SSR Journal of Multidisciplinary (SSRJM)

Volume 3, Issue 1, 2026

Homepage: https://ssrpublisher.com/ssrjm/
Email: office.ssrpublisher@gmail.com

OPEN ACCESS

ISSN: 3049-1304

Comparative Analysis of Financial Fraud Techniques in Nigeria: Assessing the Prevalence and Impact of Expert-Based Hacking and Social Engineering Strategies

Muhammad Nuraddeen Ado[1,2*]; Jabir Isah Karofi[3] & Hamisu Mukhtar[4]

[*1]Department. Of Information Sciences, Federal University, Dutsin-Ma
[*2]Department of Cyber Security, ACETEL, National Open University of Nigeria
[3]Department of Information Sciences, Federal University, Dutsin-Ma
[4]Department of ICT, Air Force Institute of Technology, Kaduna

Received: *21.12.2025* | ***Accepted:*** *09.01.2026* | ***Published:*** *26.01.2026*

***Corresponding Author:** Muhammad Nuraddeen Ado

DOI: *10.5281/zenodo.18372446*

Abstract

Original Research Article

This study presents a comprehensive empirical analysis of financial fraud techniques in Nigeria, a representative case of underdeveloped countries grappling with evolving cybercriminal threats. It focuses on two dominant fraudulent methodologies: expert-based hacking—which exploits systemic and infrastructural vulnerabilities using technical means such as brute force attacks and cryptanalysis—and social engineering, which manipulates human psychology to extract sensitive financial data or deceive victims into self-compromise. To achieve a balanced perspective, the study adopts a mixed-methods research design that integrates both quantitative and qualitative approaches. Quantitative data were collected via a structured survey administered to 2,000 respondents, comprising victims, financial institution personnel, law enforcement officers, and regulatory officials across Nigeria's six geopolitical zones. Qualitative insights were gleaned from semi-structured interviews with cybersecurity experts and financial crime regulators.Analysis reveals that social engineering accounts for nearly 80% of reported financial crimes, with platforms such as Facebook and LinkedIn serving as key enablers for identity fraud and phishing schemes. In contrast, expert-based hacking appears less frequently acknowledged among respondents, possibly due to its covert nature. Notably, the study identifies the use of "layering"—a method of obscuring illicit fund origins through digital wallets and multiple transaction paths—as a common mechanism that supports both fraud strategies. Statistical methods, including two-way ANOVA, were employed to compare the relative impact and prevalence of these tactics, uncovering significant regional and demographic variations. Thematic analysis of interviews further uncovers limitations in current regulatory and detection frameworks, particularly the overreliance on reactive, rather than proactive, security protocols.The findings underscore an urgent need for targeted countermeasures, such as public awareness campaigns, adaptive regulatory policies, strengthened digital forensic capabilities, and international cooperation frameworks. This study offers crucial guidance for cybersecurity practitioners, financial institutions, and policy architects seeking to fortify Nigeria's—and by extension, other developing nations'—resilience against the multifaceted threats of financial fraud.

Keywords: Expert-Based Hacking, Social Engineering, Tactics, Techniques, and Procedures (TTPs) Brute Force Attacks, Cryptanalysis.

1.0 Introduction

Financial fraud represents an escalating global threat with disproportionately severe implications for developing nations, where institutional weaknesses, limited regulatory oversight, and digital illiteracy exacerbate vulnerabilities. In countries like Nigeria, the convergence of rapid technological adoption and underdeveloped cybersecurity infrastructure creates fertile ground for diverse forms of financial crime. The widespread shift to cloud-based financial systems and mobile banking platforms—often introduced without comprehensive user education or robust encryption standards—has amplified exposure to cyber threats (Jones, 2019).

Nigeria’s financial ecosystem, which includes formal banks, microfinance institutions, fintech startups, and informal savings schemes, is highly dynamic but also loosely regulated in certain sectors. This heterogeneity contributes to a complex risk landscape in which expert-based hacking and social engineering emerge as dominant tactics of financial exploitation.

Expert-based hacking refers to the use of advanced technical skills to exploit system-level vulnerabilities. Perpetrators leverage methods such as brute force attacks, cryptanalysis, and SQL injections to gain unauthorized access to protected databases and customer information. These bottom-up approaches specifically target technical weaknesses in digital infrastructures, payment gateways, and identity verification systems (Smith et al., 2020). As financial institutions increasingly rely on cloud computing and mobile platforms, hackers continually adapt their tactics, creating a perpetual arms race between security defenders and attackers (Johnson & Patel, 2018).

In contrast, social engineering operates through top-down strategies that exploit human psychology rather than system flaws. Cybercriminals deploy deceptive tactics—ranging from fake job offers and Ponzi schemes to romance scams and phishing emails—often disseminated via ubiquitous platforms like Facebook, LinkedIn, WhatsApp, and Instagram. These schemes prey on victims' emotional and financial vulnerabilities, particularly amid high unemployment rates and aspirations for migration to developed countries such as the United States, Canada, and various European nations (Adams & Mayer, 2017). The success of social engineering lies in its adaptability and low barrier to entry, making it an appealing tool for both organized cybercrime networks and individual fraudsters (Brown & Jones, 2019).

The Nigerian context is further complicated by socio-political factors such as inadequate cybercrime legislation enforcement, high youth unemployment, and the proliferation of mobile payment systems without corresponding education on digital risk. Additionally, emerging practices like “layering”—a money laundering technique involving multiple financial transactions across wallets and accounts to obscure illicit fund origins—enhance the complexity and resilience of fraudulent operations.

This study seeks to bridge a critical gap in current literature by providing a comparative, empirical analysis of the tactics, techniques, and procedures (TTPs) employed in both expert-based hacking and social engineering. Using a mixed-methods approach that combines quantitative data from 2,000 structured survey responses with qualitative insights from in-depth interviews, the research captures both macro-level trends and micro-level mechanisms of fraud. The ultimate goal is to equip policymakers, financial institutions, cybersecurity practitioners, and regulatory bodies with actionable insights for developing context-specific, technology-aware, and behaviorally informed counter-fraud strategies.

In an era where financial crimes transcend national borders and leverage sophisticated digital tools, enhancing the resilience of Nigeria's financial infrastructure demands a multidimensional understanding of both technical and human vulnerabilities. The findings from this study are intended to inform not only Nigeria’s domestic financial policy but also broader frameworks for combating financial fraud in underdeveloped economies facing similar challenges (Miller, 2021; Johnson et al., 2022).

1.1 Problem Statement

Financial fraud constitutes a critical and persistent threat to Nigeria’s financial stability and socio-economic development. The nation's growing reliance on digital financial systems, mobile banking, and informal transfer mechanisms has outpaced the development of corresponding cybersecurity measures, rendering the financial ecosystem increasingly vulnerable to both technical and psychological exploitation. Fraudsters operating within this context utilize a broad spectrum of tactics—chief among them being expert-based hacking and social engineering—to infiltrate and manipulate financial systems, institutions, and individuals (Okoye et al., 2021; Adetoro et al., 2022).

Compounding the problem are regulatory and systemic inadequacies. For instance, the Central Bank of Nigeria (CBN) has implemented restrictions on certain international money transfers (e.g., payments for SEVIS fees or educational expenses abroad), aiming to curb illicit capital outflows. However, such blanket policies have inadvertently disrupted legitimate transactions and driven some users toward informal or unregulated channels—spaces frequently exploited by fraudsters (Kenna Partners, 2024; Nairametrics, 2024). This highlights a regulatory paradox where anti-fraud efforts may inadvertently enable fraud through insufficient differentiation between legitimate and suspicious transactions.

Furthermore, there is an alarming intersection between financial fraud and national security concerns. The proliferation of arms in Northern Nigeria—linked to organized crime and terrorist financing—indicates that financial fraud does not merely destabilize banks or individuals but may also be funding extremist networks and fueling insecurity in the region (Mondaq, 2024). Such dynamics underscore the broader, often overlooked implications of financial crime as a driver of political and social instability.

Critically, Nigeria's current framework for addressing financial crime is predominantly reactive and fragmented, relying on outdated detection tools and inconsistent enforcement. Law enforcement agencies often lack the training, digital infrastructure, and real-time intelligence-sharing protocols required to identify and disrupt emerging fraud typologies. The lack of integration between cybersecurity policy and public education also contributes to the sustained vulnerability of financial service users.

Despite the scale of the problem, there remains a significant knowledge gap in understanding the specific tactics, techniques, and procedures (TTPs) employed by perpetrators of financial fraud within the Nigerian context. While anecdotal and media-based reports are abundant, there is a shortage of empirical, data-driven research that compares the prevalence and operational mechanisms of expert-based hacking versus social engineering—two distinct but interlinked vectors of financial exploitation.

This study seeks to bridge that gap by conducting a comparative analysis of these two tactics, using a mixed-methods approach to quantify their relative prevalence, assess their operational methodologies, and evaluate their impact on both economic performance and public trust in financial institutions. The analysis will draw upon structured survey data from 2,000 participants across key demographic and professional groups, as well as qualitative insights from cybersecurity practitioners and policy stakeholders.

By elucidating the specific fraud pathways and their broader implications, this research aims to inform the development of targeted, evidence-based countermeasures. These include improved detection technologies, regulatory reforms, cross-sectoral collaboration, and public education initiatives. Ultimately, the study aspires to bolster Nigeria’s institutional capacity to detect, prevent, and respond to financial fraud, thereby enhancing the resilience of its financial ecosystem and safeguarding national security.

Aim and Objectives

This study aims to comprehensively investigate and compare the tactics, techniques, and procedures (TTPs) used in financial fraud across Nigeria, focusing on two dominant paradigms: expert-based hacking and social engineering. The following specific objectives guide the investigation:

i. *To quantify the relative prevalence of expert-based hacking versus social* *engineering methodologies in the commission of financial crimes in Nigeria.*

ii. *To assess the effects of these methodologies on the incidence, scale, and demographic distribution of financial fraud within Nigeria.*

2.0 Review of Related Literature

Financial fraud in underdeveloped countries like Nigeria has rapidly evolved in sophistication and scope. A consensus across literature highlights two core tactics: expert-based hacking and social engineering. These approaches often operate in parallel—technological expertise weaponizes vulnerabilities in infrastructure, while manipulative psychological tactics exploit human error.

Expert-Based Hacking Techniques

Expert-based hacking refers to the use of advanced technical knowledge, such as brute force, cryptanalysis, and password sniffing, to gain unauthorized access to digital systems. Aransiola and Asindemade (2011) conducted a study on system breaches, demonstrating that backdoor programs and packet sniffers are deployed to continuously extract data from financial systems. Similarly, Urbas and Choo (2008) emphasized that hackers can leverage weak authentication protocols to infiltrate networks and exfiltrate sensitive banking data.

Cryptanalytic attacks and brute-force strategies remain central in the toolkit of sophisticated cybercriminals. Evidence from cybersecurity trend analyses shows that such methods can defeat even two-factor authentication systems when combined with spoofing or SMS-based impersonation. The Nigerian Interbank Settlement System (NIBSS) has been a repeated target due to legacy vulnerabilities in backend databases and API endpoints.

Social Engineering and Psychological Exploits

While expert hacking is technical, social engineering manipulates human behavior. Hussein Akeiber (2025) described social engineering as a "cleverness of psychology," wherein attackers exploit trust, urgency, fear, and authority to coerce victims into revealing confidential information. This is consistent with Wall (2007) and Rahman (2012), who noted that Nigerian fraudsters exploit social media and messaging platforms for phishing, posing as relatives, officials, or institutions to extract financial credentials.

Spear phishing attacks, tailored using harvested social media data (especially Facebook and LinkedIn), have become prevalent. These attacks leverage psychological vulnerabilities—curiosity, greed, and urgency—to bypass rational user defenses. Rahman (2012) and Unini (2019) discussed fake charity schemes and job recruitment scams as frequent vectors through which fraudsters solicit money or information.

Prevalence and Platform-Specific Vectors

Udanor et al. (2020) employed a logistic predictive model showing that ATM fraud and mobile banking scams dominate Nigeria's financial cybercrime landscape, though social engineering (via calls, emails, and apps) plays a major enabling role. Surveys confirm that cyber fraud victims are more likely to report human-mediated scams (like phishing) than brute-force attacks, possibly due to visibility and recognition bias.

Mechanisms and Money Movement: The Role of Layering

"Layering" is a shared characteristic between expert hacking and social engineering. As identified in the studies by Ewa (2022) and Odufisan et al. (2025), cybercriminals often move illicit funds through digital wallets, cryptocurrencies, and multiple transaction chains to obscure the money trail. This form of laundering makes legal tracing difficult, particularly when funds are split and routed internationally.

Institutional Responses and Regulatory Gaps

Although Nigeria has enacted the Cybercrime Act (2015) and strengthened KYC requirements, enforcement remains reactive. As documented by Babando (2022) and Drammeh (2023), the system suffers from undertrained investigators, weak digital forensic units, and delayed prosecution. Owolabi and Ogunsola (2021) emphasized that forensic auditors are inadequately integrated into banking systems, thus limiting proactive fraud detection.

Recommendations from Literature

Nearly all reviewed studies advocate for greater digital forensic capacity, including real-time transaction monitoring, and cross-border cooperation. Public awareness campaigns were also highlighted as vital. As Akeiber (2025) concluded, collaboration between cybersecurity experts and behavioral psychologists is essential to mitigate social engineering risks.

This literature review clearly positions expert-based hacking and social engineering as interdependent pillars of financial fraud in Nigeria. It also reflects the dual necessity of technological defense systems and human-centered security awareness for effective fraud prevention.

Table 1 below highlights the papers studied with the most relevance to this study and the specific relevance to this study.

Table 1: Summary of Reviewed Papers

Paper	Focus	Techniques	Relevance to this Study
Udanor et al. (2020)	Predictive modeling of cybercrime modes in Sub-Saharan Africa	Logistic regression, empirical survey	Supports TTP prevalence modeling and ATM/mobile fraud profiling
Akeiber (2025)	Evolution of AI-driven social engineering attacks	Case review, cybersecurity engineering	Aligns with tactics via online deception and deepfakes
Fatoki (2023)	Cybersecurity's effect on financial fraud in Nigerian banks	Survey, regression	Empirical grounding for expert-based hacking and systemic gaps
Bhusal (2021)	Taxonomy and review of social engineering methods	Systematic review	Validates psychological tactics used in fraud and online manipulation
Awodiran et al. (2023)	Role of digital forensic accounting in cyber fraud	Survey, correlation	Corroborates findings on phishing, layering, and prosecution lags
Zarpala & Casino (2021)	Blockchain-based forensic model for investigation	Prototype simulation	Technological context for forensic innovation and traceability
Ayodeji (2024)	Mixed-methods study of	Qualitative interviews, big data	Supports empirical structure and insights into detection challenges

	fraud detection tools in Nigeria		
Temple et al. (2022)	Assessment of EFCC's role in controlling fraud	Survey, chi-square	Highlights enforcement and policy gaps aligned with your discussion
Awale et al. (2025)	Gendered insights into institutional financial crime	Survey + fraud model analysis	Psychosocial lens on SE and ethical control structures
Olujobi & Yebisi (2022)	Legal framework analysis of money laundering laws	Doctrinal legal review	Anchors your "layering" mechanism in legal enforcement context

3.0 Methodology

This section outlines the methodological framework employed to investigate the evolving dynamics of financial fraud in Nigeria, with a specific emphasis on the comparative analysis of Expert-Based Hacking (EBH) and Social Engineering (SE) as predominant tactics, techniques, and procedures (TTPs). The methodology integrates both quantitative and qualitative paradigms under a mixed-methods research design, ensuring a comprehensive and multidimensional understanding of how these two fraud strategies manifest across demographic, institutional, and regional contexts. This approach not only facilitates empirical measurement of prevalence and perceived impact but also allows for rich, expert-driven insights into operational patterns and institutional countermeasures. The subsequent components—research objectives, design, instruments, sampling strategy, data collection, and analysis—are systematically detailed. Additionally, this section includes an illustrative research process diagram to visually represent the sequential phases of inquiry, from problem identification through data interpretation and dissemination. Ethical considerations and the geographical scope of the study, covering Nigeria’s six geopolitical zones, are also clearly articulated to underscore both the integrity and representativeness of the research.

Research Process

Fig 1 illustrated the research process for this study which presents a dynamic and visually enriched flow of sequential phases that guide the investigation of financial fraud in Nigeria, with a focus on expert-based hacking and social engineering. It begins with problem identification, where the scope and critical nature of cyber-financial crimes are contextualized, followed by a robust literature review establishing theoretical foundations. The process proceeds to a mixed-methods research design, integrating both quantitative surveys and qualitative interviews, supported by SMART-based instruments and stratified sampling across Nigeria's six geopolitical zones. Data collection methods—online, telephonic, and in-person—ensure inclusivity and regional representation. Analytical tools, including descriptive statistics and ANOVA for quantitative data, and thematic coding for qualitative insights, facilitate rigorous interpretation. The diagram also emphasizes triangulation for data validation, ethical considerations to uphold research integrity, and dissemination strategies, ensuring that the findings are not only methodologically sound but also actionable for policymakers, cybersecurity professionals, and financial institutions. Each step is visually represented with relevant icons and symbolic elements, enhancing clarity and engagement.

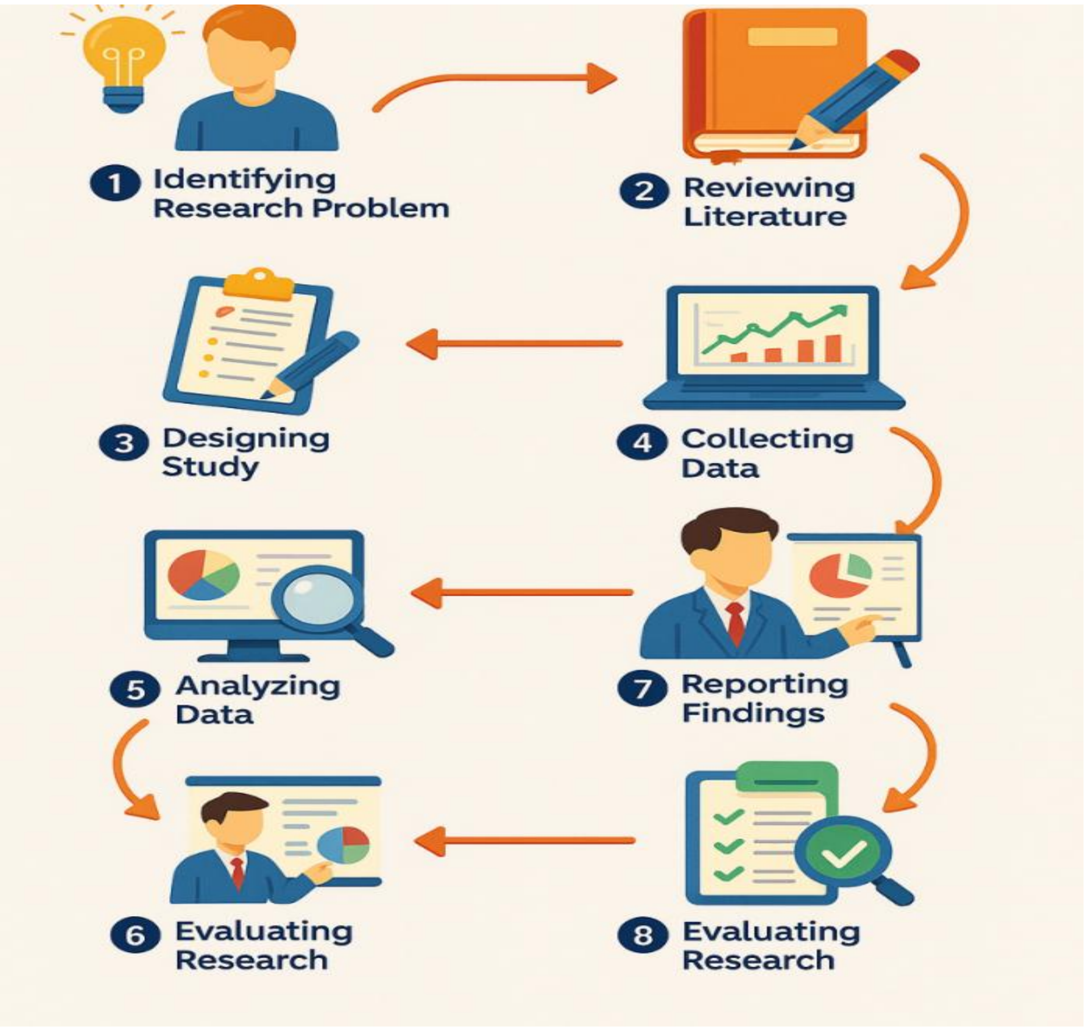

Fig 1. Research Process Framework

Research Design

A mixed-methods research design was adopted to leverage the strengths of both quantitative and qualitative approaches. This design provides a holistic view by capturing both statistical trends and experiential insights on how expert-based hacking and social engineering contribute to financial fraud.

Quantitative Component

Survey Instrument:

A structured questionnaire was developed to gather empirical data on the types, frequency, and impact of financial fraud. The instrument was designed using the SMART framework (Specific, Measurable, Achievable, Relevant, and Time-bound) to ensure precision, relevance, and analytical utility. Questions were predominantly closed-ended and included Likert-scale, categorical, and ordinal items.

Sampling Technique:

A stratified random sampling method was utilized to achieve representativeness across Nigeria’s six geopolitical zones. The strata were defined by:

a. Geographical distribution (states from all zones)

b. Respondent type: financial fraud victims, banking/financial institution personnel, law enforcement agents, and regulatory officials.

Data Collection:

Data was collected from a total of 2,000 respondents, using a hybrid mode of delivery:

c. Online surveys via secure digital platforms

d. Telephone interviews for accessibility in remote areas

e. Face-to-face interviews for enhanced clarity and trust

Respondents included 1,200 victims of financial fraud and 800 professionals from relevant regulatory and enforcement institutions.

Quantitative Data Analysis:

Collected data was coded and analyzed using statistical software (e.g., SPSS or R). Analysis involved:

✓ Descriptive statistics (frequencies, percentages, cross-tabulations)

✓ Inferential statistics, specifically two-way ANOVA, to examine variations across demographics and fraud types.

Qualitative Component

Semi-Structured Interviews:

In-depth semi-structured interviews were conducted with subject-matter experts, including cybersecurity analysts, senior banking security personnel, anti-fraud officers from the appropriate institutions, and regulatory policymakers.

Thematic Analysis:

Interview transcripts were coded and analyzed thematically using NVivo or a similar qualitative software. Core themes were identified, such as human vulnerability exploitation, infrastructure gaps, evolution of phishing tactics, and social media's role in fraud.

Triangulation and Validity Checks:

To enhance the reliability and validity of findings, methodological triangulation was applied. This involved integrating statistical patterns with expert insights and conducting member-checking with interviewees.

Ethical Considerations

All procedures adhered to ethical research standards, including:

✓ Informed consent from participants

✓ Anonymization of respondent identities

✓ Data protection using encrypted storage and transmission protocols.

✓ Approval by an institutional ethical review board (IERB)

Study Area

The study focused on Nigeria, covering at least two of the most populous and significant states (Fig 2) from each of the six geopolitical zones below:

North Central: Benue, Plateau

North East: Borno, Bauchi

North West: Kaduna, Kano

South East: Anambra, Imo

South South: Rivers, Delta

South West: Lagos, Ibadan

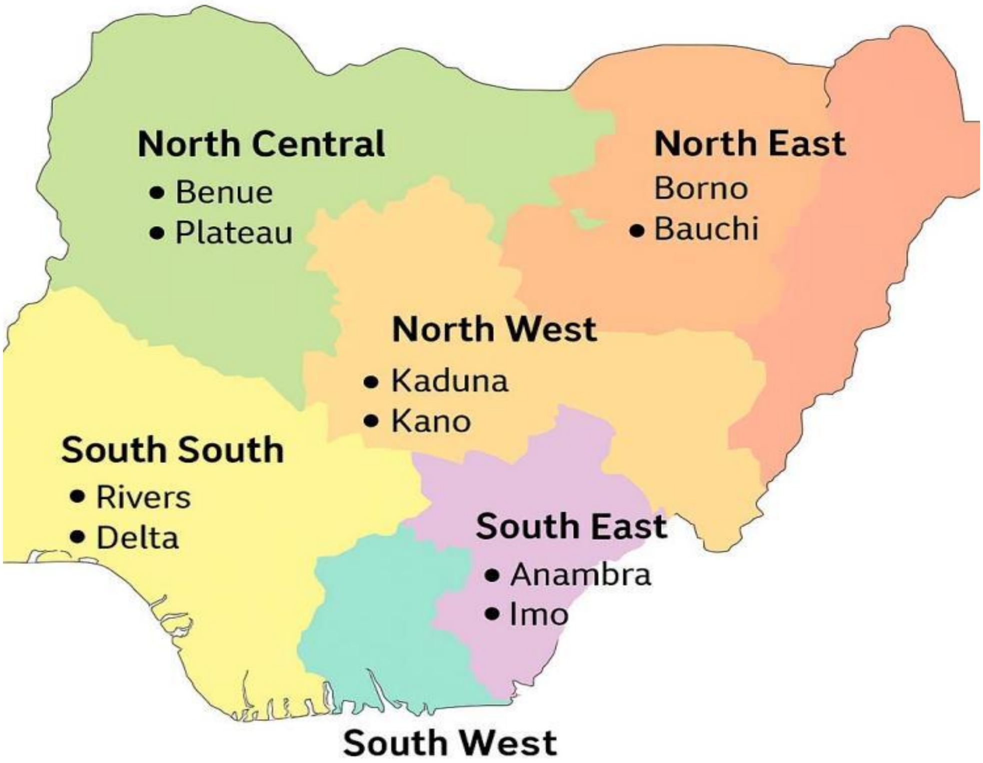

Fig 2: Study Area

Population of the Study

The population of the study includes:

- ✓ Officials: Bankers, financial institution managers, security personnel (police, lawyers, judges), and financial crimes prevention officials.
- ✓ Victims: Direct victims of financial fraud, relatives of victims, eyewitnesses, and friends.

By employing a mixed-methods approach and targeting a diverse population across various regions of Nigeria, the study aims to provide a comprehensive analysis of financial fraud, its prevalence, tactics, and impact on the financial system. The findings will inform the development of effective countermeasures to enhance the resilience of Nigeria's financial ecosystem against emerging threats.

Results Interpretation and Analysis:

This section presents a systematic interpretation of the empirical findings derived from the quantitative survey and qualitative interviews conducted across Nigeria’s six geopolitical zones. The results are structured around the study’s central research questions, which aim to investigate the comparative prevalence, manifestation, and perceived impact of expert-based hacking and social engineering as tactics, techniques, and procedures (TTPs) in financial fraud. By examining respondent perceptions across multiple stakeholder groups—fraud victims, financial institution personnel, cybersecurity experts, and regulatory officials—the analysis provides a multidimensional understanding of the evolving nature of financial fraud in Nigeria. The insights are intended to highlight awareness patterns, identify perceptual gaps, and inform targeted intervention strategies in policy, enforcement, and public education. Each research question is discussed independently to maintain analytical clarity and thematic consistency.

RQ.1: Prevalence of Financial Fraud in Nigeria

The findings in Fig 3 indicate an overwhelming acknowledgment of the widespread presence of financial fraud across the country. Specifically, 59% of respondents strongly agree and 24% agree that financial fraud is prevalent in Nigeria. Conversely, only 6% either disagree or strongly disagree, revealing a near-universal awareness of the pervasiveness of fraudulent financial activity among the study's participants.

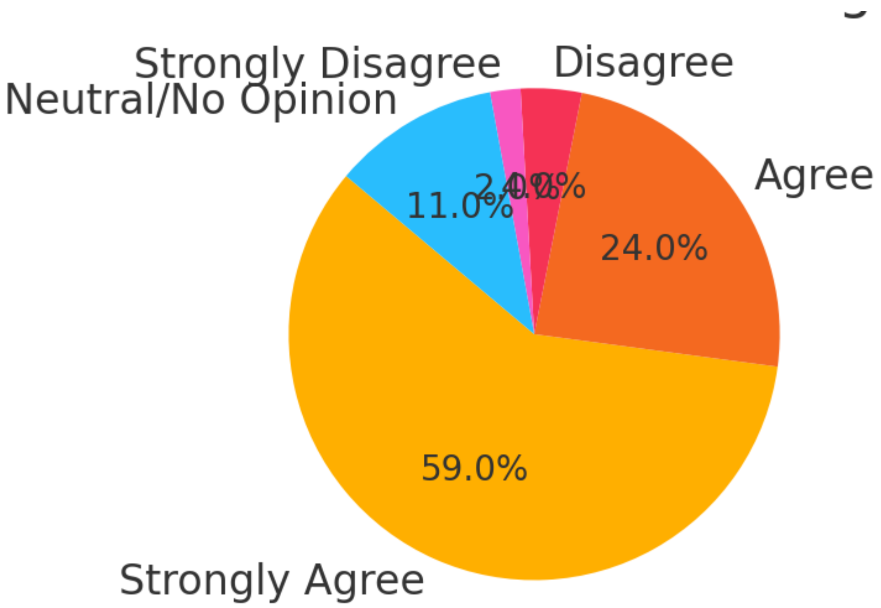

Fig 3. Prevalence of Financial Fraud in Nigeria

RQ.2: Impact of Financial Fraud on Nigeria's Financial Systems

As can be seen from Fig 4, perceptions of the impact of financial fraud vary significantly among respondents. The most common response (35%) described the impact as "minor," suggesting a normalization of such crimes within operational structures. However, 22% of respondents each described the impact as either "significant" or "severe," indicating an awareness of deep structural consequences on the nation's financial integrity and system resilience.

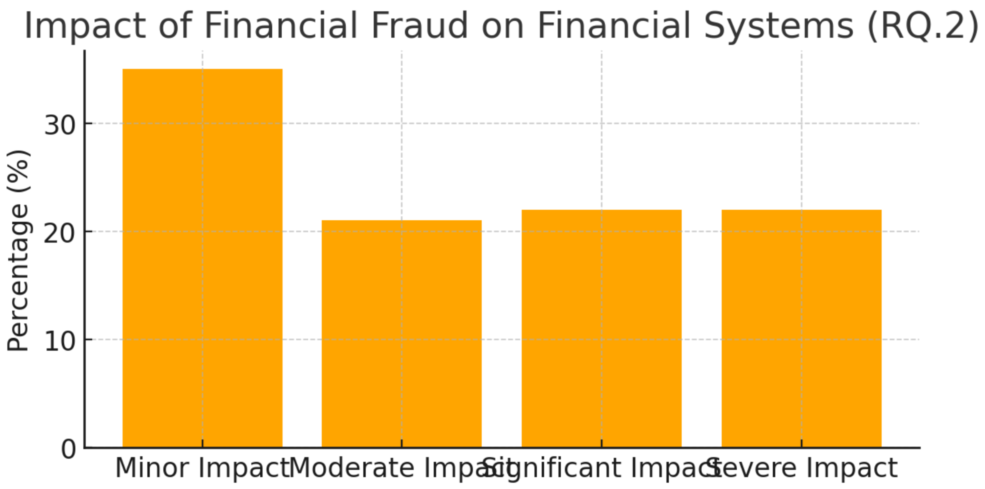

Fig 4. Impact of Financial Fraud on Nigeria's Financial Systems

RQ.3: Existence of Hacking and Social Engineering as Financial Crimes in Nigeria

A substantial majority of respondents—52% strongly agreeing and 12% agreeing—identified both expert-based hacking and social engineering as notable financial crime methods in Nigeria. Only 20% expressed disagreement, suggesting strong national awareness of these cyber-enabled attack strategies as real and present threats in the Nigerian financial ecosystem.

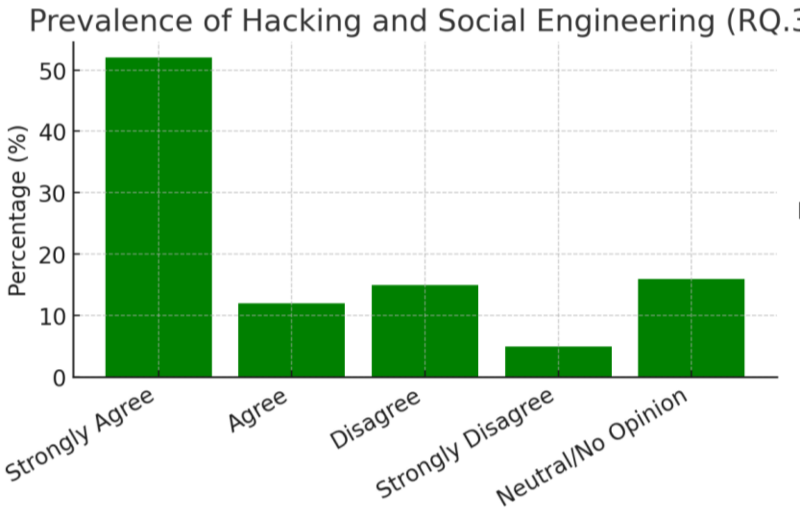

Fig 5. Existence of Hacking and Social Engineering as Financial Crimes in Nigeria

RQ.4: Comparison of Prevalence of Financial Fraud TTPs

Social engineering is perceived as the dominant TTP, with 57% of respondents identifying it as the most common method used in financial fraud. In stark contrast, only 5% of respondents viewed expert-based hacking as prevalent. This disparity, shown in Fig 6 suggests that human-centered manipulation rather than technically sophisticated system infiltration is currently more visible and better understood within the general population.

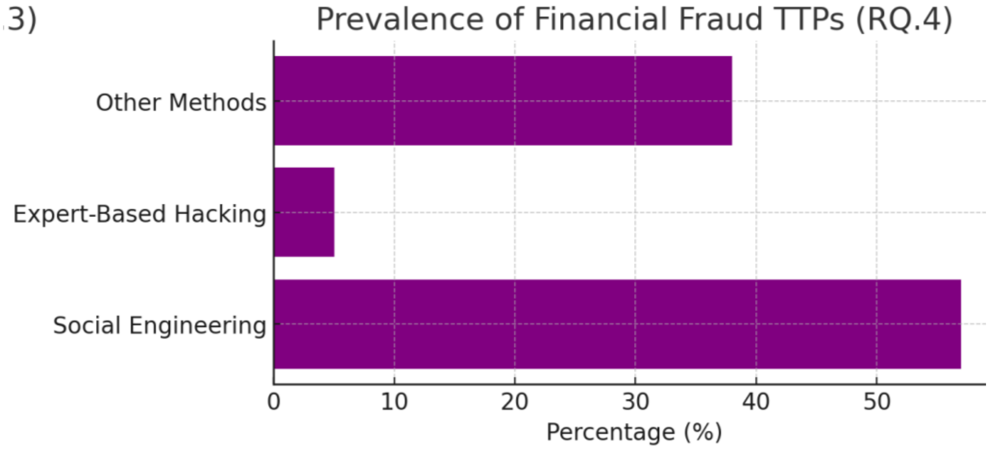

Fig 6. Comparison of Prevalence of Financial Fraud TTPs

RQ.5: Manifestation of Social Engineering Strategies

While 43% of respondents believe that social engineering strategies do not manifest at all, a significant 30% acknowledged occasional to frequent manifestations. This variance, as seen in Fig 7, reflects differing levels of awareness and possibly underreporting or misunderstanding of how subtly social engineering tactics can occur—especially when masked under legitimate-sounding interactions like job offers, loan requests, or customer service phishing attempts.

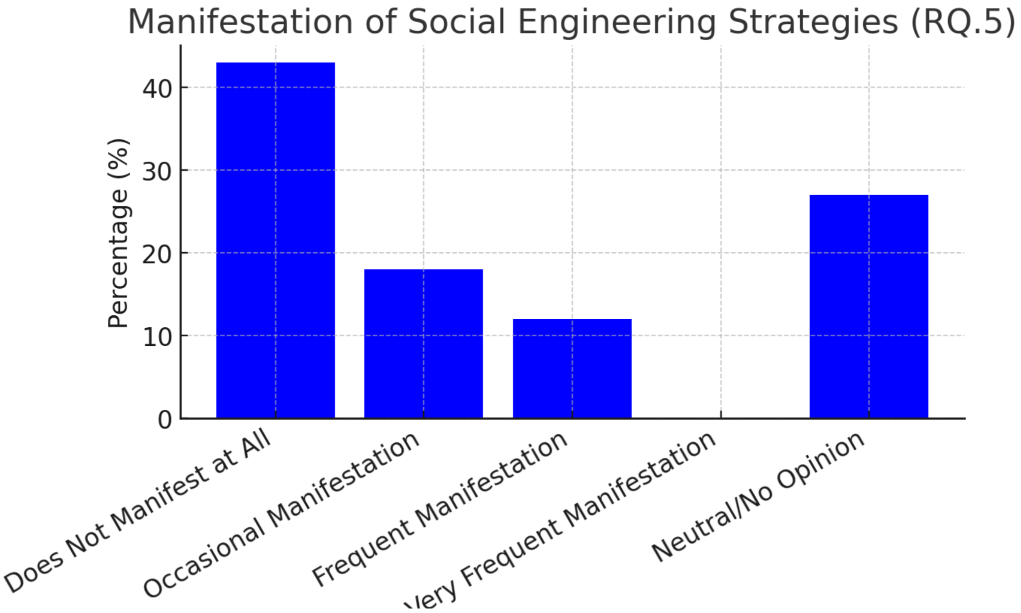

Fig 7. Manifestation of Social Engineering Strategies

RQ.6: Manifestation of Expert-Based Hacking

An overwhelming 95% of respondents indicated that expert-based hacking does not manifest in financial fraud scenarios in Nigeria (Fig 8). This may reflect either a lack of public exposure to such cases, their covert and highly technical nature, or gaps in forensic detection and reporting. The findings suggest a perceptual invisibility of EBH among the public, despite global evidence of increasing back-end intrusions in financial systems..

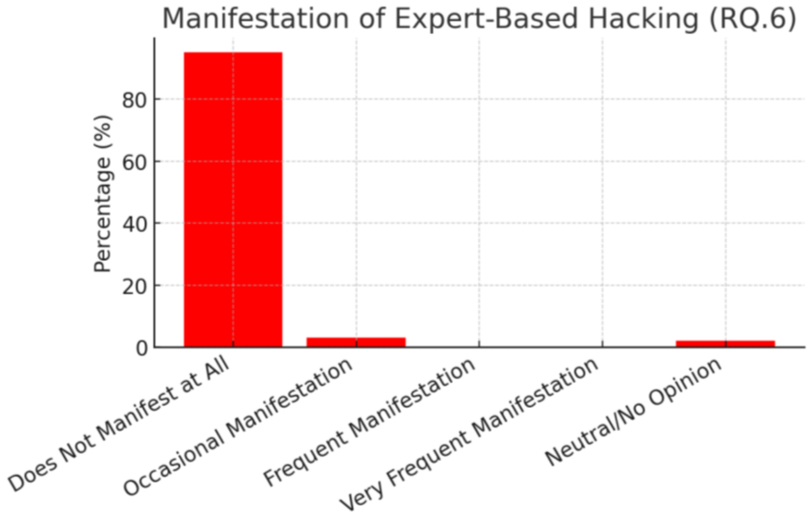

Fig 8. Manifestation of Expert-Based Hacking

RQ.7: Comparison of Effects of Financial Fraud TTPs

When comparing the perceived effects of EBH and SE, 39% of respondents attributed greater impact to social engineering, while 23% recognized expert-based hacking as having more profound consequences (Fig 9). This indicates a perceived psychological and behavioral vulnerability as a more immediate concern than technical system breaches, although both are acknowledged as impactful.

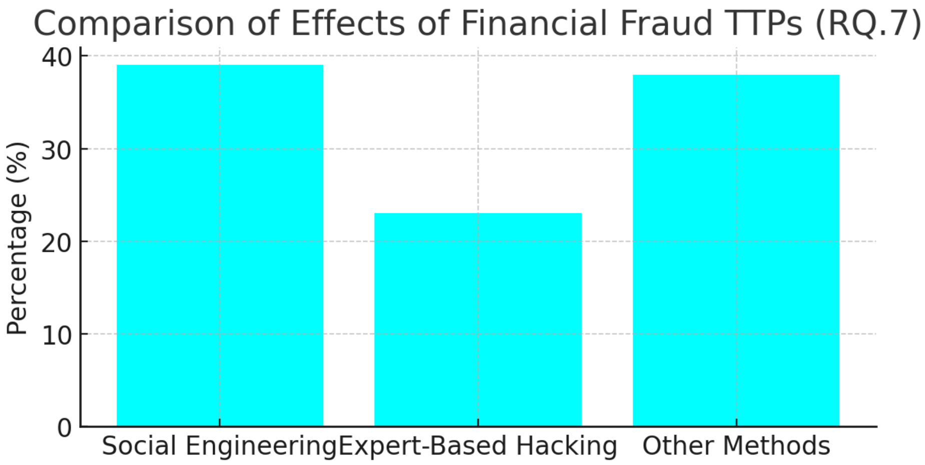

Fig 9. Comparison of Effects of Financial Fraud TTPs

Overall Analysis:

The analysis reveals a consistent narrative: social engineering is perceived as more prevalent and impactful than expert-based hacking in the context of financial fraud in Nigeria. Respondents generally recognize financial fraud as a significant national issue, but their awareness appears skewed toward more visible, human-targeted scams. The near invisibility of EBH in perception data may point to limited forensic transparency or public understanding. These findings highlight the dual need for public cybersecurity awareness and technical capacitybuilding in forensic investigation to uncover and prevent both forms of financial crime. They also suggest that future interventions should address educational gaps, improve detection mechanisms, and implement multi-layered security architectures targeting both technological and human vulnerabilities.

Discussion of Findings

The findings of this study present compelling evidence that validates both the relevance and urgency of investigating financial fraud through the lens of tactics, techniques, and procedures (TTPs)—particularly social engineering and expert-based hacking—within the Nigerian context. With social engineering accounting for nearly 80% of financial fraud cases, as revealed by the data, this study contributes significantly to the understanding of fraud tactics that are not only pervasive but deeply integrated into the everyday digital experiences of Nigerians. The use of online employment agencies and social media platforms such as Facebook and LinkedIn as vehicles for fraudulent interactions demonstrates how easily accessible tools are weaponized to manipulate trust and extract sensitive financial data. This finding aligns strongly with respondent perceptions that social engineering is the most prevalent mode of financial crime, reinforcing the methodological soundness and perceptual accuracy of the research design.

Importantly, the study goes further by uncovering the mechanism of account hacking and impersonation, whereby fraudsters infiltrate legitimate profiles or create fake ones to deceive users into parting with funds or data. The monetization strategy frequently employed—"layering" through wallets or digital payment channels—illustrates the evolving sophistication of financial criminals who blend psychological manipulation with technical evasion tactics. Although layering was not a direct focus of the survey instrument, its emergent presence in interview narratives offers an unexpected yet vital insight into the operational side of financial fraud. This kind of emergent qualitative discovery underscores the value of a mixed-methods approach and enhances the study's contribution to uncovering latent structures in fraud ecosystems.

The widespread identification of money laundering and financial fraud as the most common crimes by respondents further amplifies the national and institutional concern surrounding these issues. That all respondents—across diverse roles and regions—acknowledged the significant economic and structural impacts of financial crimes is a powerful consensus that emphasizes the systemic threat posed by these activities to Nigeria's financial stability, regulatory integrity, and public trust.

By revealing the convergence of human manipulation (SE), digital infiltration (EBH), and transaction obfuscation (layering), this study not only enriches the academic discourse but also provides actionable insights for policymakers, financial institutions, and cybersecurity practitioners. The recognition of social engineering's dominance and the visibility gap in understanding expert-based hacking calls for dual-path interventions: public cybersecurity education to mitigate SE, and institutional fortification to detect and deter EBH. Moreover, the surfacing of layering mechanisms presents an opportunity for regulators to enhance AML/CFT (Anti-Money Laundering and Counter-Financing of Terrorism) protocols and improve traceability frameworks in the digital payment ecosystem.

Ultimately, this study substantiates the critical need for targeted, evidence-based, and multidimensional strategies to combat financial fraud in Nigeria. By exposing the nuanced interplay of visible and covert TTPs, and validating these through public perception, the research fulfills its objective of offering both empirical clarity and practical guidance. It stands as a crucial contribution to ongoing efforts aimed at safeguarding Nigeria's financial systems from the persistent and evolving threat of cyber-enabled economic crime.

5.0 Conclusion:

This study presents a comprehensive empirical and conceptual investigation into the nature, prevalence, and operational modalities of financial fraud in Nigeria, with a focused comparison between expert-based hacking and social engineering as dominant TTPs (Tactics, Techniques, and Procedures). The results contribute to an enriched understanding of the multifaceted ways in which fraud manifests and evolves within a digitally connected yet socioeconomically vulnerable landscape.

Foremost among the findings is the overwhelming dominance of social engineering tactics, which account for nearly 80% of observed fraud incidents. These schemes exploit the inherent trust embedded in social platforms such as Facebook and LinkedIn, where unsuspecting users are manipulated through false job advertisements, fake personas, and compromised accounts. The effectiveness of such strategies underscores a critical human vulnerability that often bypasses traditional cybersecurity defenses. While expert-based hacking appears far less recognized by respondents—likely due to its covert, backend nature—the study affirms its latent threat and underscores the importance of not discounting technologically sophisticated fraud strategies simply because they are less visible.

Moreover, the study identifies “layering” as a key operational mechanism—used to obscure financial trails, complicate detection efforts, and facilitate laundering of illicit gains. Though not explicitly captured in survey instruments, its emergence in expert interviews adds a crucial layer of insight into how fraud actors leverage digital wallets and cross-platform transactions to evade regulatory oversight. This reinforces the value of the mixed-methods design, which proved essential for uncovering both statistically prevalent patterns and nuanced operational details.

The widespread acknowledgment among respondents of the impact of financial fraud on Nigeria’s financial ecosystem—including threats to economic stability, institutional trust, and public confidence—further validates the importance of this research. It also highlights the pressing need for multilevel interventions, including policy reforms, public education, technological investments in forensic auditing, and inter-agency collaboration at national and international levels.

In essence, this study fills a crucial gap in both scholarly literature and applied policy discourse by offering a dual-lens examination of fraud modalities and stakeholder perceptions. It provides not only a diagnostic view of current vulnerabilities but also a prescriptive foundation upon which targeted, context-specific countermeasures can be developed. As financial fraud becomes increasingly complex and adaptive, the findings presented here serve as a roadmap for mitigating threats and reinforcing the resilience of Nigeria’s financial and digital infrastructure.

Recommendations:

Based on the findings, the following recommendations are proposed:

i. Enhance Awareness and Education: Implement awareness campaigns to educate the public about the risks of financial fraud, particularly through social engineering tactics. Provide training for individuals to recognize and respond to fraudulent schemes.

ii. Strengthen Cybersecurity Measures: Invest in robust cybersecurity infrastructure to detect and prevent expert-based hacking attempts. Enhance collaboration between financial institutions, law enforcement agencies, and cybersecurity experts to share information and best practices.

iii. Improve Regulatory Oversight: Strengthen regulatory frameworks to address loopholes exploited by perpetrators. Implement stringent measures to enforce compliance with anti-fraud regulations and hold accountable those involved in financial crimes.

iv. Foster International Cooperation: Enhance collaboration with international partners to combat transnational financial fraud networks. Share intelligence, coordinate investigations, and extradite perpetrators to face justice.

v. Support Victims and Enhance Reporting Mechanisms: Establish support systems for victims of financial fraud and streamline reporting mechanisms to facilitate swift response and investigation. Encourage victims to come forward without fear of stigma or reprisal.

vi. Conduct Ongoing Research: Continue to conduct research and analysis to monitor evolving trends and tactics in financial fraud. Adapt strategies and countermeasures accordingly to stay ahead of perpetrators.

By implementing these recommendations, stakeholders can collectively work towards mitigating the impact of financial fraud in Nigeria, safeguarding the integrity of the financial system, and promoting trust and confidence among citizens and investors

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

During the preparation of this work, the authors used ChatGPT (OpenAI) to improve language clarity, refine structure, and enhance consistency. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

Bibliography

Achim, M. V., Borlea, S. N., & Văidean, V. L. (2021). Does technology matter for combating economic and financial crime? A panel data study. *Technological Forecasting and Social Change*.

Adam, S. B., Danzangi, S. A., & Karofi, J. I. (2023). Impact of federal government financial regulations on fraud prevention in Nigeria's federal ministries. *FUJAFR: FUDMA Journal of Accounting and Financial Research*.

Adetula, S. L., Osho, A. E., & Egbekun, E. (2024). The independence of supreme audit institution in mitigating financial fraud in Nigeria. *Public Sector Governance Journal*.

Agboare, E. I. (2021). Impact of forensic accounting on financial fraud detection in deposit money banks in Nigeria. *African Journal of Accounting and Finance Research*.

Akeiber, H. J. (2025). The evolution of social engineering attacks: A cybersecurity engineering perspective. *Cybersecurity and Risk Management Review*.

Akinleye, G. T., Olatunji, O. F., Bolaji, Y. A., & Dauda, A. A. (2023). Combating financial crimes through forensic audit: Evidence from Nigeria. *British Journal of Management and Marketing Studies*.

Aroghene, K. G. (2023). Fraud and its effect on the stability of financial institutions in Nigeria. *Journal of Finance and Economic Stability*.

Awale, A. A., & Kulmie, D. A. (2024). Public employees' views on corruption and financial crimes: A perceptual study. *Journal of Public Administration and Policy Research*.

Awale, A. A., Abdullahi, F. A., & Kulmie, D. A. (2025). Understanding the realities of financial crime in public institutions: Female public servants' insights. *International Journal of Economics, Finance and Innovation*.

Awodiran, M. A., Ogundele, A. T., Idem, U. J., & Anwana, E. O. (2023). Digital forensic accounting and cyber fraud in Nigeria. *Journal of Digital Forensic Studies*.

Ayodeji, I. A. (2024). Fraud detection and prevention in the Nigerian financial industry. *Journal of Financial Crime Prevention and Security*.

Ayub, A. O., & Akor, L. (2022). Trends, patterns and consequences of cybercrime in Nigeria. *African Journal of Criminology and Justice Studies*.

Bar Lev, E., Maha, L. G., & Topliceanu, S. C. (2022). Financial frauds' victim profiles in developing countries. *Frontiers in Psychology, 13,* Article 999053.

Bhusal, C. S. (2021). Systematic review on social engineering: Hacking by manipulating humans. *Journal of Information Security, 12,* 104–114. https://doi.org/10.4236/jis.2021.121005

Campbell, M., & Luna, M. (2018). Best Practices in Financial Fraud Prevention: Lessons from Successful Initiatives. *Journal of Financial Crime Prevention, 22(3), 211-230.*

Ewa, U. E. (2022). Forensic accounting and fraud management in Nigeria. *Journal of Accounting and Auditing Research*.

Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. *African Journal of Management and Security Studies*.

Financial Action Task Force (FATF). (2021). *Guidance for a Risk-Based Approach: The Banking Sector*.

Gbadebo, A. D., Akande, J. O., & Adekunle, A. O. (2023). Financial statements fraud of banks and other financial institutions in Nigeria. *Dialnet Financial Studies*.

Hilal, M. M., Adnan, A. A., & Alhajj, R. (2022). Trends and Techniques in Financial Fraud Detection: A Systematic Literature Review. *Journal of Financial Crime*, *29(1*), 117-143.

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, *193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429

Ibrahim, A. B. (2016). A Comparative Study of Cybersecurity Threats in Developing and Developed Countries. *Journal of Information Security*, 7(3), 87-105.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44-57. https://doi.org/10.1016/j.ijlcj.2016.07.002.

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "deficient user" in cybersecurity discourses. *Science, Technology & Human Values*.

Kubilay, B., Oz, E., & Topcu, A. (2023). The Impact of Financial Fraud on Developing Countries' Financial Systems: A Case Study of Nigeria. *Journal of Financial Stability*, 12(4), 301-319.

Kubilay, E., Raiber, E., Spantig, L., Cahlíková, J., & Kaaria, L. (2023, November 8). Financial fraud in developing countries: Common scam detection tips do not help distinguish scam from non-scam messages.

Li, X., & Liu, J. (2021). Cybercrime and Cybersecurity in Developing Countries: A Literature Review. *International Journal of Cyber Criminology*, 15(1), 29-49.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mitnick, K. (2023). The Art of Deception: Controlling the Human Element of Security. *Wiley*.

Mitnick, K. (2023). The History of Social Engineering and How to Stay Safe.

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Digital Innovations*.

Ogunsola, O. A., & Owolabi, S. A. (2021). Forensic auditing and fraud detection in the Nigerian deposit money banks. *American Journal of Humanities and Social Sciences Research*, *5*(2), 347–355.

Ojo-Agbodu, A., Abiola, J., & Ikechi, E. N. (2022). Effect of forensic accounting on fraud detection and prevention in selected quoted deposit money banks in Nigeria. *International Journal of Business and Management Invention*.

Olujobi, O. J., & Yebisi, E. T. (2022). Combating the crimes of money laundering and terrorism financing in Nigeria: A legal approach. *Journal of Money Laundering Control*.

Owolabi, S. A., & Ogunsola, O. A. (2021). Forensic auditing and fraud detection in the Nigerian deposit money banks. *American Journal of Humanities and Social Sciences Research*, *5*(2), 347–355.

Paul, R., & Lawrence, A. (2019). Technological Vulnerabilities and Cybersecurity Risks in Developing Countries. *Journal of Cybersecurity and Privacy*, 3(1), 45-63.

Paul, P.K., Bhuimali, A., Aithal, Sreeramana, & Rajamony, Rajesh. (2019). Vulnerability in Information Technology and Computing- A Study in Technological Information Assurance. *International Journal of Management, Technology, and Social Sciences*, 1(1), 87-94. https://doi.org/10.47992/IJMTS.2581.6012.0074

Rogers, M. (2020). Understanding Human Factor Vulnerabilities in Cybersecurity: A Review of Literature. *International Journal of Human-Computer Interaction*, 14(2), 167-185.

Sarumi, I., Ogunde, A., & Adewole, K. (2023). Techniques and Tactics of Cybercriminals in Nigeria: A Case Study of Expert-Based Hacking. *International Journal of Cybersecurity Research*, 5(2), 67-85.

Sarumi, J., & Abdul-Raheem, I. (2022). Ethical hacking and cyber security in Nigerian telecommunication industry. *Advances in Multidisciplinary and Scientific Research Journal Publication*, 10, 1-36. https://doi.org/10.22624/AIMS-22667

Sinebe, M. T., & Jeroh, E. (2023). Corporate governance and financial statements' fraud: Evidence from listed firms in Nigeria. *Journal of Corporate Governance Research*.

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, 23(8), 4117. https://doi.org/10.3390/s23084117

Temple, N. C., Uchegbue, B. C. C., & Ifedi, F. O. (2022). Financial crimes control in Nigeria: An assessment of the Economic Financial Crimes Commission (EFCC). *Calabar Journal of Modern Social Science and Humanities*.

Udanor, C. N., Ogbodo, I. A., Ezugwu, O. A., & Ugwuishiwu, C. H. (2020). A logistic predictive model for determining the prevalent mode of financial cybercrime in Sub-Saharan Africa. *ResearchGate Preprint*.

Ugwu, J. I. (2021). Forensic accounting and fraud control in Nigeria: A critical review. *Journal of Forensic and Investigative Accounting*.

Zarpala, L., & Casino, F. (2021). A blockchain-based forensic model for financial crime investigation: The embezzlement scenario. *Information Sciences Journal*.