International Journal of Functional Research in Arts & Humanities
Volume 4; Issue 4; December 2025; Page No. 38-60.

CYBERSECURITY AND FRAUD PREVENTION IN THE NIGERIAN BANKING SECTOR

[1] Onyeka A. Obi & [2]Juliet Obiakor

[1] Federal Polytechnic Oko, Anambra State, Nigeria

Abstract

This study examines the effectiveness of cybersecurity strategies in mitigating financial fraud within Nigerian commercial banks. Against the backdrop of increased digital banking adoption and rising cyber threats, the research explores how institutional frameworks, authentication systems, and customer awareness programs contribute to fraud prevention efforts. Adopting a cross-sectional survey design, primary data was collected randomly from 169 respondents with structured online questionnaires via WhatsApp groups and other social media platforms. The Binary Logistic Regression (BLR) and the Hosmer and Lemeshow Test were utilized to evaluate predictive relationships between variables. Findings reveal that the perceived effectiveness of bank-led cybersecurity frameworks significantly reduces the likelihood of fraud victimization. However, biometric and multi-factor authentication systems, as well as participation in cybersecurity awareness programs, did not demonstrate statistically significant impacts, suggesting that deployment alone is insufficient without active user engagement. The study buttresses the need for integrated, user-centred, and innovative technology-driven cybersecurity approaches in Nigeria's banking sector.

Keywords: Cybersecurity, Financial Fraud, Biometric Verification, Multi-factor Authentication, Cybersecurity Awareness.

1. INTRODUCTION

In recent years, Nigeria's banking sector has undergone a profound transformation, driven by technological advancements that have enhanced financial accessibility, efficiency, and connectivity. The rise of online banking and digital payment platforms has revolutionized financial transactions, enabling seamless interactions beyond physical branches. While these innovations have improved convenience for users, they have also introduced new cybersecurity risks, making financial fraud a growing concern (Oyewole, Okoye, Ofodile & Ugochukwu, 2024).

The implementation and increasing reliance on digital banking have exposed Nigerian banks to an escalating wave of cyber threats. Bruce, Lusthaus, Kashyap, Phair and Varese (2024), in a first ever World Cybercrime Index (WCI), has ranked Nigeria 5th following Russia, Ukraine, China and the U.S in the leading countries where cyberfraud is most prevalent. Fraudulent activities, ranging from phishing schemes and malware attacks to identity theft and social engineering tactics has been on the rise as reports have shown that various security frameworks instituted by the Government and CBN to tackle banks' vulnerability to cyber threats in Nigeria, hasn't been entirely successful (Khattri & Singh, 2018; Ama, Onwubiko & Nwankwo, 2024).

Odunewu (2025) upheld that the Nigerian Inter-Bank Settlement System (NIBSS) reported a troubling rise in financial fraud cases, with annual losses escalating from ₦2.9 billion in 2019 to ₦52.26 billion in 2024, reflecting a 196% increase over five years. These frauds and other related criminalities, perpetrated by outsiders and staff of banks, were driven by electronic payment channels through the internet and advanced technology.

Given these concerns, this study seeks to assess the effectiveness of cybersecurity measures in preventing financial fraud in Nigerian commercial banks. By evaluating cyberfraud prevention frameworks, authentication systems, and level of customer security awareness and internal institutional strategies, the study aims to provide insights into strengthening Nigeria's banking cybersecurity landscape.

1.1. Statement of the Problem

The rapid evolution of Nigeria's banking sector, fuelled by advancements in digital technology, has reshaped financial transactions, enabling seamless online banking and mobile payment solutions. However, despite regulatory and technological interventions, cybercriminals continue to exploit vulnerabilities in digital financial platforms through fraudulent techniques like phishing, identity theft, malware attacks, and social engineering scams. This worrisome development gives credence to the urgent need for enhanced fraud prevention strategies supported by advanced cybersecurity frameworks.

One of the primary concerns in mitigating financial fraud is the inadequacy of traditional authentication mechanisms, such as passwords and PINs, which are increasingly vulnerable to phishing, brute force attacks, and credential theft. The rise in cyber threats necessitates the adoption of more secure verification methods. Innovative approaches, including multi-factor authentication (MFA), biometric verification, and adaptive authentication, offer promising solutions by enhancing security beyond conventional methods. However, many financial institutions in Nigeria struggle with implementing these technologies in a way that balances security with user convenience.

Moreover, insider fraud, weak internal controls, and the evolving sophistication of cybercriminal tactics further exacerbate the challenge. While frameworks established by the CBN and National authorities aim to mitigate risks, the effectiveness of these security measures remains uncertain, particularly in semi-urban banking environments.

There is a dearth in related studies and, to the best of our knowledge, they often rely on statistical methods that offer surface-level insights but do not effectively predict fraud or account for multiple influencing factors (ANOVA, least squares, and chi-square tests). To bridge this gap, this study adopts binary logistic regression, a more dynamic and predictive analytical method, to assess how cybersecurity measures impact fraud prevention. In doing so, it aims to enrich existing knowledge and provide actionable insights for safeguarding Nigeria's financial systems.

1.2. Objectives of the Study

This research aims to evaluate the effectiveness of advanced cybersecurity strategies in preventing financial fraud while addressing challenges related to usability. Specific objectives include:

1. To evaluate the effectiveness of cybersecurity frameworks in preventing financial fraud within Nigerian commercial banks.

2. To examine the role of authentication systems in mitigating unauthorized access and cyber fraud in Nigerian financial institutions.
3. To evaluate the impact of customer awareness programs and internal institutional strategies on the prevention of digital financial fraud in Nigerian commercial banks.

1.3. Research Hypotheses

Based on the research objectives, the following hypotheses were formulated;

H_{o1}: Cybersecurity frameworks have no significant effect on mitigating financial fraud in Nigerian commercial banks.

H_{o2}: Authentication mechanisms do not significantly reduce cyberfraud in Nigeria's banking sector.

H_{o3}: Customer awareness and institutional strategies do not have a significant impact on fraud prevention in Nigerian commercial banks.

1.4. Scope of Study

This study focuses on evaluating the effectiveness of cybersecurity and fraud prevention within Nigerian commercial banks. The research gathers data through online Google Forms distributed via WhatsApp groups and other social media platforms. By capturing varied perspectives, the study aims to assess the extent to which awareness, authentication mechanisms, and institutional strategies influence fraud prevention efforts in the cybersecurity landscape in Nigeria's banking system.

2. LITERATURE REVIEW

2.1. Conceptual Review

2.1.1. Fraud and Cybersecurity

Fraud refers to the intentional deception or misrepresentation by an individual or organization for the purpose of gaining an unfair or illegal advantage, typically involving financial or personal benefit. It becomes cyberfraud when it involves the use of computer, networks and other technological devices. Cyberfraud, in the banking sector, is any illegal activity conducted over digital channels (online, mobile or networked systems) to deceitfully access or steal money, data or credentials from a bank or its customers. These vices exploit vulnerabilities within digital banking systems for financial gain.

On the premise of the increasing prevalence and sophistication of such threats, cybersecurity has become an essential line of defence. It involves both technological and procedural measures designed to protect digital systems from cyber-attacks, unauthorized access, and financial fraud. This has become very crucial for safeguarding customer data, preventing financial fraud, and ensuring regulatory compliance, especially as financial institutions increasingly rely on digital platforms. Cybersecurity, therefore, involves securing the entire digital infrastructure of a bank (online banking systems, internal databases, etc) against unauthorized access, data leaks, and malicious attacks (Luna, 2024).

2.1.2. Review of Fraud in the Nigerian Banking Industry

Financial fraud has been the bane of financial institutions globally and has adversely affected their productivity and reputation. In Nigeria, the banking sector has continued to witness a surge in financial losses over the years due to fraud. As digital banking becomes more prevalent, fraudsters continue to exploit vulnerabilities, leading to substantial financial losses.

The Nigeria Deposit Insurance Corporation (NDIC) (2018) reported that cyberfraud incidences in Nigerian banks surged from 26,182 in 2017 to 37,817 in 2018, representing a 44.4% increase. Likewise, financial losses from these incidents grew substantially in 2018, reaching ₦15.15 billion ($39.9 million), compared to ₦2.37 billion ($6.2 million) in 2017 and ₦2.4 billion ($6.3 million) in 2016. From 2019 to 2023, fraud incidence in Nigerian banks skyrocketed by 112%, rising from 44,947 cases in 2019 to 95,620 cases in 2023 (NIBSS, 2024). This sharp increase highlights the growing sophistication of financial fraud tactics, ranging from cybercrime to insider-related fraud. Fraud in the sector showed a 7.52% decrease in Q1 2024, with 11,472 reported cases, compared to 12,405 cases in Q4 2023. Financially, the total amount involved in fraud cases dropped by 56.73%, reducing from ₦6.91 billion in Q4 2023 to ₦2.99 billion in Q1 2024. More notably, the actual losses due to fraud declined by 77.62%, falling from ₦2.09 billion in Q4 2023 to ₦468.42 million in Q1 2024 (FITC, 2024a). Fraud-related losses in Nigerian banks skyrocketed by 8,993% in Q2 2024, totalling ₦42.6 billion, compared to ₦468.4 million in Q1 2024. This marks a 637% increase from Q2 2023, where banks lost ₦5.7 billion to fraud (FITC, 2024b). Additionally, the total amount involved in fraudulent transactions grew by 1,784%, from ₦2.9 billion in Q1 2024 to approximately ₦56.3 billion in Q2 2024 (FITC, 2024b).

Fraudsters continually target banking channels with the highest return on investment (ROI), making some payment methods more vulnerable than others. In 2023, Mobile fraud ranked highest, with a Fraud Interest Index (FII) of 34%, followed closely by Internet Banking (33.99%) and POS fraud (26.37%). The pattern persisted into Q1 2024, with Mobile fraud continuing to dominate, accounting for ₦768.84 million (25.73%) of fraudulent transactions. Computer/Web fraud followed closely at ₦680.75 million (22.78%), while POS fraud contributed ₦565.69 million (18.93%) (FITC, 2024a). However, Q2 2024 saw a drastic shift in fraud trends, with 'Miscellaneous and Other Fraud' surging to account for 96.46% of total fraud losses, reaching an unprecedented ₦41.14 billion. Fraudulent withdrawals and Computer/Web fraud ranked next, totalling ₦781.2 million and ₦400.7 million, respectively. Mobile fraud (which had previously dominated fraud trends), recorded a 59% decline in total losses, dropping from ₦216.4 million in Q1 2024 to ₦88.7 million in Q2 2024 (FITC, 2024b). These figures underscore the urgent need for enhanced security measures in these digital platforms, as fraudsters actively seek to circumvent banking controls where exploitation is most profitable.

2.1.3. Dimensions of Fraud in Banking

Fraud in Nigeria's banking industry can stem from both external (outsider) threats and internal (insider) misconduct. These two categories differ in their execution methods, risks, and the level of institutional damage they cause (FITC, 2024a). *Outsider fraud* is perpetrated by external actors who have no direct affiliation with the bank but exploit vulnerabilities in banking infrastructure, customers, or employees. It remains the most prevalent form of financial crime. Common methods include cyber fraud (phishing schemes, malware, and ransomware attacks), social engineering scams (manipulating bank customers/employees into divulging sensitive information), identity theft (conducting unauthorized transactions through stolen credentials), ATM card and payment fraud (exploiting weak security protocols in online banking, POS transactions, and ATMs), etc.

In contrast, *insider fraud* occurs when bank employees use their positions to manipulate systems for personal gain. It is often more damaging because it involves individuals with direct access to sensitive financial systems, which can ultimately erode customer trust, cause long-term reputational harm, lead to high financial losses, etc. Common methods include unauthorized account access (exploiting privileged access to make fraudulent transactions), manipulated settlements (tampering with financial records, altering balances or diverting funds), collusion with external fraudsters (collaborating with criminal networks to bypass security systems), loan and credit fraud (approve fraudulent loans or falsify documentation to siphon funds), etc.

2.1.4. The Overview of Cybersecurity Framework in the Nigerian Financial Sector

Cybersecurity in Nigerian banks has become increasingly critical due to the sustained prevalence of cyber threats and fraudulent activities such as phishing, identity theft, and hacking. Banks have become prime targets for cybercriminals, making it essential to deploy robust defence measures to prevent attacks, malware infections, data breaches, and unauthorized access to systems and information. By implementing advanced security technologies, continuously monitoring for system vulnerabilities, and educating both employees and customers, financial institutions can stay ahead of cybercriminals and preserve the integrity of their operations (Backbase, 2024). Commonly deployed techniques in the Nigerian financial sector include traditional authentication (PINs and passwords), multi-factor authentication, biometric verification, real-time fraud detection systems, and transaction monitoring.

The CBN has continued to play a crucial role in strengthening cybersecurity across the financial sector. In an effort to ensure the confidentiality, integrity, and operational resilience of financial institutions, the CBN has issued several sector-specific regulatory instruments, including the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs), the Risk-Based Cybersecurity Framework for Other Financial Institutions (OFIs), the Regulatory Framework for Mobile Money Services in Nigeria, and the Nigerian Payment System Risk and Information Security Management Framework (Kolade, 2022; Mukoro, 2024;

Nkwor & Adeyemo, 2024). The CBN monitors, enforces compliance and promotes awareness of these guidelines.

In addition to CBN-led measures, broader national frameworks such as the Cybercrimes (Prohibition, Prevention, etc) Act, 2015 and the National Cybersecurity Policy and Strategy (NCPS), 2021, complement institutional regulation by providing a legal and strategic foundation for combating cybercrime, protecting critical national infrastructure, and enhancing inter-agency coordination across Nigeria's cybersecurity system. These frameworks not only cover financial institutions, they consider them a strategic priority (Advocacy for Policy Innovation, 2021).

2.1.4.1. Risk-Based Cybersecurity Framework and Guidelines for DMBs and PSBs

The first Risk-Based Cybersecurity Framework and Guidelines was issued by the CBN in 2018. It applied to all deposit money banks and payment service providers which laid a foundation for cybersecurity governance. However, it was less comprehensive as it didn't address emerging technologies such as artificial intelligence, open banking, and distributed ledger technology. Again, provisions requiring board-level expertise in information and cybersecurity was vague. Furthermore, its guidance on third-party risk management and cyber threat intelligence was limited in scope and detail. To address this gap, the CBN came up with a revised Risk-Based Cybersecurity Framework and Guidelines in 2024 which applied to all deposit money banks and payment service banks. It sets out the minimum cybersecurity requirements that DMBs and PSBs must implement to strengthen their resilience against cyber threats. It requires at least two non-executive directors (one independent) possess expertise in ICT and cybersecurity; institutions to implement a robust cybersecurity risk management system with regular assessments and controls; annual self-assessments by DMBs and PSBs using the CBN Cybersecurity Self-Assessment Tool (CSAT); the establishment of documented incident response procedures; and addresses the cybersecurity implications of emerging technologies, including artificial intelligence, cloud computing, open banking, and distributed ledger (CBN, 2024; Nkwor & Adeyemo, 2024; Digital Policy Alert, 2024).

2.1.4.2. Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions (OFIs)

In the bid to reinforce resilience in digital defence across a wider range of financial institutions beyond DMBs and PSBs, the CBN issued the Risk-Based Cybersecurity Framework and Guidelines for other Financial Institutions in 2022. This framework targets all OFIs as defined under the Bank and Other Financial Institutions Act (BOFIA) 2020, which would include discount houses, bureau de change, finance companies, financial holding companies, international money transfer services, money brokerage firms, etc. The key provisions of the framework requires that cybersecurity be a standing agenda item at board and senior management meetings where the quarterly cybersecurity reports should be mandatorily submitted (Cybersecurity Governance); each Other

Financial Institution (OFI) should develop and submit a cybersecurity framework to the Director of OFI Supervision at the CBN (Framework Submission); mechanisms for detecting, preventing, and responding to cyber threats should be established by the institutions while ensuring ongoing compliance monitoring with regulatory obligations (Risk Management and Compliance Monitoring) (CBN, 2022; Timi-Koleolu, 2022).

2.1.4.3. Regulatory Framework for Mobile Money Services in Nigeria

The CBN issued the first Regulatory Framework for Mobile Payments Services in Nigeria in 2009. It focused on enabling person-to-person payments and promoting financial inclusion through mobile channels which made it a launchpad for mobile money operations in the country. In 2015, a revised version was issued by the CBN, which introduced more structure around permissible activities, operational models, and risk management (Sowunmi & Nkposong, 2021).

2021 saw, yet, another update which defined clearly, the distinctive roles of the participants, distinguishing between regulators, mobile money operators (MMOs), infrastructure providers, agents, and consumers. The telco-led model, which is one of the features of the previous versions was completely replaced with the bank-led (where a bank or group of banks lead the service) and non-bank-led (where licenced corporations, excluding telecoms, lead the service) models. More emphasis was made on know your customer (KYC), customer due diligence (CDD), and anti-money laundering (AML) requirements, tightening these processes. Enhanced consumer protection provisions and savings wallet services were introduced, allowing MMOs to offer interest-bearing wallets for investment in government securities, under strict regulatory conditions. Additionally, it set transaction and balance limits for mobile wallets and clarified the resolution process for failed MMOs and settlement banks, ensuring better protection of subscriber funds (CBN, 2021; Sowunmi & Nkposong, 2021).

2.1.4.4. The Nigerian Payment System Risk and Information Security Management Framework.

Issued by the CBN in 2020, this Framework aims to enhance the safety and stability of Nigeria's payment ecosystem by proactively identifying and addressing systemic risks. To ensure effective oversight and decision-making, it seeks to establish sound governance structures. The framework articulates detailed rules and procedures for managing a wide variety of risks (operational, credit, liquidity, and information security) and integrates risk management into the core functions of Scheme Boards and Working Groups, in alignment with the objectives of the Payment System Vision of CBN (2020a). The framework applies to domestic and international payment systems, and payment service providers excluding physical cash movement, securities settlement systems, or bilateral arrangements like correspondent banking (CBN, 2020b; Olaniwun Ajayi Newsletter, 2020).

2.1.4.5. Cybercrimes (Prohibition, Prevention, etc) Act, 2015

The *Cybercrimes (Prohibition, Prevention, etc) Act, 2015* is Nigeria's first comprehensive legislative response to cyber threats, enacted by the National Assembly to criminalize a wide range of cyber offenses and establish safeguards for critical digital infrastructure. Its provisions cover activities such as identity theft, cyberstalking, cybersquatting, and system interference, with penalties applicable to both individuals and corporate bodies.

The Act places specific obligations on financial institutions. Section 37 mandates banks and OFIs to verify the identities of customers before issuing ATM, debit, or credit cards. Section 38 requires them to retain subscriber and transaction data for a minimum of two years and to cooperate with law enforcement agencies when requested. Institutions are also expected to report suspicious activities promptly and implement cyber risk controls as part of their compliance responsibilities. The Act complements regulatory frameworks issued by the CBN by embedding these obligations into enforceable law, reinforcing the role of financial institutions as essential actors in the national cybersecurity framework (Nigerian Financial Intelligence Unit, 2015).

2.1.4.6. National Cybersecurity Policy and Strategy (NCPS), 2021

Launched by the Office of the National Security Adviser (ONSA), the NCPS*, 2021* serves as Nigeria's strategic master plan for managing cyber threats and protecting critical national information infrastructure (CNII). It outlines national objectives for cybersecurity governance, risk mitigation, public-private collaboration, legal harmonization, and capacity building.

The policy explicitly recognizes the financial sector as part of CNII, thereby placing financial institutions among its highest-priority stakeholders. It calls for sector-specific implementation of cybersecurity standards, aligned with existing regulatory efforts like those of the CBN. Financial institutions are encouraged to participate in sectoral Computer Security Incident Response Teams (CSIRTs), share threat intelligence, report incidents, and collaborate with national stakeholders. The NCPS provides the overarching strategic vision that aligns with the operational details of CBN-led frameworks, ensuring that Nigeria's cybersecurity posture is both nationally cohesive and sectorally responsive (Federal Republic of Nigeria, 2021).

2.1.5. Challenges in Cybersecurity Measures in the Nigerian Financial Sector

Abiodun (2023) and Doghudje (2025) outlined various challenges bedevilling the cybersecurity landscape in Nigeria's financial sector. Surprisingly, these challenges were corroborated by the respondents of this study. The rapid adoption of digital banking and financial technology intensified many of these challenges. Key cybersecurity challenges in the Nigerian financial sector would include;

- Surge in cyberattacks causing significant financial losses
- Outdated infrastructure and weak cyber defences in smaller institutions
- Human error, insider threats, and social engineering attacks

- Inadequate compliance with existing regulatory frameworks
- New risks emerging from rapid FinTech adoption
- Low cybersecurity awareness among consumers
- Unverified or outdated KYC
- Inadequate database management
- Conflict of interest between banks' operation staff and marketing staff (account officers)

2.2. Theoretical Framework

Several theories help explain cybersecurity measures and fraud prevention strategies. However, this study will hinge on the Technology Acceptance Model (TAM) and the Routine Activity Theory (RAT).

2.2.1. Technology Acceptance Model (TAM)

This theory was developed by Davis (1989) and it proposes that two key factors determine or explain how users or customers decide to engage a new technology. These factors influence user's attitude toward the technology, drive the user's intention to adopt a system, which in turn determines actual usage;

- Perceived Usefulness (PU): The degree to which a person believes that using a particular system would enhance their job performance.
- Perceived Ease of Use (PEOU): The degree to which a person believes that using a particular system would be free of effort (easy or seamless).

External factors like social influence, age, gender or organizational support, determine a person's PU and PEOU, and thus indirectly affect adoption. However, Venkatesh and Davis (2000) and Venkatesh and Bala (2008) extended the theory to TAM2 and TAM3 respectively to integrate other external factors like cognitive instrumental processes, trust and perceived risk in order to address its original limitations.

In the context of cybersecurity and fraud prevention in banking, this theory (TAM) examines how customers adopt cybersecurity measures based on perceived usefulness and ease of use, influencing the adoption of secure banking practices. Simply put, the core basis of this theory reflects accurately why people do or don't embrace security tools. To buttress further, perceived usefulness would capture customers'/users' belief that using cybersecurity measures will significantly reduce their risk of breach or fraud, boost performance (accelerate transaction approvals, etc), and help with seamless compliance with regulatory and audit requirements. Perceived ease of use, on the other hand, would capture simplicity in learning and of use of these cybersecurity measures, which in turn bolsters users' confidence. Again, awareness of threats and severity of potential fraud, social influence (peer usage, IT support recommendations, etc), trust issues (vendor's reputation, transparency in data handling, etc), job relevance, etc, are external drivers that can also influence adoption of cybersecurity measures.

2.2.2. Routine Activity Theory (RAT)

The RAT, introduced by Cohen and Felson (1979), explains crime as a function of everyday routines and interactions between individuals and their environments, rather than as a result of individual motivation or societal breakdown. This implies that changes in daily activities can either increase or reduce the likelihood of criminal opportunities. The theory asserts that for a crime to occur, three elements must converge in time and space; a motivated offender, a suitable target, and the absence of capable guardianship. According to Lersch and Hart (2023), RAT is based on the core assumption of a rational offender who carefully weighs the potential costs and benefits of their actions.

In the context of cybersecurity and fraud prevention in financial institutions, this theory suggests that fraud occurs when motivated cybercriminals (hacker or insider) identify suitable targets (vulnerable banking systems, unsecured account or data, etc) when there is lack of capable guardianship (deficient security defences, lack of real-time monitoring, inadequate alert systems, etc). Banks can disrupt this chain by reducing offender motivation through legal deterrents (publicizing prosecutions and improving threat intelligence sharing), protecting targets by implementing strong countermeasures (data encryption, authentication methods, system updates, etc) and strengthening guardianship (continuous real-time monitoring, staff training, etc). By disrupting any one of these three elements, banks make it far more difficult for cybercriminals to succeed.

2.3. Empirical Review

Odukwu, Eke and Chukwumati (2022) examines the role of cybersecurity in mitigating fraud within Nigerian commercial banks. Relying on primary data obtained through interviews with senior banking personnel, the findings reveal that both cloud and application security significantly enhance fraud prevention efforts. The research highlights the necessity for Nigerian financial institutions to develop capabilities for detecting and preventing fraudulent transactions. Additionally, it advocates for public awareness campaigns focused on strong password usage as a frontline defence against cyber threats and financial losses.

Fatoki (2023) examined the influence of cybersecurity on financial fraud using survey data from 557 employees across six Nigerian banks. The analysis revealed that phishing, malware, hacking, and insider fraud were the most prevalent cyber threats. Key causes included weak managerial oversight, poor encryption, and collusion. Major challenges to combating cybercrime were lack of infrastructure, national standards, and customer awareness. The research identified multi-factor authentication, biometrics, antivirus tools, and routine security audits as effective mitigation strategies. It concluded that improved cybersecurity governance and consistent monitoring are essential for reducing fraud risk in Nigerian financial institutions.

Ama, Onwubiko and Nwankwo (2024) investigates cybersecurity challenges in Nigerian DMBs with a focus on proactive measures taken by banks and customers to overcome these challenges. The

research design employs a descriptive approach and census sampling, with data collected from staff of selected DMBs using questionnaires. Data analysis was conducted using SPSS, and findings indicate that the major challenges confronting cybersecurity in banks were pharming, identity theft, SIM Swap fraud, Skimming/Website cloning and Smishing/Vishing. The major factors responsible were found to include loopholes in the banks' internal control system, insider abuse by bank staff, ignorance and lack of security consciousness among the banking customers, etc. It was found that banks implement measures such as encryption, password changes, and blocking unsolicited messages to mitigate cybersecurity risks. The study concludes with recommendations for continuous security updates, internal control reviews, and customer education campaigns.

Mustapha and Sinha (2024) investigates the growing threat of cyberfraud in Nigeria's banking sector, with a particular focus on attacks targeting bank customers. Leveraging secondary data, the study identifies a range of fraud techniques; phishing, identity theft, credential theft, ATM card swapping, skimming, and social engineering being the most prevalent tactic. The research emphasizes the importance of proactive cybersecurity strategies, such as multi-factor authentication, advanced technologies, employee training, and regulatory collaboration, to strengthen the sector's resilience and reduce customer vulnerability.

A qualitative study by Ayodeji (2024) investigates the impact of digital banking on rising fraud rates in Nigeria's financial sector, emphasizing its threat to financial inclusion and economic trust. Grounded in the unified theory of acceptance and use of technology 2 (UTAUT 2) model, the research draws on insights from 15 IT leaders through semi-structured interviews. Thematic analysis revealed key areas: categories of fraud, the intersection of technology and human vulnerabilities in fraud facilitation, and the application of big data analytics to detect and prevent fraud. Recommendations include strategic investments in analytics, governance, and staff training.

Folami, Yinusa and Toriola (2024) explores the relationship between digital payment fraud and bank fragility within Nigeria's DMBs. Using the Panel Fully Modified Least Squares (FMOLS) method and data from 14 banks spanning 2014–2023, the research finds that digital payment fraud significantly increases financial vulnerability, impacting profitability. However, larger bank size appears to mitigate this fragility. The study underscores the importance of robust cybersecurity frameworks and advanced fraud detection mechanisms to counteract fraud risks.

Adeyemo and Obafemi (2024) examines how technological innovation enhances fraud prevention in Nigeria's Deposit Money Banks (DMBs). Survey results and empirical data show strong support for advanced tools like data analytics, machine learning, blockchain, real-time monitoring, and AI. Notably, 86% of respondents confirmed their effectiveness in fraud detection and prevention. Statistical analysis, including chi-square tests, revealed a significant link between tech adoption and strengthened security. The research also highlights the importance of continuous staff training, fintech collaboration, and regular security audits, concluding that innovation is essential for building a secure, efficient, and resilient banking system.

A quantitative study by Metibemu (2025) analyses fraud and cybersecurity threats in digital-only banking using large-scale secondary data from global financial and cybersecurity reports. Employing descriptive statistics, logistic regression, and Difference-in-Differences (DiD) analysis, the research identifies phishing and ransomware as the most financially damaging attack types. The findings highlight that Basel III compliance significantly reduces fraud risk, while AI-driven fraud monitoring shows current limitations. Additionally, regulatory enforcement yields better fraud mitigation outcomes. The study recommends strengthening digital banking resilience through improved AI tools, robust compliance measures, layered security architectures, and public awareness programs.

Aburaya and Barnat (2023) examines the legal framework established by Saudi Arabia to safeguard digital banking customers from cyber threats such as fraud and identity theft. It analyses key regulatory provisions aimed at protecting personal data and securing financial transactions, while highlighting the responsibilities of financial institutions in enforcing these measures. The research also explores collaborative initiatives between banks and regulatory bodies to ensure a secure banking environment. By assessing the effectiveness of existing laws, the study offers insights into potential improvements in customer protection and cybersecurity governance within the Kingdom.

Nguyen, Pham, Nguyen, Pham, Nguyen and Vu (2024) investigates the prevailing cybersecurity risks within Vietnam's financial and banking sector by identifying and analysing 15 major cybersecurity threats. The study employed an advanced Multi-Criteria Decision Making (MCDM) framework which incorporated the DELPHI technique, Decision-Making Trial and Evaluation Laboratory (DEMATEL), and Combined Compromise Solution (COCOSO) methods, which was enhanced with Neutrosophic Sets and Z-numbers. Notably, malware infections and supply chain vulnerabilities emerged as the most critical. Findings emphasize the need for comprehensive, proactive cybersecurity strategies to ensure system integrity and resilience.

Wani and Bhosale (2024) reviews cybersecurity and fraud prevention in India's financial sector. The study explores the persistent cybersecurity threats facing financial institutions due to their vast stores of sensitive data and assets, making them prime targets for cyberattacks. The study reviews major cybersecurity incidents across sectors and emphasizes the legal, financial, and reputational risks associated with insufficient cyber defences. Key preventative measures include adopting authentication technologies, leveraging machine learning and predictive algorithms for threat detection, and investing in workforce training and awareness programs. The findings advocate for sustained cybersecurity investment to bolster consumer trust and ensure operational security in an evolving threat landscape.

3. DATA and METHODOLOGY

This study adopted a quantitative, cross-sectional survey design to investigate the effectiveness of cybersecurity measures in financial fraud prevention in Nigerian commercial banks. Data was

collected from randomly selected respondents using a structured questionnaire through online google forms distributed via WhatsApp groups and other social media platforms. The data captured demographic characteristics and varied opinions relevant for testing the hypotheses of the study. A total of 169 valid responses were obtained from individuals with experience using digital banking/payment platforms, covering different occupation categories (banking, legal, media & information, entrepreneurs, construction & engineering, healthcare, public sector, education, customer service, students, etc).

The study utilized the Hosmer and Lemeshow Test and Binary Logistic Regression (BLR) model which were conducted using SPSS 31. The model was applied to investigate how effectiveness of cybersecurity frameworks, authentication systems, and customer awareness programmes and internal institutional strategies predict fraud prevention. Hosmer and Lemeshow Test was applied to determine whether the model was best fit for the analysis. The model's relationship is expressed as follows;

$$\log\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_k x_k \quad \text{..... Eq (1)}$$

Where;

- (p = P(Y = 1)) is the probability of the event of interest,
- (β_0) is the intercept,
- (β_1, β_2, ..., β_k) are the coefficients of the independent variables (X_1, X_2, ..., X_k).

The model estimates the probability that the dependent variable, Y = 1, denoted as (p), given the values of the independent variables. Based on the objectives, the study estimated the model for the three hypotheses are as follows;

Hypothesis 1:

$$FinFraud\_Victim = \beta_0 + FPM\ Effectivess_1 + Cybersecurity\ Familiarity_2 + NG\_BankCyber\_Effectivess_3 + CyberAwareness\_Participation_4 \quad \text{.....Eq (2)}$$

Where;

FinFraud_Victim = responses to whether they have been a victim of financial fraud

FPM_Effectiveness = responses to how they rate the effectiveness of fraud prevention strategies currently in place.

NG_BankCyber_Effectiveness = responses to whether Nigerian banks enforce cybersecurity frameworks effectively

CyberAwareness_Participation = responses to whether they have participated in any bank cybersecurity awareness program.

Hypothesis 2:

$$FinFraud\_Victim = \beta_0 + used\ Biometric\ Auth?_1 + used\ Multi-factor\ auth?_2 + most\ secure\ auth_3 \quad \text{.....Eq(3)}$$

Where;

FinFraud_Victim = responses to whether they have been a victim of financial fraud

Used biometric auth? = responses to whether they have used biometric authentication
Used multi-factor auth? = responses to whether they have used multi-factor authentication.
Most secure authentication = responses to which authentication is most secure.
Hypothesis 3:

$$FinFraud\_Victim = \beta_0 + Cyberawareness\_Participation_1 + DataProtection\_Confidence_2 + CyberSecMeasures\_Index_3 \quad \text{Eq(4)}$$

Where;
FinFraud_Victim = Victims of Financial Fraud
Cyberawareness _Participation = responses to whether they have participated in any bank cybersecurity awareness program.
DataProtection_Confidence = responses to whether they have confidence in banks' ability to protect customers' data.
CyberSecMeasures_Index = Computed sum of responses to which preventive measures will assure more security.

4. ANALYSIS and RESULTS

Table 1. Demographic Distribution of Respondents

Variable	Categories	Freq	%age	Total	Variable	Categories	Freq	%age	Total
Gender	Male	58	34.30%		**Occupation Category**	Accounting	1	0.59%	
	Female	111	65.70%	169 (100%)		Architecture & Design	2	1.18%	
Marital Status	Single	112	66.3%			Banking	11	6.51%	
	Married	56	33.10%			Construction/Engineering	2	1.18%	
	Divorced	1	0.60%	169 (100%)		Courier Service	1	0.59%	
Age Group	18 - 25	71	42.00%			Customer Service	2	1.18%	
	26 - 35	46	27.20%			Education	18	10.65%	
	36 - 45	39	23.10%			Healthcare	4	2.37%	
	46 - above	13	7.70%	169 (100%)		Legal	1	0.59%	
Access to Digital Payment System	Yes	168	99.41%			Media & Communication	1	0.59%	
	No	1	0.59%	169 (100%)		Public Sector	15	8.88%	
Online Banking Use Frequency	Daily	132	78.11%			Sales	1	0.59%	
	Weekly	23	13.61%			Self Employed	12	7.10%	
	Monthly	4	2.37%			Student	98	57.99%	169 (100%)
	Rarely	9	5.33%						
	None	1	0.59%	169 (100%)					
Source: Researchers' Survey Output, 2025									

The demographic distribution in Table 1 shows critical insights into the composition and the background influencing the respondents' behaviour and attitudes toward digital banking. The data reflects a predominantly young and digitally inclined respondents with 65.7% identifying as female and 66.3% as single. Students represent the most common occupation at 57.99%, followed by those in education and the public sector. 99.41% have access to digital payment systems, and 78.11% use digital banking daily, indicating a high level of digital finance adoption. Overall, the

demographic skews toward individuals who are digitally engaged and likely comfortable making use of modern financial technology.

4.1. Test of Hypothesis: Hypothesis 1

Ho[1]: Cybersecurity frameworks have no significant effect on mitigating financial fraud in Nigerian commercial banks.

Table 2 showcases the survey questions and responses which formed the basis for testing hypothesis 1.

Table 2: Responses for Hypothesis 1

S/N	Variable	Responses/Code	Freq	%age	Total
1	Have you ever been a victim of financial fraud? **Dependent Variable**	Yes = 1	52	30.77%	
		No = 0	117	69.23%	169 (100%)
2	How familiar are you with the cybersecurity policies implemented by Nigerian banks? **Independent Variable**	Very Familiar = 3	55	32.54%	
		Somewhat Familiar = 2	70	41.42%	
		Not Familiar = 1	44	26.04%	169 (100%)
3	How would you rate the effectiveness of fraud prevention strategies currently in place? **Independent Variable**	Not Effective = 1	44	26.04%	
		Moderately Effective = 2	90	53.25%	
		Very Effective = 3	35	20.71%	169 (100%)
4	Do you believe Nigerian Banks enforce cybersecurity frameworks effectively? **Independent Variable**	Strongly Disagree = 1	25	14.79%	
		Disagree = 2	22	13%	
		Neutral = 3	61	36%	
		Agree = 4	24	14%	
		Strongly Agree = 5	37	22%	169 (100%)
	Source: Researchers' Survey Output, 2025				

Source: Researchers' Survey Output, 2025

Table 3: BLR & Hosmer and Lemeshow Test for Hypothesis 1

Variables in the Equation		B (Coefficient)	S.E.	Wald	df	Sig.	Exp(B) - Odds Ratio
Step 1[a]	FPM_Effectiveness	0.367	0.273	1.800	1	0.180	1.443
	NG_BankCyber_Effectiveness	-0.291	0.147	3.924	1	0.048	0.748
	CybersecFramework_Familiarity	0.239	0.239	1.005	1	0.316	1.270
	CyberAwareness_Participation	0.653	0.466	1.967	1	0.161	1.922
	Constant	-1.253	0.721	3.021	1	0.082	0.286
Hosmer and Lemeshow Test							
Step	Chi-square	df	Sig.				
1	6.093	8	0.637				

Researchers' Computation using SPSS 31

Table 3 shows the outcome of a binary logistic regression conducted to examine whether cybersecurity frameworks significantly influence the prevention of financial fraud. As indicated by the Hosmer and Lemeshow test, the model was confirmed a good fit ($\chi^2(8) = 6.093$, $p = 0.637$). Among the independent variables, only NG_BankCyber_Effectiveness (the perceived effectiveness of Nigerian banks' cybersecurity frameworks) was statistically significant (p-value = 0.048) with a coefficient of -0.291 and odds ratio (OR) of 0.748. This suggests that for each one-unit increase in perceived effectiveness, the odds of being a fraud victim decrease by approximately 25.2%. This

suggests that with intensified public messaging and transparency, cybersecurity policies have the potentials of actually protecting more bank customers from digital financial deception. Consequently, the null hypothesis, cybersecurity frameworks have no significant effect on mitigating financial fraud in Nigerian commercial banks is rejected based on the significance of NG_BankCyber_Effectiveness (p = .048), indicating that institutional cybersecurity controls contribute meaningfully to financial fraud mitigation.

4.2. Test of Hypothesis: Hypothesis 2

Ho^2: Authentication mechanisms do not significantly reduce cyber fraud in Nigeria's banking sector.

The survey questions and responses that formed the basis for testing hypothesis 2 are shown in Table 4.

Table 4: Responses for Hypothesis 2

S/N	Variable	Responses/Code	Freq	%age	Total
1	Have you ever been a victim of financial fraud? **Dependent Variable**	Yes = 1	52	30.77%	
		No = 0	117	69.23%	169 (100%)
2	Have you used biometric authentication? **Independent Variable**	Yes = 1	129	76.33%	
		No = 0	40	23.67%	169 (100%)
3	Have you used multi-factor authentication? **Independent Variable**	Yes = 1	88	52.07%	
		No = 0	81	47.93%	169 (100%)
4	Which athentication method do you find most secure? **Independent Variable**	Passwords & PINs = 1	56	33%	
		Biometric Verification = 2	65	38%	
		Multi-factor Authentication = 3	48	28%	169 (100%)
	Source: Researchers' Survey Output, 2025				

Table 5: BLR & Hosmer and Lemeshow Test for Hypothesis 2

Variables in the Equation		B (Coefficient)	S.E.	Wald	df	Sig.	Exp(B) - Odds Ratio
Step 1[a]	Used Biometric Auth	0.100	0.445	0.050	1	0.822	1.105
	Used multifactor Auth	-0.126	0.374	0.113	1	0.736	0.882
	Mostsecureauth	0.012	0.236	0.002	1	0.961	1.012
	Constant	-0.846	0.480	3.100	1	0.078	0.429
Hosmer and Lemeshow Test							
Step	Chi-square	df	Sig.				
1	6.972	5	0.223				
Source: Researchers's Computation using SPSS 31							

In assessing whether authentication systems reduce cyberfraud in Nigeria's banking sector, binary logistic regression was conducted and the results depicted in Table 5. With a statistically insignificant p-value of 0.223, the Hosmer and Lemeshow test indicates that the model is fit. However, none of the independent variables were statistically significant judging from their p-values (*ps* > .05), indicating that the use of biometrics, multi-factor authentication, or user-

reported secure methods had no significant impact on cyberfraud reduction. These results suggest that authentication practices alone may be insufficient to reduce fraud risk or that other behavioural (user abuse or inadequate implementation) and contextual variables enable this relationship. Since there is no statistically significant evidence that these authentication mechanisms reduce cyberfraud, the null hypothesis in hypothesis 2 cannot be rejected.

4.3. Test of Hypothesis: Hypothesis 3

Ho^3: Customer awareness and institutional strategies do not have a significant impact on fraud prevention in Nigerian banks.

The survey questions and responses that formed the basis for testing hypothesis 3 are shown in Table 6.

Table 6: Responses for Hypothesis 3

S/N	Variable	Responses/Code	Freq	%age	Total
1	Have you ever been a victim of financial fraud? **Dependent Variable**	Yes = 1	52	30.77%	
		No = 0	117	69.23%	169 (100%)
2	How confident are you in Nigerian banks' ability to protect customer data? **Independent Variable**	Not Confident = 1	37	21.89%	
		Somewhat Confident = 2	93	55.03%	
		Very Confident = 3	39	23.08%	169 (100%)
3	Have you attended any cybersecurity awareness programs offered by a bank? **Independent Variable**	Yes = 1	25	14.79%	
		No = 0	144	85.21%	169 (100%)
4	Cybersecurity Measures Index. **Independent Variable** generated from the responses to the question; What would make you more secure using online banking? (select all that apply)	Stronger Authentication Methods	177	105%	
		Improved Fraud Monitoring System	93	55%	
		Increased Customer Education on Cybersecurity	94	56%	
		Enhanced Bank Security Policies	100	59%	
	Source: Researchers' Survey Output, 2025				

Table 7: BLR & Hosmer and Lemeshow Test for Hypothesis 3

Variables in the Equation		B (Coefficient)	S.E.	Wald	df	Sig.	Exp(B) - Odds Ratio
Step 1[a]	CyberAwareness_Participation	0.762	0.454	2.822	1	0.093	2.143
	DataProtection_Confidence	-0.143	0.258	0.309	1	0.578	0.866
	CyberSecMeasures_Index	-0.166	0.117	2.030	1	0.154	0.847
	Constant	-0.288	0.582	0.245	1	0.621	0.750
Hosmer and Lemeshow Test							
Step	Chi-square	df	Sig.				
1	2.165	7	0.950				
Source: Researchers's Computation using SPSS 31							

Table 7 shows the logistic regression model assessing the participation of customers in cybersecurity awareness programs, confidence in banks' data protection, and cybersecurity measures index. With a statistically insignificant p-value (0.95), the model fitness is very good as indicated by the Hosmer and Lemeshow test. Considering the p-values, none of the independent variables were statistically significant at the 5% level. This implies that the study data doesn't support a statistically significant link between customer awareness/institutional strategy and fraud

prevention. This is an indication that deploying cybersecurity frameworks doesn't ensure good results (effective cyberfraud elimination) without complete user engagement or buy-in. However, though statistically insignificant, Cyberawareness_Participation with an odds ratio of 2.14, proves to be a key potential driver for boosting cybersecurity. This is suggestive of the fact that individuals that have undergone cybersecurity awareness campaigns or training are most likely to evade cyberfraud. Consequently, the null hypothesis in hypothesis 3 cannot be rejected.

Although authentication mechanisms and customer awareness programs did not show statistically significant effects, their practical relevance remains important, especially when supported by user-friendly design and engagement strategies.

5. CONCLUSION

The study evaluates the effectiveness of cybersecurity measures in preventing financial fraud in Nigeria's banking sector. Adopting a cross-sectional survey design, data were retrieved randomly from 169 valid responses using online (Google Form) structured survey. Specifically, the binary logistic regression model was used to evaluate how perceived effectiveness of Nigerian banking cybersecurity frameworks, authentication mechanisms and, customer awareness and institutional strategies predicts the incidence of financial fraud in the banking sector.

The study revealed that perceived effectiveness of Nigerian banking cybersecurity frameworks has a significant effect on mitigating financial fraud in Nigerian commercial banks. Cybersecurity frameworks have the potentials of actually shielding bank customers from cyber threats once they are implemented with transparency and adequate public outreach. However, authentication measures (Passwords & PINs, biometric verification and multi-factor authentication) and participation in cyber awareness programs did not exhibit statistically significant effects, stressing a disconnect between cybersecurity measures adoption and cyberfraud prevention. This suggests that deployment and adoption alone, without adequate user-engagement and buy-in, doesn't enforce security in the financial cyber space.

6. RECOMMENDATIONS

Considering the analysis and findings, and also based on the opinions of the respondents on how best to enhance cybersecurity in banks, the study recommends the following;

1. Improve on Proactive Cyber Awareness: There is need to prioritize timely, interactive awareness campaigns, especially for rural and less technically inclined users, in order to build cybersecurity habits before fraud exposure.
2. Match up Cybersecurity Measures with Education: Besides strengthening the authentication methods (biometrics, multi-factor authentication), it is important to integrate them with training to prevent misuse and overreliance.
3. Incorporate Behavioural Biometrics for Continuous Authentication: In addition to the traditional and other authentication methods, implementing continuous monitoring based

on bank customer behaviour/patterns (keystroke dynamics, mouse movement, or mobile usage patterns), will enhance real time fraud detection.

4. Leverage AI-Driven Cybersecurity measures: The advent of AI has broken barriers in the technological ecosystem. Adopting AI featured cybersecurity measures alongside machine learning and blockchain technology will effectively improve on real time monitoring and prevention of cyber threats in the financial sector.
5. Foster Institutional Trust and Strong Security Policies: The need for transparency on the part of financial institutions cannot be overemphasized as clear, regular communication can enhance user trust and indirectly reduce fraud risk. Furthermore, zero trust models, regular risk assessments, and internal controls should be effectively implemented.
6. Data Protection and Improved User Experience: Efforts should be made to protect customers' data using enhanced data encryption and firewalls. Again, there is need to design simple and user-friendly interface or frameworks to encourage practical adoption by a wider audience.
7. Adopting Human-Centred Approach: Whatever policies, technologies, and behavioural strategies that are deployed should be organized into interventions that centre end-user practices.

References

Abiodun, A. (2023, November 19). Nigeria's financial sector under siege: The alarming rise of cyber fraud and inadequate defences. Business Day. https://businessday.ng/opinion/article/nigerias-financial-sector-under-siege-the-alarming-rise-of-cyber-fraud-and-inadequate-defenses/

Aburaya, N. M., & Barnat, S. E. (2023). Protecting bank customers from cyber threats (electronic fraud and identity theft) and the legal guarantees introduced in Saudi legislation. Migration Letters, 20(11), 28 – 36. https://migrationletters.com/index.php/ml/article/download/5582/3811/15466.

Adeyemo, K. & Obafemi, F. J. (2024). Technological innovation as a catalyst for fraud prevention in Nigeria deposit money banks. Journal of Research in International Business and Management, 11(1). https://www.interesjournals.-org/articles/technological-innovation-as-a-catalyst-for-fraud-prevention-in-nigeria-deposit-money-banks-104691.html.

Advocacy for Policy Innovation (2021). National cybersecurity policy & strategy, 2021. https://api.apiintelligence.org/upload/4650ae0b15daf1e5c3fac12e93cb-de610.pdf.

Ama, G. A. N., Onwubiko, C. O., & Nwankwo, H. A. (2024). Cybersecurity challenge in Nigeria deposit money banks. Journal of Information Security, 15, 494 – 523. https://doi.org/10.4236/jis.2024.154028.

Ayodeji, I. A. (2024). Fraud detection and prevention in the Nigerian financial industry (Doctoral Dissertation). Walden University. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=18284&context=dissertations.

Backbase (2024, November 9). Cybersecurity in banking:
the complete guide. https://www.backbase.com/blog/modernization/-cybersecurity-in-banking-the-complete-guide.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. PLOS ONE, 19(4), 1 – 16. https://doi.org/10.1371/journal.pone.0297312.

CBN (2018). Risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers. https://www.cbn.gov.ng/out/2018-/bsd/risk%20based%20cybersecurity%20framework%20final.pdf.

CBN (2020a). Payments system vision 2020. https://www.cbn.gov.ng/-PaymentsSystem/PSV2020.html#:~:text=The%20Payment%20Systems%20Vision%202020%20provides%20a,and%20internationally%20recognized%20as%20being%20world%20class.

CBN (2020b). The Nigerian payment system risk and information security management framework. https://www.cbn.gov.ng/out/2020/psmd/nigerian-%20payments%20system%20risk%20and%20information%20security%20management%20framework.pdf

CBN (2021). Regulatory framework for mobile money services in Nigeria. https://www.cbn.gov.ng/Out/2021/CCD/Framework%20and%20Guidelines%20on%20Mobile%20Money%20Services%20in%20Nigeria%20-%20July%202021.pdf

CBN (2022). Risk-based cybersecurity framework and guidelines for other financial institutions. https://www.cbn.gov.ng/Out/2022/OFISD/Letter%20to%20all%20OFIs%20Issuance%20of%20Risk-Based%20Cybersecurity%20Framework%20and%20Guidelines%20for%20Other%20Financial%20Institutions.pdf

CBN (2024). Risk-based cybersecurity framework and guidelines for DMBs and PSBs. https://www.cbn.gov.ng/Out/2024/BSD/CBN%20Risk-Based%20Cybersecurity%20Framework%20for%20DMBs%20and%20PSBs_2024.pdf

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

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319 – 340. https://www.researchgate.net/profile/Fred-Davis-3/publication/200085965_Perceived_Usefulness_Perceived_Ease_of_Use_and_User_Acceptance_of_Information_Technology/links/54ad66dc0cf24aca1c6f3765/Perceived-Usefulness-Perceived-Ease-of-Use-and-User-Acceptance-of-Information-Technology.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Digital Policy Alert. (2024). Nigeria: adopted CBN risk-based cybersecurity framework and guidelines for deposit money banks and payment service banks, including minimum cybersecurity requirements. https://digitalpolicyalert.org/event/25170-adopted-cbn-risk-based-cybersecurity-framework-and-guidelines-for-deposit-money-banks-and-payment-service-banks-including-minimum-cybersecurity-requirements.

Doghudje, I. (2025, January 22). Safeguarding Nigeria's Financial Future: Lessons from cybersecurity breaches. The Guardian. https://guardian.ng/technology/safeguarding-nigerias-financial-future-lessons-from-cybersecurity-breaches/

Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. International Journal of Science and Research Archive, 9(2), 503–515. https://doi.org/10.30574/ijsra.2023.9.2.0609.

Federal Republic of Nigeria (2021). National Cybersecurity Policy and Strategy, 2021. https://www.ncc.gov.ng/media/800/view.

FITC (2024a). Report on frauds and forgeries in Nigerian banks; quarter 1 2024. https://fitc-ng.com/wp-content/uploads/2024/07/Q1-24.pdf.

FITC (2024b). Report on frauds and forgeries in Nigerian banks; quarter 2 2024. https://fitc-ng.com/wp-content/uploads/2024/09/Fraud-and-Forgery-2024-2nd-Quarter.pdf#:~:text=Additionally%2C%20the%20total%20amount%20lost%20due%20to,2024%20to%20%E2%82%A642.6%20billion%20in%20Q2%202024.&text=In%20summary%2C%20the%20second%20quarter%20of%202024,cases%20reported%20in%20the%20first%20quarter%20of2024.

Folami, R. A., Yinusa, G. O., & Toriola, A. K. (2024). Digital payment fraud and bank fragility: evidence from deposit money banks in Nigeria. African Journal of Economic Review, 12 (4), 21 – 37. https://www.ajol.info/index.php/ajer/article/view/283619.

Khattri, V. & Singh, D. K. (2018). Parameters of automated fraud detection techniques during online transactions. Journal of Financial Crime, 25(3), 702 – 720. https://www.emerald.com/insight/content/doi/10.1108/JFC-03-2017-0024/full/html?utm_source=repec&utm_medium=feed&utm_campaign=repec

Kolade, E. (2022, May 13) Cybersecurity in Nigeria's financial industry: enhancing consumer trust and security. https://carnegieendowment.org/research/2022-/05/cybersecurity-in-nigerias-financial-industry-enhancing-consumer-trust-and-security?lang=en.

Lersch, K. M., & Hart, T. C. (2023). Does routine activity theory still matter during COVID-19 restrictions? The geography of sexual assaults before, during, and after COVID-19 restrictions. Journal of Criminal Justice, 86, 102050. https://doi.org/10.1016/j.jcrimjus.2023.102050

Luna, C. (2024, September 13). Cybersecurity in banking: threats, solutions & best practices. https://www.esecurityplanet.com/cloud/cyber-security-in-banking/

Metibemu, O. C. (2025). Financial risk management in digital-only banks: addressing fraud and cybersecurity threats in a cashless economy. Asian Journal of Research in Computer Science, 18(3), 434 – 455. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5166723.

Mukoro, G. (2024, September 6). Cybersecurity in finance companies: adhering to the CBN framework and guidelines in Nigeria. https://uidcfinancecompany.com.ng/news/detail/cybersecurity-in-finance-companies-adhering-to-the-cbn-framework-and-guidelines-in-nigeria/

Mustapha, A., & Sinha, A. (2024). Cyberfraud in Nigerian banking sector: The techniques and preventive measures. International Journal of Innovative Science and Research Technology, 9(8), 171 – 179. https://doi.org/10.38124/ijisrt/IJISRT24AUG395.

NIBSS (2024). 2023 Annual fraud landscape. https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdf.

Nigeria Deposit Insurance Corporation (2018) Annual Report. https://ndic.gov.ng/wp-content/uploads/2020/08/Year-2018-Annual-Report.pdf.

Nigerian Financial Intelligence Unit (2015). Cybercrime (prohibition, prevention, etc) act. https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf.

Nguyen, P., Pham, T., Nguyen, L. T., Pham, H. T., Nguyen, T. T., & Vu, T. (2024). Assessing cybersecurity risks and prioritizing top strategies in Vietnam's finance and banking system using strategic decision-making models-based neutrosophic sets and Z number. Heliyon, 10(19), 1 – 27. https://doi.org/10.1016/j.heliyon.2024.e37893.

Nkwor, L. & Adeyemo, I. (2024). Overview of the CBN Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks. https://www.gelias.com/images/Newsletter/_Overview_of_the_CBN_Risk-Based_Cyber_Security_Framework.pdf

Odukwu, V. C., Eke, P., & Chukwumati, M. N. (2022). Impact of cyber-security on fraud prevention in Nigerian commercial banks. Jurnal Akuntansi, Keuangan, dan Manajemen (Jakman), 4(1), 15 – 27. https://doi.org/10.35912/jakman.v4i1.1527.

Odunewu, S. (2025, February 27). Financial sector fraud surges to N52.26bn in 2024 – Report. Blueprint. https://blueprint.ng/financial-sector-fraud-surges-to-n52-26bn-in-2024-report/.

Olaniwun Ajayi Newsletter (2020, January). The Nigerian payments system risk and information security management framework 2020. https://www.olaniwunajayi.net/wp-content/uploads/2020/01/The-Nigerian-Payments-System-Risk-And-Information-Security-Management-Framework-2020.pdf

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cyber security risks in online banking: a detailed review and preventative strategies application. World Journal of Advanced Research and Reviews, 14, 45-60.

Timi-Koleolu, S., & Aroh, E. (2022). Regulatory update: cybersecurity framework and guidelines for financial institutions in Nigeria. https://www.mondaq.com/nigeria/security/1210436/regulatory-update-cybersecurity-framework-and-guidelines-for-financial-institutions-in-nigeria

Sowunmi, T., & Nkposong, M. (2021). CBN issues revised guidelines on mobile money services in Nigeria. https://www.aluko-oyebode.com/wp-content/uploads/2021/07/CBN-ISSUES-REVISED-GUIDELINES-ON-MOBILE-MONEY-SERVICES-IN-NIGERIA-001.pdf.

Venkatesh, V. & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. Management Science, 46(2), 186 – 204. http://dx.doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V. and Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. Decision Science, 39(2), 273 – 312.

Wani, P., & Bhosale, V. P. (2024). Cybersecurity and fraud prevention in India's financial sector: A comprehensive review. International Journal of Creative Research Thoughts, 12(15), 494 – 501. https://ijcrt.org/papers/IJCRT2405271.pdf. .