoring is inadequate, and users lack awareness.

2.1.9.2 Digital Platforms in Banking

Digital platforms encompass internet banking, mobile banking, automated teller machines, and fintech applications. Adoption of digital platforms is linked to reduced human error and decreased fraud opportunity (CBN, 2023).

2.1.9.3 Fraud Detection Mechanisms

Fraud detection mechanisms include transaction monitoring, anomaly detection algorithms, AI systems, and data analytics. Onyema & Igbokwe (2019) found that banks employing these systems detected 30–40% more fraudulent transactions compared to banks relying on manual systems.

2.1.9.4 Real-Time Monitoring

Real-time monitoring involves continuous observation of transactions to detect suspicious activities instantly (Albrecht, 2018). Empirical studies in Nigeria indicate that real-time monitoring reduces fraud escalation rates by 25% (EFCC, 2022).

2.1.9.5 User Awareness

Educating users on fraud schemes and secure banking practices is crucial for minimizing vulnerability. Adeyemi & Agboola (2020) observed that user awareness amplified fraud prevention effectiveness by 15–20%, showing that technology alone is insufficient.

2.2 Theoretical Review

The theoretical review provides the intellectual foundation for explaining how and why digital platforms may contribute to the mitigation of financial fraud. Several theories can be applied to the study, but the Technology Acceptance Model (TAM), Routine Activity Theory (RAT), and Fraud Triangle Theory (FTT) are particularly relevant.

2.2.1 Technology Acceptance Model (TAM)

The Technology Acceptance Model was developed by Davis (1989) to explain why individuals accept or reject information technology. The model proposes that two major factors influence technology acceptance: perceived usefulness and perceived ease of use.

Perceived usefulness refers to the extent to which an individual believes that using a particular technology will improve his or her performance. Perceived ease of use refers to the extent to which the individual believes that using the technology will require little effort.

Applied to digital financial platforms, TAM suggests that customers are more likely to adopt mobile banking, internet banking, fintech applications, and electronic payment platforms when they perceive these platforms as useful and easy to use. The theory is relevant to fraud mitigation because security mechanisms must be accepted and properly used by customers. For example, multi-factor authentication, biometric verification, transaction alerts, and security notifications may improve fraud protection, but their effectiveness can be reduced if users perceive them as inconvenient or difficult to use. Therefore, TAM provides a useful explanation of the user dimension of digital fraud mitigation. A technologically sophisticated platform may not provide adequate protection if customers do not properly use its security features.

Relevance of TAM to the Study

The Technology Acceptance Model is relevant because the study examines digital platforms whose effectiveness depends partly on user adoption and behaviour. It helps explain whether customers' perceptions of the usefulness and ease of use of digital platforms influence their willingness to use security features and comply with fraud-prevention procedures.

However, TAM focuses primarily on technology acceptance and does not adequately explain the motivations behind fraudulent behaviour. Consequently, another theory is necessary to explain why fraud occurs.

2.2.2 Routine Activity Theory (RAT)

Routine Activity Theory was developed by Cohen and Felson (1979). The theory explains crime as occurring when three elements converge in time and space:

1. A motivated offender;
2. A suitable target; and
3. The absence of a capable guardian.

The theory is highly relevant to digital financial fraud. In the digital environment, a motivated offender may be a cybercriminal, dishonest employee, or fraudster. A suitable target may be a customer's bank account, payment card, mobile wallet, or online banking credentials. A capable guardian may include authentication systems, fraud-monitoring software, cybersecurity personnel, regulatory controls, or an informed customer.

Digital platforms can therefore influence the likelihood of fraud by either increasing the suitability of targets or strengthening capable guardianship.

For example, the increasing availability of online banking and mobile payment services provides more opportunities for offenders to target financial accounts. Conversely, biometric authentication, transaction monitoring, artificial intelligence, and real-time alerts increase capable guardianship and can reduce the likelihood of successful fraud.

Relevance of RAT to the Study

Routine Activity Theory is particularly useful because it provides a direct framework for understanding how digital platforms can mitigate financial fraud. Digital technologies can serve as capable guardians by monitoring transactions, verifying identities, detecting anomalies, and preventing unauthorised access.

The theory therefore supports the argument that effective digital security mechanisms can reduce financial fraud by increasing the level of guardianship around digital financial transactions.

2.2.3 Fraud Triangle Theory

Fraud Triangle Theory was developed by Cressey (1953) to explain the conditions under which individuals engage in occupational fraud. The theory identifies three major elements:

- Pressure
- Opportunity
- Rationalisation

Pressure represents a financial or personal motivation that may encourage an individual to commit fraud. Opportunity refers to weaknesses in an organisation's internal controls that allow fraud to occur. Rationalisation represents the justification an individual use to convince himself or herself that the fraudulent act is acceptable. The theory is relevant to the Nigerian financial sector because fraud may involve both external and internal actors. Weak authentication, inadequate access controls, poor segregation of duties, insufficient transaction monitoring, and weak cybersecurity can create opportunities for fraud. Digital platforms can reduce the opportunity component of the Fraud Triangle by strengthening internal controls. For example, biometric verification can make identity impersonation more difficult, while real-time transaction monitoring can reduce the opportunity for fraudulent transactions to remain undetected.

However, digital technology does not eliminate pressure or rationalisation. Therefore, technological controls must be complemented by ethical standards, employee monitoring, organisational governance, customer awareness, and appropriate sanctions.

Relevance of Fraud Triangle Theory to the Study

Fraud Triangle Theory is relevant because it helps explain the causes and opportunities associated with financial fraud. It is particularly useful for examining how digital platforms reduce opportunities through stronger controls, authentication, monitoring, and accountability mechanisms.

2.3 Theoretical Framework for the Study

Based on the foregoing theories, the study can adopt Routine Activity Theory as its principal theoretical framework, supported by the Technology Acceptance Model and Fraud Triangle Theory. Routine Activity Theory is considered the most appropriate primary theory because the central concern of the study is whether digital platforms can function as capable guardians against financial fraud. Digital platforms provide mechanisms such as authentication, transaction monitoring, artificial intelligence, biometric verification, and alerts that can prevent or detect

fraudulent activities. The Technology Acceptance Model complements RAT by explaining the role of users. Even sophisticated security technologies will have limited effectiveness when users do not adopt or properly utilise them.

Fraud Triangle Theory complements the framework by explaining how weaknesses in internal controls create opportunities for fraudulent behaviour. Digital platforms can reduce these opportunities by strengthening organisational controls and monitoring mechanisms.

Table 2.1: Summary of Theoretical Relevance

Theory	Major Proponents	Main Concept	Relevance to the Study
Technology Acceptance Model	Davis (1989)	Perceived usefulness and perceived ease of use influence technology adoption	Explains customers' adoption and use of digital financial platforms and their security features
Routine Activity Theory	Cohen & Felson (1979)	Crime occurs through the convergence of offender, suitable target, and absence of capable guardian	Explains how digital security technologies can act as capable guardians against financial fraud
Fraud Triangle Theory	Cressey (1953)	Fraud arises from pressure, opportunity, and rationalisation	Explains how digital controls can reduce opportunities for fraud

2.4 Empirical Review

Obadeyi, Akande, and Jekayioluwa (2022) empirically examined the effect of electronic banking fraud on the performance of commercial banks in Nigeria. The study used secondary data covering a 14-year period from 2006 to 2019 and employed simple regression analysis. The findings revealed that electronic banking fraud negatively affected the returns of commercial banks. The study further established that internet banking recorded more fraudulent activities than other electronic banking channels. The authors concluded that although electronic banking improves the quality and efficiency of banking services, the associated fraudulent activities constitute a major threat to bank performance. Similarly, Muoghalu, Okonkwo, and Ananwude (2018) investigated the effect of electronic banking-related fraud on the financial performance of deposit money banks in Nigeria. Their study focused on the fraud risks associated with electronic banking platforms and examined their implications for bank performance. The study demonstrated that fraud associated with electronic banking constitutes an important factor that can undermine the financial benefits derived from technological innovation in banking.

Tade (2022) examined the nature of fraud in Nigeria's banking ecosystem between 2015 and 2019 using secondary data from reports on fraud and forgeries. The findings showed that fraud attacks against deposit money banks increased over the period studied, although the monetary loss declined in 2019 compared with 2018. Importantly, technology-mediated transactions, particularly automated teller machines (ATMs) and internet-based transactions, were among the channels most exposed to fraud. This finding demonstrates that the expansion of digital banking has created both opportunities for financial inclusion and vulnerabilities that fraudsters can exploit.

Tade and Adeniyi (2020) investigated electronic fraud and trust governance within Nigeria's emerging cashless ecosystem. Using qualitative methods, the researchers conducted in-depth and

key-informant interviews with 30 participants. Their findings identified internal, external, and collaborative dimensions of electronic fraud. The study further found that experiences of fraud negatively influenced customers' willingness to adopt or migrate to electronic banking platforms. However, banks were found to be adopting security measures such as scam-alert messages and disciplinary measures against compromised staff to improve customer confidence.

The implication of this finding is that the effectiveness of digital platforms in mitigating fraud goes beyond technological controls. Customer awareness, institutional governance, employee accountability, and trust are also important components of an effective fraud-mitigation framework. Thus, digital platforms may reduce financial fraud only when technological mechanisms are supported by appropriate institutional and behavioural controls.

Galadima and Akinyebi (2024) examined electronic banking fraud in Nigeria using data covering six electronic banking channels between 2013 and 2021. The study employed descriptive statistics and one-way analysis of variance (ANOVA) to examine the volume and monetary value of electronic fraud. The results showed an increasing trend in attempted fraud cases and monetary losses over the study period. The web channel recorded the highest number of fraud cases and monetary losses, while mobile banking fraud showed greater volatility than other channels. Internet banking, on the other hand, recorded a higher value of loss per fraud incident. These findings suggest that different digital platforms present different levels and forms of fraud risk, requiring channel-specific fraud-control mechanisms.

More recently, Obadeyi et al. (2026) investigated digital fraud and the financial performance of Nigerian deposit money banks using panel data from 12 banks covering 2010–2023. The researchers employed the Feasible Generalised Least Squares (FGLS) technique to address heteroskedasticity and autocorrelation. The findings revealed that ATM/card-related fraud and e-commerce fraud had statistically significant negative effects on bank financial performance, whereas internet banking and web-based fraud did not have statistically significant effects. The study also identified a substantial increase in digital fraud incidents between 2014 and 2023. The authors recommended technology-driven prevention strategies involving secure authentication, real-time monitoring, consumer protection, and artificial intelligence.

The application of artificial intelligence (AI) and machine learning (ML) has emerged as an important technological approach to financial fraud detection. Osa et al. (2025) investigated the use of machine-learning models to predict fraud and forgery in the Nigerian banking industry. The study examined models including Gradient Boosting and Lasso Regression for predicting the number of fraud cases, amounts involved, and amounts lost. Gradient Boosting performed best for predicting total cases reported and total amount involved, while Lasso Regression performed better for predicting total amount lost. The study concluded that machine-learning models could provide useful predictive information for fraud management, policy formulation, and strategic decision-making in the Nigerian banking sector.

Sanusi, Sanusi, and Briggs (2026) examined the integration of digital forensics and machine learning for fraud detection in Nigerian deposit money banks. The study focused on five major Nigerian banks and examined the contribution of network, cloud, mobile, and Internet-of-Things (IoT) forensic capabilities to fraud-detection effectiveness. The study is significant to the present research because it moves beyond conventional electronic banking controls and considers how advanced digital forensic technologies can strengthen the identification and investigation of fraudulent activities.

Similarly, Soyemi and Olasina (2026) investigated a hybrid machine-learning framework for fraud detection within the Nigerian financial ecosystem. Their study argues that conventional rule-based

fraud-detection systems may produce high false-positive rates and may have limited adaptability to evolving fraud patterns. The researchers therefore examined a hybrid ensemble approach using localized data. The study highlights the importance of developing fraud-detection technologies that reflect the peculiarities of Nigeria's financial and fintech environment rather than relying exclusively on models developed from foreign datasets.

Empirical Gap

The reviewed studies generally establish that digitalisation has transformed the Nigerian financial system while simultaneously increasing exposure to technology-enabled fraud. Existing empirical evidence shows that internet banking, web-based transactions, ATM/card transactions, mobile banking, and e-commerce platforms are susceptible to different forms of fraud. Studies also indicate that technological mechanisms such as artificial intelligence, machine learning, digital forensics, authentication, and transaction monitoring can contribute to fraud detection and prevention. However, several gaps remain. First, many earlier Nigerian studies concentrated on the effect of electronic fraud on bank performance, rather than directly examining the effectiveness of digital platforms as fraud-mitigation mechanisms. Second, much of the empirical literature relies on historical secondary data, leaving limited evidence concerning how users and financial-sector personnel perceive the effectiveness of contemporary digital fraud-control mechanisms. Third, the rapid development of fintech, mobile payments, artificial intelligence, and real-time payment systems means that findings from earlier periods may not adequately capture current fraud patterns. Finally, there is limited integrated evidence examining digital platforms, fraud-detection technologies, institutional controls, customer awareness, and regulatory mechanisms within a single framework. The present study therefore seeks to address this gap by examining the role of digital platforms in mitigating financial fraud in Nigeria, with emphasis on the extent to which digital technologies contribute to fraud prevention and detection, the challenges limiting their effectiveness, and the measures required to strengthen their application.

3. Methods

3.1 Research Design and Sources of Data

The study adopted an ex-post facto research design and relies entirely on secondary time-series data to examine the role of digital platforms in mitigating financial fraud in Nigeria. The use of ex-post facto design is appropriate because the study utilised historical data that already exist and cannot be manipulated by the researchers. Data for the study is obtained from credible secondary sources, particularly publications and databases of the Central Bank of Nigeria (CBN), Nigeria Inter-Bank Settlement System (NIBSS), Nigeria Deposit Insurance Corporation (NDIC), National Bureau of Statistics (NBS), and other relevant official sources. The data covered the selected study period based on availability and consistency of observations.

3.2 Techniques

To evaluate the stationarity of the variables employed, the Augmented Dickey Fuller (ADF) unit root test is used. Because of the dynamic nature of the variables under study, Autoregressive Distributive Lags (ARDL) is engaged estimating the models.

3.3. Model Specification

The model is functionally specified as;

Financial Fraud Reduction = f (Digital Platforms Variables) (1)

Financial Fraud Reduction = f (Digital Platform Adoption, Fraud Detection Capability, Real time Monitoring, User Awareness) (2)

FraudCA = f (DPAI, FDCI, RTMI, UAI) (3)

Explicitly;

$FraudCA = \alpha_0 + \alpha_1 FraudCA_{t-1} + \alpha_2 DPAI + \alpha_3 DPAI_{t-1} + \alpha_4 FDCI + \alpha_5 FDCI_{t-1} + \alpha_6 RTMI + \alpha_7 RTMI_{t-1} + \alpha_8 UAI + \alpha_9 UAI_{t-1} + e_{t-1}$ (4)

$FraudCA = \alpha_0 + \alpha_1 logFraudCA_{t-1} + \alpha_2 logDPAI + \alpha_3 logDPAI_{t-1} + \alpha_4 logFDCI + \alpha_5 logFDCI_{t-1} + \alpha_6 logRTMI + \alpha_7 logRTMI_{t-1} + \alpha_8 logUAI + \alpha_9 logUAI_{t-1} + e_{t-1}$ (5)

Where et_{-1} are stochastic elements

Operational form (Apriori Expectation)

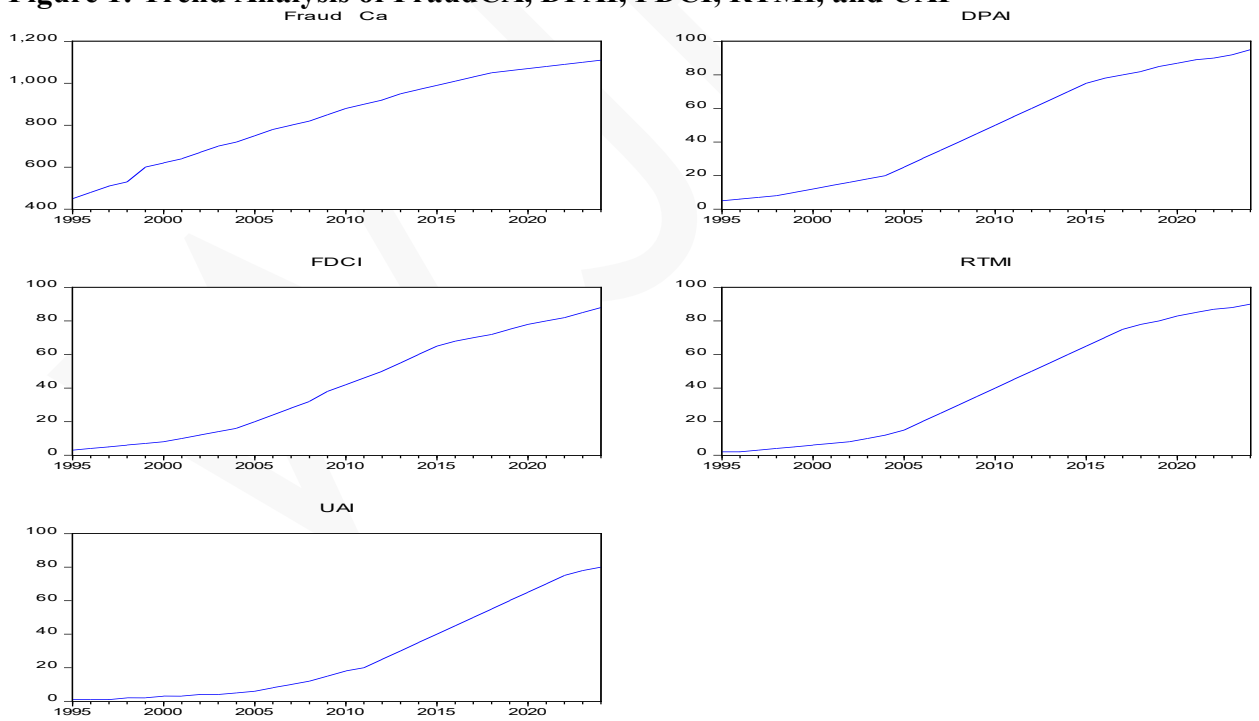
α_1, α_2, α_3, and α_4 are coefficient of DPAI, FDCI, RTMI, and UAI respectively. It is expected that Digital Platforms Variables will either positively or negatively influence Financial Fraud Reduction.

4. Results and Analysis

4.1: Trend Analysis of Data

This estimation of the model specified in this study will commence with trend analysis of data. The time series plot of the data is shown in figure I below. The figures below revealed that all the variables trended smoothly upwards, though not absolutely smooth, suggesting non-stationarity of the variables as expected.

Figure 1: Trend Analysis of FraudCA, DPAI, FDCI, RTMI, and UAI



Authors' computation output using E-view 10.

Next is descriptive statistical analysis;

4.2: Description of Variables

Table 1 below depicts a summary of statistics that describe the distributional features of all the data. The variables recorded standard deviation of the following: 207.05, 32.08, 29.57, 32.42 and 27.25 for FraudCA, DPAI, FDCI, RTMI, and UAI respectively. All variables showed Kurtosis lower than 3 indicating platykurtic distributions. All variables revealed positive stewed distribution, except FraudCA. All variables recorded p-values of JarqueBera insignificant at 5% suggesting normal distribution. For all the variables, the difference between the values of maximum and minimum are wide suggesting fluctuations in the variables as seen in the standard deviation.

Table 1: Descriptive Statistics for FraudCA, DPAI, FDCI, RTMI, and UAI

	FRAUD___CA	DPAI	FDCI	RTMI	UAI
Mean	837.6667	48.13333	41.43333	41.16667	27.43333
Median	865.0000	47.50000	40.00000	37.50000	16.50000
Maximum	1110.000	95.00000	88.00000	90.00000	80.00000
Minimum	450.0000	5.000000	3.000000	2.000000	1.000000
Std. Dev.	207.0596	32.08366	29.57245	32.42826	27.25067
Skewness	-0.346168	0.038910	0.129463	0.190392	0.698974
Kurtosis	1.868095	1.437719	1.491665	1.459465	2.009253
Jarque-Bera	2.200674	3.058473	2.927647	3.147806	3.669798
Probability	0.332759	0.216701	0.231350	0.207235	0.159630
Sum	25130.00	1444.000	1243.000	1235.000	823.0000
Sum Sq. Dev.	1243337.	29851.47	25361.37	30496.17	21535.37
Observations	30	30	30	30	30

Authors' computation output using E-view 10.

The researchers proceeded to testing the stationarity of the variables. This procedure is normal in macroeconomic time series analysis to know the most suitable technique for estimating the model. Here, the researchers employed Augmented Dickey Fuller (ADF) unit root test as depicted below;

4.4: Stationarity/Unit Root Test

Stationarity is statistical proven procedure in macroeconomic time series to ascertain a suitable method for data analysis. Table 4 below depicts the stationary test for both level and first difference data.

Level

Null Hypothesis: Unit root (individual unit root process)				
Series: LNFRAUDCA, LNDPAI, LNFDCI, LN_RTMI, LNUAI				
Method			Statistic	Prob.**
ADF - Fisher Chi-square			67.9748	0.0000
ADF - Choi Z-stat			-6.51666	0.0000
Intermediate ADF test results UNTITLED				
Series	Prob.	Lag	Max Lag	Obs
LNFRAUDCA	0.0000	0	6	29
LNDPAI	0.0945	1	6	28

LNFDCI	0.0018	5	6	24
LN_RTMI	0.0069	6	6	23
LNUAI	0.0001	2	6	27

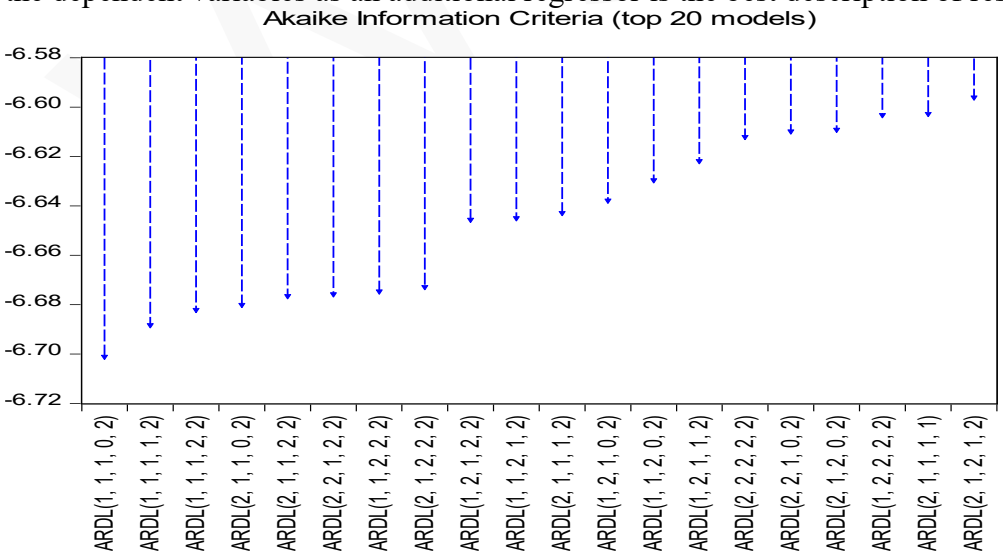
First Difference

Null Hypothesis: Unit root (individual unit root process)				
Series: LNFRAUDCA, LNDPAI, LNFDCI, LN_RTMI, LNUAI				
Method			Statistic	Prob.**
ADF - Fisher Chi-square			24.4059	0.0066
ADF - Choi Z-stat			-0.21835	0.4136
Intermediate ADF test results D(UNTITLED)				
Series	Prob.	Lag	Max Lag	Obs
D(LNFRAUDCA)	0.0001	3	6	25
D(LNDPAI)	0.0156	3	6	28
D(LNFDCI)	0.9667	4	6	24
D(LN_RTMI)	0.0992	0	6	28
D(LNUAI)	0.9956	6	6	22

The results show DPAI is integrated at order one, while others are stationary at level. The variables have different orders of integration, justifying the earlier adopted ARDL model.
The researchers confirmed and validated the adoption Autoregressive Distributive Lag (ARDL) to estimating the model, then proceed to model selection using Akaike Information Criterion (AIC) as shown below in Figure 2 below.

4. 5: Model Selection

Figure 2 below depicts ARDL model selection based on Akaike Information Criterion (AIC). Information criteria select models that minimize their values. From figure 1 below, the best model, according to AIC, is an ARDL (2,1,2,1,2). This implies that a model that includes lagged value of the dependent variables as an additional regressor is the best description of researchers' data.



Authors' computation output using E-view 10.

Figure 2: Model Selection based on AIC

The researchers therefore proceeded to estimating the models with ARDL, aimed at proffering dynamic solution to the static problem of time series. This is shown in table 5 below.

4.6: Model Estimation and Results

Having satisfied with all previous tests, the researchers confidently proceeded to estimating the relationship between Financial Fraud Reduction (FraudCA) and Digital Platforms Variables (FDPAI, FDCI, RTMI, and UAI) in Nigeria with ARDL framework.

Table 5: ARDL Estimation Results

Dependent Variable: LNFRAUDCA				
Method: ARDL				
Variable	Coefficient	Std. Error	t-Statistic	Prob.*
LNFRAUDCA(-1)	0.608510	0.082770	7.351858	0.0000
LNDPAI	0.268113	0.094104	2.849114	0.0107
LNDPAI(-1)	-0.264720	0.076051	-3.480808	0.0027
LNFDCI	-0.124363	0.071356	-1.742846	0.0984
LNFDCI(-1)	0.350895	0.086935	4.036315	0.0008
LN_RTMI	-0.149783	0.063215	-2.369414	0.0292
LNUAI	-0.000901	0.017891	-0.050383	0.9604
LNUAI(-1)	0.071935	0.013109	5.487379	0.0000
LNUAI(-2)	-0.049968	0.017096	-2.922701	0.0091
C	2.310508	0.463500	4.984919	0.0001
R-squared	0.89327	Mean dependent var		6.737019
Adjusted R-squared	0.898991	S.D. dependent var		0.233109
F-statistic	2971.865	Durbin-Watson stat		2.460573
Prob(F-statistic)	0.000000			
*Note: p-values and any subsequent tests do not account for model selection.				

Authors' computation output using E-view 10.

Table 5 above reveals that FraudCA has p-value of 0.0000 suggesting that FraudCA is autoregressive. It is statistically confirmed evidence suggesting that FraudCA in the past can predict future events in the Financial Fraud Reduction in Nigeria. It conspicuously revealed that DPAI, FDCI, RTMI, and UAI have significant relationship with FruadCA at 5% significant level, though with either positively/or negatively impact FraudCA. The adjusted R-square is 0.898 suggesting that the estimated ARDL (2,1,2,1,2) model is moderately fitted, with the explanatory variables jointly accounting for 89.8% of total variation of FraudCA. The probability of F-Statistic is 0.000000, an indication that the estimated model is highly significant. Durbin-Watson Statistics (Dw) is 2.460573 telling the researchers not to border about autocorrelation. The researchers can boldly say that the model did a good job to describe the relationship between macroeconomic variables and stock market in Nigeria. The autonomous component or constant (C) has coefficient of 2.310508 with p-value of 0.0001, which is significant. This shows that Digital Platform Adoption, Fraud Detection Capability, Real time Monitoring, and User Awareness are not the most important among Digital Platforms Variables which affect Financial Fraud Reduction in Nigeria.

4.6.1: Test of long run Relationships between Financial Fraud Reduction and Digital Platforms Variables

Table 6: ARDL Bound Cointegration Test

F-Bounds Test		Null Hypothesis: No levels relationship		
Test Statistic	Value	Signif.	I(0)	I(1)
			Asymptotic: n=1000	
F-statistic	11.51348	10%	2.2	3.09
K	4	5%	2.56	3.49
		2.5%	2.88	3.87
		1%	3.29	4.37

Authors' computation output using E-view 10.

Table 6 above depicts ARDL Bound cointegration Test examining if there is long run relationship in the model. From the bound test, it can be seen that the F-Statistics is 11.51348 which is greater than all the critical values at 1(0) and 1(1) bounds at 1% to 10%. These reject the null hypothesis of no levels of relationship. With this result the researchers have enough evidence to pronounce a long run relationship between Financial Fraud Reduction and Digital Platforms Variables adopted in this study.

4.6.2: Short run and long run impact of Financial Fraud Reduction and Digital Platforms Variables

Table 7: Cointegrating and Long run Form

ARDL Long Run Form and Bounds Test				
Dependent Variable: D(LNFRAUDCA)				
Cointegrating Form				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	2.310508	0.463500	4.984919	0.0001
LNFRAUDCA(-1)*	-0.391490	0.082770	-4.729872	0.0002
LNDPAI(-1)	0.003393	0.081767	0.041497	0.9674
LNFDCI(-1)	0.226532	0.069388	3.264728	0.0043
LN_RTMI**	-0.149783	0.063215	-2.369414	0.0292
LNUAI(-1)	0.021066	0.013599	1.549073	0.1388
D(LNDPAI)	0.268113	0.094104	2.849114	0.0107
D(LNFDCI)	-0.124363	0.071356	-1.742846	0.0984
D(LNUAI)	-0.000901	0.017891	-0.050383	0.9604
D(LNUAI(-1))	0.049968	0.017096	2.922701	0.0091
Long run Form				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
LNDPAI	0.008667	0.208078	0.041653	0.9672
LNFDCI	0.578642	0.200352	2.888132	0.0098
LN_RTMI	-0.382599	0.149205	-2.564241	0.0195
LNUAI	0.053809	0.030623	1.757136	0.0959

C	5.901837	0.195753	30.14938	0.0000
EC = LNFRAUDCA - (0.0087*LNDPAI + 0.5786*LNFDCI - 0.3826*LN_RTMI + 0.0538*LNUAI + 5.9018)				

Authors' computation output using E-view 10.

Table 7 above reveals all digital platform variables affect Financial Fraud Reduction in short run and but Fraud Detection Capability and Real time Monitoring in the long run.

4.6.3: Correction Short Run Error Test

Table 8: ARDL Error Correction Regression

ARDL Error Correction Regression				
Dependent Variable: D(LNFRAUDCA)				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
D(LNDPAI)	0.268113	0.054358	4.932363	0.0001
D(LNFDCI)	-0.124363	0.043780	-2.840611	0.0108
D(LNUAI)	-0.000901	0.009823	-0.091761	0.9279
D(LNUAI(-1))	0.049968	0.010927	4.572789	0.0002
CointEq(-1)*	-0.391490	0.041669	-9.395212	0.0000
R-squared	0.928630	Mean dependent var		0.029940
Adjusted R-squared	0.916218	S.D. dependent var		0.022628
Durbin-Watson stat	2.460573			

Authors' computation output using E-view 10.

As shown in the output in Table 8 above, error correction equation, CointEq(-1) has expected negative sign of -0.391490 and p-value of 0.0000 indicating the model is statistically significant. It can also be seen that 39.1% of errors from the equilibrium can be corrected in the next period, and speed of adjustment is 39.1%.

4.8: Causality Relationship

Table 11: Pairwise Granger Causality Test

Pairwise Granger Causality Tests			
DPAI does not Granger Cause FRAUD___CA	29	0.03069	0.8623
FRAUD___CA does not Granger Cause DPAI		20.4934	0.0001
FDCI does not Granger Cause FRAUD___CA	29	0.10393	0.7497
FRAUD___CA does not Granger Cause FDCI		23.3897	5.E-05
RTMI does not Granger Cause FRAUD___CA	29	0.23091	0.6349
FRAUD___CA does not Granger Cause RTMI		30.2565	9.E-06
UAI does not Granger Cause FRAUD___CA	29	1.06503	0.3116
FRAUD___CA does not Granger Cause UAI		28.7478	1.E-05

Authors' computation output using E-view 10.

From the table 11 above, it reveals that all digital platform variables do not granger cause Financial Fraud reduction, whereas Financial Fraud reduction granger causes all digital platform variables.

That suggests a unidirectional causality between digital platform variables and Financial Fraud reduction.

4.7 Discussion of Findings

The findings of the study indicate that digital platforms play a significant role in mitigating financial fraud in Nigeria. The adoption of mobile banking, internet banking, automated teller machines (ATMs), point-of-sale (POS) terminals, USSD services, and fintech platforms has improved the ability of financial institutions to prevent, detect, and respond to fraudulent activities. Security mechanisms such as biometric authentication, Bank Verification Number (BVN), multi-factor authentication, transaction alerts, and automated transaction monitoring provide additional layers of protection against unauthorised access and suspicious transactions.

The finding that digital platforms enhance fraud prevention is consistent with Tade and Adeniyi (2020), who found that Nigerian financial institutions had introduced several security measures to address electronic fraud within the cashless economy. Similarly, Tade (2022) observed that technology-mediated transactions, including ATM and internet-based transactions, constitute important channels through which fraud occurs in Nigeria. This indicates that while digital platforms create opportunities for fraud, they also provide institutions with mechanisms for controlling and detecting fraudulent activities.

The study further reveals that the use of advanced technologies such as artificial intelligence, machine learning, data analytics, and real-time transaction monitoring improves the detection of suspicious financial activities. This finding agrees with Osa et al. (2025), who established that artificial intelligence and machine-learning models have considerable potential for predicting fraud and forgery in the Nigerian banking industry. It also supports Sanusi et al. (2026), who found that integrating digital forensics and machine learning can strengthen fraud detection among Nigerian deposit money banks. The findings can also be explained by Routine Activity Theory (Cohen & Felson, 1979), which states that crime is more likely to occur when a motivated offender encounters a suitable target in the absence of capable guardianship. In digital banking, fraudsters represent motivated offenders, while customers' accounts and digital payment channels constitute potential targets. Digital authentication, transaction monitoring, fraud alerts, and artificial intelligence therefore serve as forms of capable guardianship that make fraudulent activities more difficult to perpetrate and easier to detect. However, the findings indicate that technological solutions alone cannot completely eliminate financial fraud. Challenges such as phishing, social engineering, identity theft, SIM-swap fraud, insider abuse, inadequate cybersecurity infrastructure, and low customer awareness continue to undermine the effectiveness of digital fraud-control mechanisms. This supports Tade and Adeniyi (2020), who identified internal, external, and collaborative dimensions of electronic fraud in Nigeria. Overall, the findings suggest that digital platforms are important instruments for mitigating financial fraud in Nigeria, but their effectiveness depends on continuous technological upgrading, strong internal controls, customer awareness, effective regulation, and collaboration among banks, fintech companies, telecommunications operators, regulators, and law-enforcement agencies. Thus, digitalisation should be accompanied by appropriate institutional and human controls to achieve sustainable reductions in financial fraud.

5. Conclusion and Recommendation

5.1 Conclusion

The study examined the role of digital platforms in mitigating financial fraud in Nigeria. Based on the findings, it is concluded that digital platforms have become important instruments for preventing, detecting, and responding to financial fraud. The adoption of mobile banking, internet banking, POS terminals, ATMs, USSD services, and fintech applications has enabled financial institutions to introduce stronger authentication, transaction monitoring, real-time alerts, biometric verification, and other security mechanisms. These technologies have improved the capacity of financial institutions to identify suspicious transactions and reduce the opportunities available to fraudsters. However, the study also concludes that digital platforms are not without challenges. The same technologies that improve financial efficiency can create new opportunities for fraud through phishing, social engineering, identity theft, SIM-swap fraud, cyberattacks, and insider abuse. Consequently, the effectiveness of digital platforms in mitigating financial fraud depends on the quality of their implementation, the strength of cybersecurity infrastructure, customer awareness, regulatory enforcement, and cooperation among relevant stakeholders. Digital technology should therefore be regarded as an important component of a broader fraud-management framework rather than as a complete solution to financial fraud in Nigeria.

5.2 Recommendations

Based on the findings and conclusion of the study, the following recommendations are made:

i. Financial institutions should strengthen digital security infrastructure. Banks and fintech companies should continuously upgrade their cybersecurity systems and adopt advanced technologies such as artificial intelligence, machine learning, biometric authentication, and real-time transaction monitoring to identify and prevent fraudulent activities.

ii. Customer awareness should be improved. Financial institutions should regularly educate customers on phishing, social engineering, SIM-swap fraud, fake links, OTP protection, password security, and other emerging forms of digital fraud. Such education should be provided through SMS, mobile applications, social media, and other accessible channels.

iii. Authentication mechanisms should be strengthened. Banks and other financial-service providers should implement robust multi-factor authentication and biometric verification while ensuring that security procedures remain convenient and accessible to legitimate customers.

iv. Regulatory agencies should strengthen monitoring and enforcement. The Central Bank of Nigeria and other relevant agencies should regularly review digital-payment security requirements and ensure that financial institutions comply with established fraud-prevention and cybersecurity standards.

v. Stakeholder collaboration should be enhanced. Banks, fintech companies, telecommunications operators, regulatory bodies, and law-enforcement agencies should improve information sharing and develop coordinated mechanisms for identifying, freezing, investigating, and recovering funds associated with fraudulent transactions.

vi. Financial institutions should strengthen internal controls. Regular employee screening, segregation of duties, access controls, internal audits, and continuous staff training should be implemented to minimise insider-related fraud and reduce weaknesses within digital financial systems.

In conclusion, effective mitigation of financial fraud in Nigeria requires a combination of advanced digital technologies, strong institutional controls, informed customers, effective regulation, and continuous collaboration among stakeholders.

References

Aladejubelo, O. S. (2026). Cyber fraud and digital payment systems in Nigeria: Causes and control measures. *British Journal of Interdisciplinary Research, 3*(12), 243–272. https://doi.org/10.31039/bjir.v3i12.144

Bello, H. (2022). Digitalisation and financial system stability: What role for macroprudential policies? *CBN Economic and Financial Review, 60*(4), 61–77.

Central Bank of Nigeria. (2022). *Payments system management*. Central Bank of Nigeria.

Central Bank of Nigeria. (2025). *Draft guidelines for handling authorised push payment fraud*. Central Bank of Nigeria.

Central Bank of Nigeria. (2025). *Payments system supervision*. Central Bank of Nigeria.

Central Bank of Nigeria. (2025). *The Nigeria Electronic Fraud Forum (NeFF)*.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Galadima, W. M., & Akinyebi, O. (2024). *Electronic banking fraud: The Nigerian experience*. https://doi.org/10.6084/m9.figshare.26117167

Garbaa, K. H., Lazarus, S., & Button, M. (2026). An assessment of convicted cryptocurrency fraudsters. *Current Issues in Criminal Justice, 38*(1), 164–180. https://doi.org/10.1080/10345329.2024.2403294.

Muoghalu, A. I., Okonkwo, J. J., & Ananwude, A. (2018). Effect of electronic banking related fraud on deposit money banks financial performance in Nigeria. *Discovery, 54*(276), 496–503.

Nkechika, C. G. (2022). Digital financial services and financial inclusion in Nigeria: Milestones and new directions. *CBN Economic and Financial Review, 60*(4), 151–170. https://doi.org/10.33429/1957-2968.2089.

Obadeyi, J. A., Akande, A. A., & Jekayioluwa, Y. S. (2022). Electronic banking fraud and commercial banks' performance: An empirical prove of Nigeria. *International Journal of Innovative Research in Accounting and Sustainability, 7*(4), 88–99.

Obadeyi, J. A., Odewole, P. O., Akande, A. A., & Jekayinoluwa, A. S. (2026). An empirical investigation of digital frauds and financial performance of Nigerian deposit money banks. *EKSU International Journal of Management and Development Studies, 2*(1).

Osa, E., Orukpe, P. E., Igori, S., & Ekoko, E. C. (2025). Artificial intelligence intervention for predicting fraud and forgeries in the Nigerian banking industry. In V. Odumuyiwa & O. Sennaike (Eds.), *Proceedings of the 5th International Conference on Artificial Intelligence and Robotics* (pp. 45–56). Machine Intelligence Research Group, University of Lagos.

Sanusi, R. A., Sanusi, I., & Briggs, D. O. B. (2026). Integrating digital forensics and machine learning for fraud detection in Nigerian deposit money banks: A PLS-SEM and artificial neural network approach. *FUDMA Journal of Accounting and Finance Research, 4*(1), 53–69. https://doi.org/10.33003/fujafr-2026.v4i1.286.53-69

Tade, O. (2022). Nature of frauds in Nigeria's banking ecosystem, 2015–2019. *Journal of Financial Crime, 29*(4), 1241–1248. https://doi.org/10.1108/JFC-08-2021-0185

Tade, O., & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology, 64*(16), 1641–1660. https://doi.org/10.1177/0306624X20928028

WJFIR