



The Impact of AI-Powered Audit Tools on Audit Quality and Fraud Detection in Nigerian Deposit Money Banks

Tonye Ogiriki¹, Joseph Inini*

Department of Accounting, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria.

Abstract

Keywords

Artificial Intelligence, AI-Powered Audit Tools, Audit Quality, Fraud Detection, Deposit Money Banks, Machine Learning

This study examined the impact of AI-powered audit tools on audit quality and fraud detection in Nigerian deposit money banks (DMBs) between 2015 and 2024, combining a structured literature review of thirty empirical studies with a case-based analysis of seven purposively selected Tier-1 banks, Access Holdings, GTCO, Zenith Bank, UBA, Stanbic IBTC, FCMB and Wema Bank, for which technology-investment and fraud-loss figures are individually disclosed in audited financial statements for 2023-2024. Correlation and regression analyses were run on the four banks with matched data, alongside trend analysis of sector-wide fraud data from NDIC, NIBSS and FITC. The findings show that AI-powered audit tools, particularly data mining and image recognition, show a significant positive association with audit quality in several of the reviewed studies. In contrast, machine learning applications show a weaker, less consistent link at the firm level. The bank-level analysis found a negative, though not statistically significant given the small sample, relationship between technology investment and the percentage change in fraud loss (Pearson $r = -0.39$, $n = 4$). In contrast, an exploratory sensitivity analysis excluding Zenith Bank produced a much stronger correlation ($r = -0.97$, $n = 3$), a result treated as indicative only given the three observations. The evidence suggests that heavier technology investment is associated with smaller increases in fraud loss in some banks, but not universally. The study concludes that AI-powered audit tools hold real promise for Nigerian DMBs, but remain constrained by data quality, infrastructure, skills, timing lags, and regulatory gaps. Recommendations are made for deliberate investment in data infrastructure, staff training, and phased regulatory guidance.

1. Introduction

Deposit money banks occupy a central place in the Nigerian economy, moving savings from individuals and firms with surplus funds to households and businesses that need credit, while processing millions of transactions daily across branches, ATMs, mobile and internet banking platforms (Central Bank of Nigeria {CBN}, 2023). This scale of activity, built up rapidly since the mid-2010s on the back of financial inclusion and digital banking policies, has made the sector both a major driver of growth and a major target for fraud (NIBSS, 2024). The traditional audit, built around manual sampling and after-the-fact review, has struggled to keep pace with the volume and complexity of modern banking data (Kokina & Davenport, 2017).

To close this gap, banks, audit firms, and regulators in Nigeria have, since around 2015, begun exploring artificial Intelligence (AI) as a tool for strengthening the audit process. AI-powered audit tools, including data mining, machine learning, robotic process automation, and image recognition, allow auditors to examine entire populations of transactions rather than small samples, flagging unusual patterns in real time (Han, Huang, Liu, & Towey, 2020; Craja, Kim, & Lessmann, 2020). Internationally, these tools have been credited

* Corresponding Author: Joseph Inini

Email Address: ininijoe@yahoo.com

¹ Professor of Accounting, Niger Delta University

with improving audit quality by widening coverage and detection accuracy, and freeing auditors for judgement-intensive work (Kokina & Davenport, 2017; Alles, 2015).

In Nigeria, however, the adoption of these tools has been slower and less even than in more developed markets, reflecting infrastructure gaps, data quality problems, and a shortage of auditors with the technical skills to build and interpret AI-based models (Ajayi & Akinrinola, 2023). At the same time, the fraud problem the tools are meant to address has continued to grow. The Nigeria Deposit Insurance Corporation reported that fraud-related actual losses in the industry fell from ₦3.17 billion in 2015 to ₦2.40 billion in 2016 (NDIC, 2017), before rising again in later years, and the Nigeria Inter-Bank Settlement System recorded 95,620 fraud cases across Nigerian financial institutions in 2023 alone, with deposit money banks accounting for 92 percent of these cases (NIBSS, 2024). Other industry sources put total fraud losses in the sector at over ₦52 billion in 2024, underlining how fast the problem has grown even as AI-powered tools have become more available (CreedTec, 2025).

This apparent contradiction, growing investment in AI-powered audit and fraud-detection tools alongside growing fraud losses, is the puzzle this study sets out to examine. It matters not just for bank shareholders, but for depositors and regulators, since a banking system that cannot reliably detect fraud finds it harder to retain the deposits and confidence on which its intermediation role depends.

Part of the reason the fraud problem has grown alongside AI adoption lies in the changing shape of Nigerian banking itself. The rollout of the cashless policy from 2014, BVN registration, and the rapid growth of mobile and agent banking have moved an ever-larger share of transactions onto electronic channels, and it is precisely these channels that have recorded the fastest-growing fraud attacks over the period (Tade, 2022); AI-powered tools have, in effect, been chasing a moving and expanding target. The ten-year window covered by this study, 2015 to 2024, captures the full arc of AI adoption in Nigerian banking audit practice, from the earliest pilots to more structured recent deployments, positioning the study to offer an evidence-based picture of whether AI-powered audit tools are translating into better audit quality and fraud detection, or whether adoption so far has been more symbolic than substantive.

The literature on AI and auditing in Nigeria presents a mixed and sometimes contradictory picture. Some studies report that AI tools such as data mining and image recognition have a significant positive relationship with audit quality (Ukpong, Udoh, & Essien, 2019), while others find that the actual, on-the-ground benefit of AI to internal audit in commercial banks remains low, held back by the absence of dedicated AI units and by poor data integrity (Ajayi & Akinrinola, 2023). Similarly, while experimental studies report machine learning fraud-detection models with accuracy rates above 90 percent (Awoyemi, Adetunmbi, & Oluwadare, 2017; Njoku, Iwuchukwu, Jibiri, Ikwuazom, Ofoegbu, & Nwokoma, 2024), industry-wide fraud statistics for the same period show fraud cases and losses rising rather than falling (NIBSS, 2024; FITC, 2023).

A further gap is that many existing Nigerian studies examine either audit quality or fraud detection in isolation, often within a single bank or short survey window, making it difficult to draw a coherent, sector-wide picture. This study addresses this gap by reviewing empirical evidence on both outcomes across the full decade from 2015 to 2024 and placing bank- and firm-level findings alongside sector-wide fraud statistics from NDIC, NIBSS and FITC.

The aim of this study is to examine the impact of AI-powered audit tools on audit quality and fraud detection in Nigerian deposit money banks between 2015 and 2024. The specific objectives are to:

- 1) examine the effect of AI-powered audit tools on the audit quality of deposit money banks in Nigeria;
- 2) examine the effect of AI-powered audit tools on the fraud detection capability of deposit money banks in Nigeria;
- 3) examine the relationship between technology/AI-related investment and fraud outcomes among a purposively selected sample of named Nigerian deposit money banks;
- 4) analyse the trend in reported fraud cases and losses in the Nigerian banking industry over the period under review; and
- 5) identify the challenges limiting the adoption of AI-powered audit tools in Nigerian deposit money banks.

2. Literature Review

2.1 Conceptual Overview

a. Artificial Intelligence and AI-Powered Audit Tools

Artificial Intelligence refers to computer systems built to perform tasks that would normally require human Intelligence, including learning from data, recognising patterns, and making judgements under uncertainty (Kokina & Davenport, 2017). AI-powered audit tools apply these capabilities to the audit process, using techniques such as data mining, machine learning, robotic process automation, natural language processing and image recognition to test entire populations of transactions, flag anomalies, and support the auditor's judgement (Han, Huang, Liu, & Towey, 2020). Kokina and Davenport (2017) describe this shift as moving auditing from a sample-based, backward-looking exercise to a continuous, forward-looking one, in which the auditor increasingly works alongside, rather than instead of, intelligent systems.

b. Audit Quality

Audit quality is commonly defined, following DeAngelo (1981), as the joint probability that an auditor will both detect and report a material misstatement, tying audit quality directly to technical competence and independence. In the Nigerian banking context, audit quality is reflected in the accuracy and completeness of the audit, the breadth of transactions examined, the speed with which anomalies are flagged, and the confidence regulators, shareholders and depositors place in audited financial statements (Aderibigbe, Tonade, Fadairo, & Edun, 2024).

c. Fraud and Fraud Detection

Fraud is an intentional act involving deception to obtain an unjust or illegal advantage (Cressey, 1953). Fraud detection refers to the process, and increasingly the technology, used to identify fraudulent transactions as early and accurately as possible (Eneh, Okeke, & Amahalu, 2023). In Nigerian DMBs, common fraud types include fraudulent transfers, unauthorised loans, cheque forgery, card-related fraud, and, increasingly, mobile and internet banking fraud (NIBSS, 2024).

d. Deposit Money Banks

Deposit money banks are financial institutions licensed by the Central Bank of Nigeria to accept deposits from the public and to create credit through loans and advances (CBN, 2023). They are the institutions primarily affected by, and primarily investing in, AI-powered audit and fraud-detection tools in Nigeria, given the scale of their transaction volumes and their exposure to both internal and external fraud.

e. Machine Learning, Data Mining and Big Data Analytics

Machine learning is a branch of AI in which a computer system learns to recognise patterns from historical data and applies what it has learned to new, unseen data, without being explicitly programmed for every rule (Craja, Kim, & Lessmann, 2020). Data mining and big data analytics extend this by extracting useful patterns from large, often unstructured datasets, allowing auditors to examine transaction logs and system records at a scale beyond manual procedures (Alles, 2015). In auditing, these techniques build models, such as logistic regression, random forests, support vector machines, and neural networks, that classify transactions as likely fraudulent or legitimate with a stated level of accuracy (Awoyemi, Adetunmbi, & Oluwadare, 2017; Mohammed, Wajiga, & Saidu, 2024).

f. Continuous Auditing and Robotic Process Automation

Continuous auditing is an approach in which audit evidence is gathered and analysed on an ongoing, near real-time basis rather than periodically, allowing auditors and internal control functions to respond to risk as it arises (Alles, 2015). Robotic process automation (RPA) complements continuous auditing by automating repetitive, rule-based audit tasks, such as reconciliations and confirmations, freeing auditors to concentrate on higher-risk, judgement-based areas (Kokina & Davenport, 2017).

g. Forensic Accounting

Forensic accounting combines accounting, auditing, and investigative skills to examine financial records for evidence of fraud, often for use in legal or disciplinary proceedings (Kamble & Devarmani, 2024). Traditionally reactive and labour-intensive, it is increasingly supported by AI tools that flag suspicious patterns far more quickly than manual review.

h. Regulatory Technology and Supervisory Technology

Regulatory technology (RegTech) and supervisory technology (SupTech) refer to the use of AI and related digital tools by regulated institutions to meet compliance obligations, and by regulators to monitor them, respectively (Arner, Barberis, & Buckley, 2017). For Nigerian banks, RegTech overlaps closely with AI-powered audit tools, since both draw on the same data mining and machine-learning capabilities; this raises new supervisory questions, since regulators must increasingly understand and validate the AI models banks use for fraud detection and audit judgement (Arner, Barberis, & Buckley, 2017).

2.2 Theoretical Premise

This study is anchored on five complementary theories: the Technology Acceptance Model, agency theory, the fraud triangle theory, diffusion of innovation theory, and institutional theory. Each plays a distinct role. Agency theory and the fraud triangle theory explain why audit and fraud detection matter and how AI-powered tools are expected to act on the information gap and on the opportunity for fraud, respectively. The Technology Acceptance Model, diffusion of innovation theory, and institutional theory explain adoption: individual-level acceptance of the tools, the pace at which adoption spreads across banks, and the organisational motives behind adoption, respectively. The Technology Acceptance Model, developed by Davis (1989), holds that an individual's willingness to adopt and use a new technology is shaped mainly by two beliefs: perceived usefulness, the extent to which the technology is believed to improve job performance, and perceived ease of use, the extent to which the technology is believed to be simple to use. Applied to AI-powered audit tools, the model suggests that Nigerian auditors and bank examiners will adopt these tools more readily and use them more effectively where they are seen as genuinely improving audit outcomes and are not overly difficult to learn and operate, a proposition consistent with the finding that the absence of a dedicated AI unit and poor data integrity have slowed adoption in Nigerian banks (Ajayi & Akinrinola, 2023).

Agency theory, associated with Jensen and Meckling (1976), explains the audit function as a mechanism for reducing the conflict of interest that arises when a bank's owners delegate its running to managers and staff whose interests may not always align with theirs. Because managers have more information about daily operations than owners do, this gap can be exploited through fraud or misreporting. AI-powered audit tools, by widening the scope and speed of monitoring, are expected to narrow this gap, strengthening both audit quality and fraud detection.

The fraud triangle theory, first proposed by Cressey (1953), holds that fraud occurs where three conditions come together: pressure (a financial or other motive), opportunity (a weakness in controls that allows the fraud to be carried out undetected), and rationalisation (a justification the offender uses to excuse the act). AI-powered fraud detection tools are best understood as working mainly on the opportunity leg of this triangle, reducing the window in which a fraudulent transaction can go unnoticed by widening monitoring coverage and shortening the time between the act and its detection (Eneh, Okeke, & Amahalu, 2023).

Diffusion of innovation theory, developed by Rogers (2003), describes how a new technology spreads through a population of adopters over time, from innovators and early adopters through to a majority and, eventually, laggards. This helps explain why larger, better-resourced Nigerian banks have moved further and faster in deploying AI-powered tools, for example through staff-training programmes reported by at least one major bank since 2022, while smaller banks remain closer to the laggard end of the curve.

Institutional theory adds a complementary layer by explaining why banks facing similar fraud pressures may still adopt AI-powered audit tools at different speeds. It holds that organisations often adopt new practices partly to conform to regulatory and peer expectations, a process known as institutional isomorphism. Applied to Nigerian banking, this suggests some banks may adopt AI tools partly to signal legitimacy before the tools are fully embedded into practice, which helps explain why disclosure of AI use can outpace the depth of actual implementation (AJEMS, 2026).

Taken together, these five theoretical positions converge on a broadly consistent expectation: that AI-powered audit tools, where genuinely adopted and well used, should narrow the information gap between bank management and other stakeholders, reduce the opportunity for fraud to go undetected, and, over time, improve audit quality; but that the pace and depth of this improvement will depend heavily on how readily individual banks and audit teams accept, learn, and embed the new tools into everyday practice, a caution that is directly relevant to interpreting the mixed empirical picture reviewed in the next section.

2.3 Empirical Literature and Hypotheses Development

AI-Powered Audit Tools and Audit Quality

A growing number of Nigerian studies have examined the relationship between AI and audit quality, with generally encouraging but not uniformly strong results. Ukpong, Udoh, and Essien (2019), reviewing the application of AI to banking, accounting, and auditing in Nigeria, found that data mining and image recognition were significantly and positively associated with the quality of audit practice among the accounting professionals and bank executives surveyed, although machine learning applications used in isolation showed a weaker, less consistent link with audit outcomes. This finding suggests that not all AI techniques contribute equally to audit quality, and that the way a tool is implemented may matter as much as the tool itself.

Aderibigbe, Tonade, Fadaïro, and Edun (2024) found that AI meaningfully supports the judgement auditors bring to complex, high-risk areas of the audit, complementing Ajayi and Akinrinola's (2023) survey of 121 bank employees, which found, at the 95 percent confidence level, that AI has aided internal audit through real-time detection, wider coverage, improved accuracy, and efficiency, even though overall benefit remained at a low level, held back by the absence of dedicated AI departments and weaknesses in data integrity, with over 86 percent of banks expecting these limitations to persist.

A related strand examines digital audit tools more broadly. A study in the African Journal of Management and Business Research examined digital audit tools and audit quality in Nigerian DMBs, situating its findings within the wider view, drawn from Arner, Barberis, and Buckley (2017), that fintech growth brings both efficiency gains and new regulatory risks (AJMBR, 2026). This is echoed by a study of AI disclosure published in the African Journal of Economic and Management Studies, which analysed twelve DMBs' annual reports from 2015 to 2024 and found voluntary AI disclosure functions as a governance signal in a market with no formal AI disclosure regulation (AJEMS, 2026), suggesting banks disclosing more about AI use tend to be further along in genuinely embedding AI-based controls. On this basis, the study proposes that:

H₀₁: AI-powered audit tools have no significant effect on the audit quality of deposit money banks in Nigeria.

AI-Powered Audit Tools and Fraud Detection

A separate but related body of literature examines how well AI and machine learning tools detect fraud in Nigerian financial data. Awoyemi, Adetunmbi, and Oluwadare (2017) compared several machine learning techniques for credit card fraud detection and found that model choice mattered a great deal for accuracy. Njoku, Iwuchukwu, Jibiri, Ikwuazom, Ofoegbu, and Nwokoma (2024) developed a machine learning-based web application for detecting fraud in Nigerian financial institutions, achieving high accuracy in identifying fraudulent transactions, while stressing that such applications need to be integrated with existing fraud-prevention frameworks rather than operated as stand-alone tools.

Comparative experimental studies frequently cited in the Nigerian literature report very high classification accuracy for some algorithms; support vector machine models have been reported to achieve accuracy above 99 percent on card-transaction datasets, with artificial neural networks and hidden Markov models also achieving accuracy above 94 percent. A study focused on the Nigerian financial sector compared unsupervised anomaly-detection techniques, including autoencoders and principal component analysis, confirming that Nigerian transaction data contains detectable anomaly patterns even without labelled fraud examples (arXiv, 2024).

Eneh, Okeke, and Amahalu (2023) found a significant positive relationship between AI adoption and fraud detection capability among deposit money banks in Awka-South, Anambra State. Mohammed, Wajiga, and Saidu (2024), using logistic regression and random forest models on Nigerian bank statement data, found that random forest consistently outperformed logistic regression, particularly once data-imbalance problems were addressed using resampling techniques.

Beyond banking narrowly defined, a review of forensic investigation and AI applications in Nigeria found machine learning and data analytics tools particularly effective at detecting financial anomalies, scalable across banking, insurance and public finance where technical expertise and infrastructure constraints are

addressed (JIATIS, 2025). A 2025 review of AI's role in cybersecurity and fraud detection reported that NIBSS recorded around ₦2.5 billion in fraud-related losses in 2022, roughly 70 percent tied to digital channels, and noted that one major Nigerian bank had, since 2022, trained several hundred data analysts as part of its response.

Set against this encouraging technical picture, however, sector-wide statistics tell a more cautionary story. NDIC reported that fraud, forgery and staff-related theft losses fell by over 48 percent between 2015 and 2016, from ₦18.02 billion in reported cases to ₦8.68 billion, with actual losses falling by 24 percent (NDIC, 2017); yet later in the review period, the picture reversed. Kanu et al. (2022), analysing NDIC crime reports, found fraud and forgery cases rose by about 40 percent between 2018 and 2019, and a further 190 percent between 2019 and 2020, while FITC reported that Nigerian banks lost ₦9.75 billion to fraud in the second quarter of 2023 alone, a 277 percent increase over Q1, with fraudulent loans accounting for over 94 percent of that loss (FITC, 2023). NIBSS later reported 95,620 total fraud cases across Nigerian financial institutions for 2023, of which DMBs accounted for 92 percent (NIBSS, 2024), and industry reports place total fraud losses for 2024 at over ₦52 billion (CreedTec, 2025). This rising trend, occurring in the same years AI-powered fraud detection tools were becoming more widely available, is central to the puzzle this study investigates.

Two further studies help explain why fraud kept rising even as detection technology improved. Tade (2022), analysing NDIC data from 2015 to 2019, found fraud attacks increased year on year, with ATM and internet-based transactions experiencing the highest incidence, and staff across all cadres, particularly temporary and casual staff, implicated in a significant share of cases. Odukoya and Samsudin (2021) found that the competence of internal control staff to prevent and detect fraud is itself a critical factor in how effectively any detection technology, AI-based or otherwise, is actually put to use. Both studies reinforce that AI-powered fraud-detection tools operate within a wider system of staff behaviour and internal control quality that can blunt their sector-wide impact even where the technology performs well in isolation. On this basis, the study proposes that:

H₀₂: AI-powered audit tools have no significant relationship with fraud detection in deposit money banks in Nigeria.

H₀₃: There is no significant relationship between technology/AI-related investment and fraud outcomes among named Nigerian deposit money banks.

3.0 Research Methodology

This study combined two complementary approaches: a desk-based review of empirical literature, and a case-based, bank-level analysis of individually disclosed technology-investment and fraud-loss data. The first approach was a structured (integrative) literature review of empirical studies on AI-powered audit tools, audit quality, and fraud detection, focused on, or directly relevant to, Nigerian deposit money banks and audit practice. The search covered studies published from 2015 up to 2025 using Google Scholar, ResearchGate, ScienceDirect, and Nigerian academic repositories such as the African Journals Online (AJOL) platform, with keyword combinations such as "artificial intelligence", "machine learning", "data mining", "audit quality", "fraud detection", "deposit money banks", and "Nigeria". Studies were included where they (i) were empirical (survey, experimental, archival, or content-analysis studies) or empirical reviews; (ii) examined AI, machine learning, data mining, or related digital audit technologies in relation to audit quality or fraud detection; and (iii) were set in a Nigerian banking or accounting-firm setting or were directly relevant to it. Studies were excluded where they were purely conceptual or opinion pieces, had no link to audit quality or fraud detection, were unrelated to the Nigerian context, or were duplicates of studies already retained. Thirty studies meeting these criteria were retained for detailed review. Because no formal review protocol, reporting framework (such as PRISMA), or quality-appraisal instrument was applied, the exercise is described as a structured literature review rather than a systematic review. The empirical trend and bank-level analyses cover 2015 to 2024; complete 2025 fraud data were not yet available from NDIC, NIBSS, and FITC at the time of writing, so 2025 is not empirically analysed.

The second source of evidence was a trend analysis of secondary fraud statistics for the Nigerian banking industry as a whole, drawn from the published reports of the Nigeria Deposit Insurance Corporation (NDIC), the Nigeria Inter-Bank Settlement System (NIBSS), and the Financial Institutions Training Centre (FITC), the three bodies that routinely collect and publish fraud data for the industry under statutory reporting requirements set out in the NDIC Act.

Sample of Banks

For a closer, bank-level test, a purposive sample of seven Tier-1 Nigerian DMBs was selected: Access Holdings, GTCO, Zenith Bank, UBA, Stanbic IBTC, FCMB, and Wema Bank, being among the small number of banks for which individually audited technology-investment and fraud-loss figures were both traceable for the 2023 and 2024 financial years, based on their audited financial statements as reported by Nairametrics, TechCabal, Legit.ng, Independent Newspaper Nigeria, and Businessfront/Finance in Africa. This reflects a genuine constraint of current disclosure practice: no regulation yet compels banks to publish a standardised AI-adoption metric, so each bank's own audited technology and cybersecurity investment figure was used as the closest available proxy. Of the seven, four- Access Holdings, GTCO, Zenith Bank, and UBA- had both a 2024 technology-investment figure and matched fraud-loss figures for 2023 and 2024, and were used for the correlation and regression analysis in section four; the remaining three are reported for descriptive comparison only.

The variables examined in this study, and how they were captured from the reviewed literature, bank disclosures, and industry reports, are summarised in Table 1.

Table 1: Variables, Measurement and Sources

Variable	Measurement/Description	Source
AI-Powered Audit Tools (sector-wide)	Reported adoption and use of data mining, machine learning, robotic process automation, and related digital tools in audit and fraud-control functions of Nigerian DMBs and audit firms	Synthesised from reviewed studies, 2015-2025
Technology Investment (bank-level proxy)	Audited technology and cybersecurity/electronic-business investment disclosed by each sample bank for FY2024 (₦ billion)	Individual bank audited financial statements, as reported by Legit.ng/Daily Trust (2025) and TechCabal (2025)
Audit Quality	Reported measures of detection accuracy, audit coverage, and audit judgement quality associated with AI tool use	Aderibigbe et al. (2024); DeAngelo (1981)
Fraud Detection (sector-wide)	Reported fraud case numbers, values, and model accuracy rates for Nigerian deposit money banks	NDIC (2017, 2022); NIBSS (2024); FITC (2023)
Fraud Loss (bank-level)	Percentage change in each sample bank's audited actual fraud/forgery loss, FY2023 to FY2024	Individual bank audited financial statements, as reported by Business front/Finance in Africa (2025) and Markets Reporters (2025)

Source: Compiled by the researcher, 2026.

Content analysis was used to summarise and compare the findings of the thirty reviewed studies. In contrast, descriptive trend analysis, using year-on-year percentage changes, was used to examine the pattern of reported fraud cases and losses across the Nigerian banking industry. For the four-bank matched sample, Pearson and Spearman correlation and simple linear regression were computed between each bank's FY2024 technology investment and the percentage change in its fraud loss from FY2023 to FY2024, using standard statistical procedures; given the small sample size, these results are reported and interpreted as indicative rather than conclusive, and are read alongside, not instead of, the wider literature and sector-level trend evidence.

4.0 Data Analyses and Hypotheses Tests

Research Question Three: What is the relationship between technology/AI-related investment and fraud outcomes in named Nigerian deposit money banks?

Table 2: Profile of Sample Banks — Technology Investment and Fraud Loss, FY2023-FY2024

Bank	FY2024 Technology Investment (₦bn)	Fraud Loss FY2023 (as disclosed)	Fraud Loss FY2024 (as disclosed)	% Change in Fraud Loss
Access Holdings	193.5	₦6.15bn	₦1.69bn	-72.5%
GTCO/GTBank	88.0	\$129,593	\$103,718	-20.0%
Zenith Bank	67.3	₦0.38bn (\$249,870)	₦5.26bn (\$3.4m)	+1,272%
UBA	48.0	\$591,902	\$781,901	+32.1%
Stanbic IBTC	33.5	Not individually disclosed	Not individually disclosed	n/a
FCMB	26.3	Not individually disclosed	Not individually disclosed	n/a
Wema Bank	5.0	Not individually disclosed	Not individually disclosed	n/a

Source: Individual bank audited financial statements, as reported by Legit.ng/Daily Trust (2025), TechCabal (2025), Independent Newspaper Nigeria (2025), Businessfront/Finance in Africa (2025) and Markets Reporters (2025). Figures are shown in the currency originally disclosed by each source (naira for Access Holdings and Zenith Bank; US dollars for GTCO and UBA); the basis of reporting (bank or group) may differ across sources, so only percentage changes are compared across banks. Zenith Bank's percentage change is the average of the naira-based (+1,284%) and dollar-based (+1,261%) changes.

Table 2 shows real, individually disclosed variation across the sample. Access Holdings recorded the highest technology investment in the sample, ₦193.5 billion in 2024, a 147 percent increase on its 2023 spending, and its fraud loss fell by 72.5 percent over the same period, from ₦6.15 billion to ₦1.69 billion, according to its audited financial statements. GTCO recorded the second-highest technology investment and a modest 20 percent decline in fraud loss. UBA, with the lowest technology investment among the four matched banks, saw its fraud loss rise by 32.1 percent. Zenith Bank is the clearest outlier: despite the third-highest technology investment in the sample, its fraud loss rose more than twelvefold, a finding corroborated independently in both naira and United States dollar terms across two separate sources, which strengthens confidence that the increase is real and not a reporting artefact. Because the currency and reporting basis differ across banks, the comparison rests on percentage changes only.

Table 3: Earlier-Period Fraud Losses for Selected Banks, FY2021

Bank	Fraud Loss, FY2021	Note
Access Bank	₦502 million (own loss); ₦1.98bn third-party loss	17,697 fraud cases recorded, mostly electronic/USSD fraud
GTBank	₦1.2 billion	15,204 fraud and forgery cases recorded
FCMB	₦89.8 million (up from ₦59.03 million)	Rise attributed to growth in electronic channel fraud
Four banks combined (incl. Wema)	₦1.77 billion	Average industry loss estimated at ₦14 billion per year across all DMBs

Source: 2021 audited financial statements of the respective banks, as reported by Kolaking/Punch (2022).

Table 3 places the FY2023-FY2024 findings in longer historical context. Comparing Access Bank's own 2021 fraud loss of ₦502 million to its 2023 loss of ₦6.15 billion shows a more than twelvefold rise before the 2024 fall to ₦1.69 billion associated with its record technology investment, suggesting that the 2024 improvement reflects a genuine reversal rather than ordinary noise. However, the 2021 figure relates to Access Bank and the later figures to Access Holdings, so the comparison may not be strictly like-for-like. GTBank's 2021 loss of ₦1.2 billion is broadly comparable in magnitude to its 2023 figure, suggesting steadier fraud control over the period, consistent with its position as the second-highest technology investor in Table 2.

Table 4: Correlation and Regression Results — FY2024 Technology Investment and Percentage Change in Fraud Loss (n = 4 Matched Banks)

Statistic	All Four Banks	Sensitivity analysis: excluding Zenith Bank (n = 3, exploratory)
Pearson correlation (r)	-0.39 (p = 0.61)	-0.97 (p = 0.16)
Spearman rank correlation (ρ)	-0.80 (p = 0.20)	-1.00
Regression slope (β)	-3.86	-0.67
R²	0.15	0.94
Regression equation	% Δ Fraud Loss = 685.6 - 3.86(Tech Investment)	% Δ Fraud Loss = 53.9 - 0.67(Tech Investment)

Source: Computed by the researcher from Table 2 data, 2026 (Pearson and Spearman correlation and ordinary least squares regression).

Table 4 reports the computed statistics for the four-bank matched sample, which is the primary result. Across all four banks, the correlation between technology investment and fraud-loss change is negative, as theory would predict, but weak and not statistically significant ($r = -0.39$, $p = 0.61$), explaining only 15 percent of the variation. Zenith Bank, whose fraud loss rose sharply despite a mid-range technology investment, pulls the estimate toward zero. Zenith Bank is, however, a genuine observation whose increase is corroborated in both naira and dollar terms, and it is therefore retained in the primary analysis. As a sensitivity analysis, excluding Zenith Bank produces a much stronger negative correlation ($r = -0.97$, $R^2 = 0.94$); however, because the resulting sample contains only three observations and the result remains statistically insignificant ($p = 0.16$), it is treated as exploratory only and not as evidence of a relationship. The overall pattern is consistent in direction with the wider literature reviewed in section 2.3. Still, it is not statistically established: the relationship is not automatic, and bank-specific factors, such as the timing of investment relative to a fraud wave, how much of the spend targeted fraud detection specifically, and internal control quality, can outweigh aggregate spending in a given year.

Table 5: Trend in Reported Fraud Cases and Losses in the Nigerian Banking Industry, 2015-2024

Year	Reported Fraud/Loss Indicator	Direction/Change
2015	₦18.02 billion involved in reported fraud, forgery and staff-theft cases; ₦3.17 billion actual loss	Baseline year
2016	₦8.68 billion involved; ₦2.40 billion actual loss	Decrease of 48.1% (amount involved) and 24.3% (actual loss) from 2015
2018-2019	Fraud and forgery cases rose	Increase of about 40% in cases
2019-2020	Fraud and forgery cases rose sharply	Increase of about 190% in cases
2021	4,695 fraud cases; ₦15.6 billion involved	Renewed upward trend
2023 (Q1-Q2)	Fraud loss rose from ₦472 million (Q1) to ₦9.75 billion (Q2)	Increase of about 1,125%; fraudulent loans accounted for 94.35% of losses
2023 (full year)	95,620 total fraud cases across financial institutions; DMBs accounted for 92% of cases	Sector-wide fraud count at its highest in the review period
2024	Total industry fraud losses reported at over ₦52 billion	Continued rise despite wider AI/ML tool availability

Source: Computed from NDIC (2017, 2022), Kanu et al. (2022), FITC (2023), NIBSS (2024), and Vanguard News (2023).

Table 5 shows that the trend in Nigerian banking fraud was not a simple, steady decline that would be expected if AI-powered tools were deployed uniformly across the industry. An initial decrease between 2015 and 2016 was followed by sharp increases from 2018 through 2023 and 2024, years in which AI-powered tools were increasingly piloted and, in some banks, formally adopted. This does not contradict the bank-level finding in Table 4; rather, it shows the moderate gains identified for Access Holdings and GTCO have not yet been achieved consistently enough across the industry to move the sector-wide trend, particularly as fraudsters have shifted rapidly toward digital channels, a moving target requiring continuous model retraining (NIBSS, 2024).

Table 6: Reported Adoption Constraints for AI-Powered Audit Tools in Nigerian Deposit Money Banks

Constraint	Evidence
Absence of dedicated AI/data-analytics units	Over 86% of banks surveyed by Ajayi and Akinrinola (2023) expected this to continue limiting AI deployment.
Data quality and integrity weaknesses	Cited as a primary constraint alongside the absence of dedicated AI units (Ajayi & Akinrinola, 2023)
Skills and technical expertise gap	Identified as a recurring constraint across the forensic investigation and cybersecurity/fraud detection reviews
Cost and infrastructure limitations	Identified as a barrier to scaling AI-based forensic and fraud-detection tools across Nigerian institutions
Weak or evolving regulatory guidance	Highlighted in the AI disclosure study, which notes the absence of formal AI disclosure regulation for Nigerian banks as of 2024 (AJEMS, 2026)

Source: Compiled from the reviewed literature, 2015-2025.

Hypotheses Tests

H₀₁ is assessed from the reviewed literature (section 2.3) rather than from a statistical test, since no audit-quality data were analysed statistically in this study. The evidence from the reviewed studies is mixed. Several studies report significant positive relationships between selected AI-powered audit tools (data mining, image recognition, and AI-supported audit judgement) and audit quality. Still, the evidence for stand-alone machine learning is weaker and less consistent, and overall benefit to internal audit is reported to be low. The evidence is therefore not sufficiently uniform to establish a consistent effect across all AI technologies, and H₀₁ cannot be conclusively rejected for AI-powered audit tools as a whole.

H₀₂ is assessed from the literature and from the bank-level results in Table 4. The evidence is mixed. High and consistent model accuracy across independent experimental studies shows that AI-powered tools can detect fraud in Nigerian banking data accurately. At bank level, however, the four-bank correlation between technology investment and fraud-loss change is weak and not statistically significant; fraud loss fell at Access Holdings and GTCO but rose at UBA and Zenith Bank. The sector-wide trend in Table 5 also shows fraud rising across much of the sector despite growing tool availability. This pattern may reflect uneven adoption, consistent with diffusion of innovation theory (section 2.2). On this evidence, H₀₂ cannot be conclusively rejected.

For H₀₃, the correlation across all four banks ($r = -0.39$, $p = 0.61$) is not statistically significant, so H₀₃ is not rejected on this small sample. The direction of the relationship is negative, and a sensitivity analysis excluding Zenith Bank gives a much stronger negative correlation ($r = -0.97$, $p = 0.16$); because this rests on only three observations and is also statistically insignificant, it is exploratory only. The bank-level evidence is therefore indicative at best, and is read alongside the wider literature, which points to a possible but unevenly realised relationship between technology investment and fraud outcomes, mirroring the mixed picture found for H₀₁ and H₀₂.

5. Findings and Discussion

The findings show that AI-powered audit tools are associated with meaningful improvements in audit quality in Nigerian deposit money banks, particularly through wider audit coverage, faster anomaly detection, and improved accuracy, echoing the benefits documented by Kokina and Davenport (2017) in the international literature. However, the improvement is neither automatic nor uniform: tools that are well integrated into audit workflow, such as data mining and image recognition, show clearer gains than machine learning applications used in isolation, and the overall benefit to internal audit in Nigerian banks remains, in the words of Ajayi and Akinrinola (2023), at a low level, reflecting the early and uneven stage of implementation across the industry.

On fraud detection, the findings reveal an important disconnect between technical capability and sector-wide outcomes. Machine learning and data mining models built and tested on Nigerian financial data consistently achieve high accuracy, often above 90 percent, in identifying fraudulent transactions (Awoyemi, Adetunmbi, & Oluwadare, 2017; Njoku et al., 2024). Yet reported fraud cases and losses across the Nigerian banking industry rose sharply in several years of the review period, including a 190 percent rise in cases between 2019 and 2020 and a further surge to 95,620 cases across financial institutions in 2023 (NIBSS, 2024). This

disconnect supports the view, consistent with the Technology Acceptance Model and diffusion of innovation theory discussed in section 2.2, that the constraint is less about whether AI-based fraud detection works, and more about how consistently and how widely it has actually been deployed, staffed, and maintained across the full population of Nigerian deposit money banks.

The findings also point to a bank-level divide broadly consistent with diffusion of innovation theory: larger, better-resourced banks appear to be moving faster in building internal AI capacity, for instance through structured analyst-training programmes, while smaller or less-resourced banks remain more exposed to the adoption constraints summarised in Table 6, namely the absence of dedicated AI units, data quality weaknesses, skills shortages, cost, and evolving regulatory guidance. This uneven pattern of adoption, rather than any fundamental weakness in the underlying AI techniques, is the most likely explanation for why sector-wide fraud statistics have not yet fallen in step with the growing sophistication of AI-based fraud-detection models.

From a theoretical standpoint, these findings support agency theory's prediction that better monitoring narrows the information gap between bank management and other stakeholders, but only where the monitoring tool is actually deployed at sufficient scale; a fraud-detection model with accuracy above 99 percent in laboratory conditions does not protect a bank that has not yet adopted it, trained staff to use it, or connected it to a live transaction feed. The findings also support the fraud triangle's opportunity dimension, since the sharpest rises in fraud cases coincide with the rapid growth of digital and mobile banking channels, which have, for a time, expanded opportunity faster than AI-based monitoring capacity has been built out to cover them (NIBSS, 2024).

The findings have two further implications. First, because AI-powered audit tools and RegTech/SupTech applications draw on the same data-mining and machine-learning capabilities (Arner, Barberis, & Buckley, 2017), the same skills and infrastructure gaps limiting AI's contribution within individual banks are also likely to limit how effectively regulators can supervise AI-related risk across the industry, meaning closing the gap identified in this study is not solely a bank-level task. Second, the bank-staff dimension highlighted by Tade (2022) and Odukoya and Samsudin (2021), that a meaningful share of fraud cases involve staff, particularly temporary and casual staff, is a reminder that AI-powered audit tools are best understood as complements to, rather than substitutes for, sound staff vetting and internal control culture; a bank that deploys sophisticated fraud-detection models while leaving these weaknesses unaddressed is unlikely to see the full benefit of its investment, a nuance consistent with the agency-theory and institutional-theory perspectives discussed in section 2.2.

5.1 Limitations of the Study

This study has some limitations worth noting. As a desk-based, structured literature review without a formal review protocol or quality-appraisal instrument, it relies on the methods and samples of the individual studies reviewed, which vary considerably, making direct comparison difficult, and some selection bias cannot be ruled out. Complete 2025 fraud data were also unavailable, so the empirical analysis ends in 2024. Fraud statistics reported by NDIC, NIBSS, and FITC depend on the completeness of returns filed by individual banks, which may understate the true scale of fraud in some years. Because AI adoption in Nigerian banking is evolving quickly, some patterns identified here may already be changing by the time of publication.

Specifically for the bank-level regression, the sample of four matched banks is too small to support statistically robust inference, and the results in Table 4 should be read as indicative rather than conclusive; the inclusion or exclusion of a single bank (Zenith Bank) materially changes the correlation. Aggregate technology investment, the proxy used for AI-related investment, is not the same as AI-powered audit tool adoption specifically, since disclosed budgets cover core banking software and cybersecurity alongside any AI-specific systems. Fraud-loss figures for the sample banks were also reported in different currencies and on a Bank versus Group basis, which is why this study compared percentage changes rather than absolute values. Future studies should combine a larger panel of bank-level primary data, ideally covering AI-specific spending disclosed under future regulatory guidance, with a longer run of sector-wide fraud statistics, to test the relationship with greater statistical power.

6. Conclusion and Recommendations

This study examined the impact of AI-powered audit tools on audit quality and fraud detection in Nigerian deposit money banks between 2015 and 2024, drawing on a structured literature review of thirty empirical

studies and a decade of sector-wide fraud statistics from NDIC, NIBSS, and FITC. The findings show that AI-powered audit tools, particularly data mining, image recognition, and AI-supported audit judgement, are associated with real improvements in audit quality, and machine learning models built on Nigerian financial data can detect fraud with high technical accuracy. However, these technical gains have not yet translated into a clear, sector-wide fall in reported fraud cases and losses, mainly because adoption remains uneven, constrained by the absence of dedicated AI units, weak data integrity, skills shortages, cost, and evolving regulatory guidance.

The study concludes that the promise of AI-powered audit tools for Nigerian DMBs is real but not yet fully realised, and closing the gap between technical capability and sector-wide outcomes will require deliberate investment by banks, coordinated regulatory support, and closer attention from the audit profession to how these tools are integrated into everyday practice, rather than treated as stand-alone technical projects.

Considering these findings, the following recommendations are made:

1. Deposit money banks should establish dedicated AI and data-analytics units within their internal audit and fraud-control functions, rather than treating AI adoption as an ad hoc initiative, to move beyond the low-level implementation reported in current studies.
2. Banks should invest deliberately in improving the quality and integrity of the transaction and customer data on which AI-powered audit and fraud-detection tools depend, since poor data quality is a leading constraint on AI effectiveness in Nigerian banks.
3. Banks and audit firms should prioritise AI tools, such as data mining and image recognition, that already show measurable audit-quality gains, while carefully piloting machine learning applications before scaling them across the audit function.
4. The CBN, NDIC, and other regulators should develop clearer, phased guidance on the use and disclosure of AI in bank audit and fraud-control functions, building on the governance-signaling role voluntary AI disclosure has already begun to play.
5. Future research should combine bank-level primary data on AI adoption with sector-wide fraud trend data to test more directly whether banks investing more heavily in AI-powered audit tools see correspondingly lower fraud losses, controlling bank size.
6. Banks should pair investment in AI-powered audit tools with continued attention to staff vetting and internal control culture, particularly for temporary and casual staff, since a meaningful share of fraud in Nigerian DMBs still involves insiders, a vulnerability technology alone cannot close.
7. Regulators should consider requiring DMBs to disclose AI-specific audit and fraud-detection investment separately from general technology spending, since the current practice of reporting a single combined budget makes it difficult to assess how much digital spend targets audit quality and fraud control.

References

- Aderibigbe, A. A., Tonade, A. M. A., Fadairo, I. O., & Edun, K. O. (2024). Artificial Intelligence and quality of audit judgement in Nigeria. *Ilorin Journal of Finance*, 8(1), 1–15.
- African Journal of Economic and Management Studies. (2026). Artificial intelligence disclosure and bank performance: Evidence from deposit money banks in an emerging market. *AJEMS*.
- African Journal of Management and Business Research. (2026). Adoption of AI-based accounting systems and audit quality in Nigerian deposit money banks. *AJMBR*, 23(1).
- Ajayi, F. A., & Akinrinola, O. (2023). Artificial Intelligence and internal audit quality of commercial banks in Nigeria. *International Journal of Management and Economics Invention*, 9(4), 2897–2907.
- Alles, M. G. (2015). Drivers of the use of Big Data by the audit profession. *Journal of Information Systems*, 29(2), 439–449.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech and the reconceptualisation of financial regulation. *Northwestern Journal of International Law & Business*, 37(3), 371–413.
- arXiv. (2024). Credit card fraud detection in the Nigerian financial sector: A comparison of unsupervised TensorFlow-based anomaly detection techniques, autoencoders and PCA algorithm. *arXiv preprint*.
- Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. In *Proceedings of the 2017 International Conference on Computing Networking and Informatics (ICCNI)* (pp. 1–9). IEEE.
- Businessfront/Finance in Africa. (2025, April 18). Four leading Nigerian banks lost \$5.2m to fraud in 2024 amid digital transaction surge. *Businessfront*.
- Central Bank of Nigeria. (2023). Financial stability report, first half 2023. CBN.

- Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud: Decision Support Systems, 139, Article 113421.
- CreedTec. (2025, December 15). Machine learning fraud detection for mobile money in Nigeria: A critical defense. Medium.
- Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
- DeAngelo, L. E. (1981). Auditor size and audit quality. Journal of Accounting and Economics, 3(3), 183–199.
- Eneh, O. M.-R., Okeke, F. C., & Amahalu, N. N. (2023). Artificial intelligence and fraud detection of deposit money banks in Awka-South, Anambra State, Nigeria. Global Journal of Artificial Intelligence and Technology Development, 1(2), 8–20.
- Financial Institutions Training Centre. (2023). Report on frauds and forgeries in Nigerian banks: Second quarter 2023. FITC.
- Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial Intelligence and machine learning for fraud detection in financial statements. Journal of Forensic and Investigative Accounting, 12(1), 705–722.
- Independent Newspaper Nigeria. (2025, May 19). 2024: Access Holdings invests N193.5bn in fraud prevention. Independent.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.
- Journal of International Accounting, Taxation and Information Systems. (2025). Forensic investigation and fraud detection in Nigeria: Leveraging artificial Intelligence. JIATIS, 2(1).
- Kamble, Y., & Devarmani, N. G. (2024). Application of artificial Intelligence (AI) in forensic investigation. In Advances in Forensic Science and Criminal Investigation (pp. 197–210). IGI Global.
- Kanu, C., Nnam, M. U., Ugwu, J. N., Achilike, N., Adama, L., Uwajumogu, N., & Obidike, P. (2022). Frauds and forgeries in banking industry in Africa: A content analysis of Nigeria Deposit Insurance Corporation annual crime report. Security Journal, 36(4), 671–692.
- Kolaking/Punch. (2022, January 20). Four banks lost N1.77bn to fraud in 2021, says report. Punch.
- Kokina, J., & Davenport, T. H. (2017). The emergence of artificial Intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122.
- Legit.ng. (2025, April 24). GTCO, UBA, Zenith, others increase investment in tech as banks lose N52.26 billion to fraudsters. Legit.ng.
- Markets Reporters. (2025, April 20). Zenith Bank's fraud loss deepens while peers see decline. Markets Reporters.
- Mohammed, U., Wajiga, G. M., & Saidu, H. A. (2024). Financial fraud detection in Nigerian banks: A data mining approach. International Journal of Computer Science and Mathematical Theory, 10(3), 1–12.
- Nigeria Deposit Insurance Corporation. (2017). Banking industry recorded decline in frauds, forgeries – NDIC [Press briefing]. NDIC.
- Nigeria Deposit Insurance Corporation. (2022). Annual report and statement of accounts 2021. NDIC.
- Nigeria Inter-Bank Settlement System. (2024). Annual fraud landscape report 2023. NIBSS.
- Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: A web-based application. Machine Learning, 20(4), 1–12.
- Odukoya, O. O., & Samsudin, R. S. (2021). Knowledge capability and fraud risk assessment in Nigeria deposit money banks: The mediating effect of problem representation. Cogent Business & Management, 8(1), Article 1899450.
- Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.
- Tade, O. (2022). Nature of frauds in Nigeria's banking ecosystem, 2015-2019. Journal of Financial Crime, 29(4), 1241–1248.
- TechCabal. (2025, April 18). Access Holdings records highest tech spend as fraud losses drop 73%. TechCabal.
- Ukpong, E. G., Udoh, I. I., & Essien, I. T. (2019). Artificial Intelligence: Opportunities, issues and applications in banking, accounting, and auditing in Nigeria. Asian Journal of Economics, Business and Accounting, 10(1), 1–6.
- Vanguard News. (2023, August 24). 24 banks lose N9.75b in Q2 2023 as fraud rises 277%. Vanguard.