Innovations

Technological Tools for Enhancing Fraud Management in Nigeria Banks

[1]Timi Joshua Ayeni (MSc); [2]Dr. Sylvester Erabie (PhD)
[1,2] Accounting Department, College of Management and Social Science Covenant University

Abstract: *The study examines the impact of technology on fraud management in international authorized banks, specifically within Nigerian banks. The study utilized a descriptive survey research design with quantitative techniques, distributing questionnaires to staff members in the authorized banks. Data analysis using SPSS and SEM-PLS revealed a significant positive impact of artificial intelligence on fraud management. Adopting technological tools, such as distributed ledger technology, machine learning, X-ways forensic and artificial intelligence, enhances fraud awareness (fraud management) strategies in banks. The findings highlighted the importance of leveraging these technologies to protect customer assets, build trust, and mitigate risks. Continuous updating and refinement of fraud management systems are essential to combat evolving fraudulent activities successfully. Employing technological tools empowers banks to safeguard operations and customers from potential financial risks.*

Keywords: *Technological, fraud Management, international authorized banks, AI.*

Background of the study

In an era where digital transformation is revolutionizing industries worldwide, the banking sector in Nigeria is no exception. As financial institutions embrace advanced technologies to enhance their services, they also face the growing challenge of sophisticated fraud schemes. The need for robust, innovative solutions to combat financial fraud has never been more critical. Technological tools are emerging as powerful allies in the fight against bank fraud, offering unparalleled capabilities to detect, prevent, and mitigate fraudulent activities. This paper explores the cutting-edge technological tools employed in modern bank fraud management in Nigeria, highlighting how these innovations are safeguarding financial integrity and fostering trust in the banking system. From artificial intelligence and machine learning to distributed ledger technology and biometric

authentication, we delve into the strategies that Nigerian banks are deploying to stay ahead of fraudsters in an increasingly digital world.

Financial institutions in all nations worldwide have in most respects, due to their unique standpoints in a given economy, been of major impact regarding the enhancement and development of their country's economic status. The banking system in a country is significant because of its key function of collecting funds from surplus in an area and then furthering them to the deficit area, indebted to by bringing such financial lacks for the community into the sector of finance. The main function of this sector is to foster economic growth and stability which are the two essential elements of any economy. (Ogechukwu, 2013). This banking sector took shape as an important part of the economy affecting not only the scale of economic growth but also the type of changes the development experiences. It is, also, a key factor in forming many economic signposts like unemployment and inflation which have the overall effect of determining the standard of living. Diamond (1984) offers an important interpretation that banking activities provide an intermediary monitoring role between key lenders (depositors) and the borrower. The role of banks as intermediaries in various financial crises across the globe has been a major issue of debate. As far as building a special relationship with depositors and borrowers, bank should not only focus on their clients trust and confidence. Notwithstanding, safety assurance in banking practices is the most essential task of any bank, its ability or inability to perform its function as a financial intermediary has made a huge difference in financial crises across the globe.

In 2023, Access Bank, Nigeria's largest commercial bank by assets, reported ₦6.15 billion in losses due to fraud and forgery, a significant increase from ₦1.44 billion the previous year. Fraudulent transfers, withdrawals, and reactivations accounted for 80% of the losses, followed by embezzlement (29%), which included cash theft, suppression, pilferage, and dry posting, as well as electronic fraud and USSD (9%) (Osamu Ekhator, 2024).

First Bank, a Nigerian bank with a market capitalization of ₦829 billion, has initiated legal action to recover substantial funds allegedly diverted by an employee from its head office team in Iganmu, Lagos. The employee, who is now a fugitive, is accused of transferring the funds to 98 bank accounts, including one belonging to his wife. The bank reported the incident to the Nigerian Police Force on March 25, 2024, and obtained three court orders between April 4-8, 2024, to freeze hundreds of accounts suspected of receiving the stolen money. Sources informed TechCabal that the amount initially discovered to have been diverted was approximately ₦12 billion, but it has since increased to around ₦40 billion ($29 million) (Olumuyiwa&Muktar, 2024).

TijaniMuizAdeyinka, the accused employee and manager on the electronic products team at First Bank, had the authority to process customer reversals. According to a

First Bank employee familiar with the case, Muiz allegedly used his position to credit customer reversal requests to a merchant account he controlled. As the final authorizer on the team, he did not require further approvals, allowing him to divert customer funds undetected for nearly two years (Olumuyiwa & Muktar, 2024).
The upsurge of scamming hence, especially in digital technologies and electronic payments systems, becomes alarming, therefore the attention of the financial sector is necessary and urgent for the relevant authorities. In their effort to conceal internal abuse, unethical bankers collude with external parties to defraud innocent customers by creating false accounts to deposit funds from the victims. Furthermore, it indicates not only the comprehensive corruption in society, but in addition reveals how financial establishments, which are supposed to be reliable keepers of individuals' assets, have turned into a shelter for criminals. In 2016, there were already 16,751 cases reported on bank frauds. The number of bank frauds have even doubled in 2017. The growing number of these illegal activities necessitates the development of strict measures by the regulatory bodies and the law enforcement agencies to protect the integrity and the stability of our financial system.

Statement of research problem

Fraud is a huge danger to the development and progress of any nation, and it ought not be taken lightly on an international scale. Hence, the functionality of forensic accounting is seen as that which prevents corruption in the public sector of Nigeria. (Abdurrahman, 2019) On the other hand, there is the continuously alarming trend of rampant and malicious activities that the Nigerian banking sector faces. Several researchers such as Ojaide (2000), Okoye and Akamobi (2009), Owojori and Asaolu (2009), and Izedonmi and Mgbame (2011) have also acknowledged this phenomenon, emphasizing the importance of visibility and utilization of forensic accounting services to fight against these financial crimes.The rapid digital transformation in the banking sector has brought about significant improvements in service delivery and customer experience. However, it has also led to an increase in sophisticated fraud schemes, posing a serious threat to the financial stability and integrity of banks in Nigeria. Traditional methods of fraud detection and prevention are no longer sufficient to combat these advanced fraudulent activities. Fraud is one of the major threats to the business world as no company has the power to resist its negative effects (Adeniran, 2017). Consumers in the banking industry want accountability, fairness, openness, and effective intermediation. Banks are allowed to fulfil their commitments honestly and without committing fraud. The restoration of public confidence and goodwill in the banking industry is of great importance. There is an urgent need to investigate and implement modern technological tools that can effectively manage and mitigate bank fraud. This research aims to explore

the utilization of advanced technologies such as artificial intelligence, machine learning, distributed ledger technology, and biometric authentication in Nigerian banks, examining their effectiveness and impact on enhancing fraud management and fostering trust within the banking system. The study seeks to address the gap in understanding how these technological innovations can be optimally deployed to safeguard financial institutions against the evolving threat of fraudulent activity

Objectives of the study

The basic goal of this research is to examine the relevance of technical tools., methods to ascertain if banks have totally adopted the usage in order to proffer solutions that banking sector can use in fraud management (which is to prevent and detect fraud). The specific objectives are to:

1. evaluate the effect of distributed ledger technology on fraud management among international authorized banks in Nigeria.
2. appraise the effect of artificial intelligence on fraud management among international authorized banks in Nigeria.
3. determine the effect of machine learning on fraud management among international authorized banks in Nigeria.
4. examine the effect of X-ways forensic on fraud management among international authorized banks in Nigeria.

Research Question

The study's questions for this research assignment are listed below:

1. What is the impact of distributed ledger technology on fraud management among international authorized banks in Nigeria?
2. What is the impact ofartificial intelligence on the effectiveness of fraud management among international authorized banks in Nigeria?
3. What is the impact of machine learning on the effectiveness of fraud management among international authorized banks in Nigeria?
4. What is the impact of X-Ways Forensic on the effectiveness of fraud management among international authorized banks in Nigeria?

Underpinning Theory of Study

The Theory of Technology- Enable Crime

Technological Facilitation: Technology opens up new avenues for criminal activities that were previously unavailable or more difficult to execute. For instance, the internet has given rise to cybercrimes like phishing, identity theft, hacking, and online fraud. The theory acknowledges that technological progress makes certain crimes more efficient, accessible, and harder to detect.

Expanded Criminal Opportunities: Technology creates fresh opportunities for criminal behaviour. The widespread use of smartphones and digital devices, coupled with our growing reliance on digital platforms, has broadened the scope of criminal activities. Criminals can now target individuals and organizations from a distance, exploit network vulnerabilities, and engage in illegal acts on a global scale.

Evolving Criminal Tactics: The theory recognizes that criminals adjust their strategies and tactics to harness technological advancements. They develop sophisticated techniques to exploit software vulnerabilities, networks or even human behaviours. This includes social engineering tactics as well as methods such as malware distribution, ransom ware attacks, among other cybercrime practices. Criminals continuously innovate and adapt their tactics to evade detection while maximizing their illicit gains.

Global Reach and Transnational Crime: Technology has transcended geographical boundaries, making it possible for criminals to engage in transnational criminal activities. Cybercriminals can operate from anywhere globally, targeting victims residing in different countries. This globalization of crime presents challenges for law enforcement agencies worldwide, and necessitates international collaboration efforts to effectively investigate and combat technology-enabled crimes.

Evolving Legal Frameworks: The theory recognizes that technology-enabled crime poses challenges to existing legal frameworks. Laws often struggle to keep pace with technological advancements, making it difficult to effectively prosecute and prevent these crimes. Governments and legal systems need to continuously adapt to address emerging challenges, such as privacy concerns, jurisdictional issues, and the complexities of cross-border crime.

Response and Prevention Strategies: The theory emphasizes the importance of developing comprehensive response and prevention strategies to tackle technology-enabled crime. This includes investing in robust cyber security measures, educating individuals and organizations about potential risks, enhancing law enforcement capabilities in digital investigations, promoting international cooperation, and fostering partnerships between the public and private sectors to share information and expertise.

By comprehending the theory of technology-enabled crime, policymakers, law enforcement agencies, and other stakeholders can devise proactive strategies to combat emerging cyber threats and mitigate the impact of technology on criminal activities. It underscores the necessity for a multidisciplinary approach that combines technology, law, policy, and social factors in order to effectively address the challenges posed by technology-enabled crime.

The Policeman Theory

Dr. Peter Tickner, a forensic accountant and former detective, developed the concept of the "policeman theory" in forensic accounting. He emphasized the role of forensic accountants as financial detectives, drawing parallels between their work and that of police officers in investigating and deterring financial crimes.

The policeman theory highlights the proactive nature of forensic accountants (which aditors can also use), who actively seek out financial irregularities, analyse evidence, and report their findings. This theory underscores the importance of forensic accountants acting as watchdogs, enforcing financial regulations, and maintaining the integrity of financial systems within organizations.

While, Dr. Peter Tickner is associated with the development of the policeman theory in forensic accounting, it is important to note that forensic accounting as a whole has been shaped by the contributions of many experts and professionals in the field.

The term "policeman theory" in forensic accounting refers to the role of a forensic accountant as a financial investigator and enforcer. Forensic accountants are trained professionals who apply their accounting knowledge and investigative skills to uncover and analyse financial fraud, misconduct, and other financial irregularities.

The policeman theory emphasizes the proactive and preventive aspects of forensic accounting. Like police officers who enforce laws and maintain order, forensic accountants act as financial watchdogs to detect and deter fraudulent activities within organizations.

Empirical Review

A significant number of empirical studies have been performed on fraud investigation, fraud management, information communication in banking sector, risk management approach to deterrence fraud at fraud at bank, forensic accounting with a focus on fraud detection and prevention. Most of these research efforts draw their conclusions from data in developed countries such as the United States, the United Kingdom, and Canada and some developing countries. In addition to insights from former convicts, the empirical data also corroborate the relationship between technology, fraud management, accounting and fraud detection. The subsequent paragraphs outline the methodologies, samples, and primary findings of these investigations.

Oyetoyan (2021), conducted a study on impact of regulation of financial technonlogy service on the performance of deposit money banks in Nigeria. This study examines how regulating Financial Technological services affects the performance of selected DMBs in Kwara State, Nigeria. Data was collected from 220 employees across five DMBs in Ilorin through structured questionnaires, targeting bank managers and senior staff. Statistical analyses, including Pearson Moment Correlation, ANOVA, and Multiple Regression, were used. The results indicate a positive impact of financial

technology platforms such as PayStack, Branch,PiggyVest, Mines and NetPlus on the performance of DMBs. The study concludes that FinTech services enhance bank performance and recommends that Nigerian DMBs conduct regulatory oversight to align FinTech and bank services effectively.

Doni (2022) conducted a study on the approach to managing fraud in Indonesian banks. The study aimed to inform practitioners about the level of understanding and awareness among bank employees regarding fraud risk management in fraud prevention. Utilizing a qualitative descriptive analysis method, the research presented its findings narratively. The data used was non-numeric secondary data obtained from reports, journals, books, and websites. The study concluded that implementing a fraud risk management approach within the fraud triangle model framework can effectively prevent, detect, and respond to fraud in banks.

Chukwukaelo (2018), examined the impact of Information Technology on Performance of Banks in Nigeria, the study examined the impact of four e-banking channels—ATMs, POS, internet banking, and mobile banking—on the profitability of Deposit Money Banks from 2006 to 2016. Using a panel data regression model, the study found a significant and positive impact of electronic banking on bank profitability. It recommends collaboration among the government, regulatory authorities, and banks to create a supportive environment and effective regulatory framework for optimal e-banking deployment.

Dumbulu (2024), investigated examined Centenary Bank's internal audit practices for fraud management to evaluate their effectiveness and identify improvements. With rising fraud rates in Uganda causing significant financial losses, robust internal audits are crucial. Despite their importance, many firms, including Centenary Bank, underutilize internal audits for fraud prevention. Using qualitative case study methods, including document analysis and interviews with internal auditors and anticorruption officers, the study found a positive correlation between internal auditing and fraud detection (r=0.615). The study benchmarks Centenary Bank’s practices against best practices to identify gaps and provide recommendations to enhance fraud detection, prevention, and response protocols, with a focus on fraud related to assets and financial reporting.

Study population

This research concentrated on the technological tools on fraud management in Nigeria banks. This is because Nigeria ranks among the highest-risk countries in the World Threat Impacts Survey 2017, which was released in May 2017. Among the over 21 known commercial banks, these are classified into two major classes: international banking authorizations (First bank, Access bank, UBA, Union, Zenith, GTB, FCMB and Fidelity), commercial banks with national banking authorizations (Eco, Citibank, Polaris, Unity, Wemaetc), and regional authorizations. The sample

population to be considered for this study are the staff of commercial banks (international authorized), the forensic unit, general investigative units, the information communication Technology units in the international authorized banks.

Sampling Procedures/Sample Size Determination

The method of sampling employed in this research study is the generic census, where all the international authorized banks were considered. Questionnaires were distributed to these banks. These questionnaires were served only to those considered relevant to this study. The names of the banks are shown in the appendix

Data Collection Methods

The data that were in this study were from both primary and secondary sources. It is quantitative, more specifically relational because it includes feedback directly from the interviewees using the questionnaires. I the secondary data were gotten from the Central Bank of Nigeria.

Data Analysis Techniques

According to Baridam (2001), the main aim of statistical inferences is to test statistical hypotheses and to estimate population parameters. The data involving the surveys, documents or the observations were examined with SPSS and structural equation modelling (SEM), which are the most relevant techniques for the purpose and success of this study. Data were tested for normality statistics by applying skewness and Kurtosis tests.

The gathered data were subjected to further processing with the help of Partial Least Square Structural Equation Modelling (PLS-SEM) on SmartPls3. Structural equation modelling (SEM) was the tool adopted in this study as a model it works better with small sample effects and is more appropriate for complex constructs in modeling (Urbach&Ahlemann, 2010). SmartPls3 has two modes, the measurement model and the structural model also recognized as the outer/inner model. The outer model is the one that cycles between path coefficients and path loadings, and the inner model is the one that cycles among path coefficients, total effect coefficients, and indirect effect coefficients (Garson, 2016). The data collected underwent an analysis process to ensure that they are reliable, have convergent validity, and discriminant validity after which an analysis using structural equation modelling (SEM) was conducted afterwards. Although SEM did not support all the hypotheses of the research, it still found that national choice made a difference in the effectiveness of regulations. The study used the following to describe how they conducted these pre-tests.

Method of Data analysis:

Construct Reliability and Validity

It is essential to ensure that the instruments employed to make the measurements of the traits used in the study provide reliability and validity. The data were subjected to a reliability and convergent validity test. Convergent validity is usually used in the assessment of the correlations of the varied indicators of the said dimension. Later corrections were added as required, in order to fix the result that had not passed any of the trials.

The reliability of constructs was evaluated using Cronbach's Alpha and composite reliability. At the same time, co- AVE was used by Fornell and Larcker (1981) to analyse for convergent validity. Correlating to Cronbach's Alpha coefficient of 0 should be ≥. 7 (Hair et al. 2014). Composite reliability coefficient must be ≥ to show high consistency. AVE factor loading should be ≥ 0. 12 or more (Lee & Chen, 2013).5 (Garson, 2016). In this scenario, if any of the construct fails to meet any of these minimum standards, adjustments are made. To keep the scrutiny level high, we have removed the items, which lessens the impact on the construct in any way violates the criteria. This process took a continuous path until all the models had successfully crossed each of the thresholds for every experiment.

Factor Loadings

It is essential that the indicators have a reliable power in order to load consistently beneath their individual structures. According to Hair et al. (2014), the purpose of the indicators is not to be lower than 0. 7. The items having capacity below 0 were of the cargo which ware estricted. Our overall efficiency improvement was 7%, which was achieved through the removal of (Hair et al. 2014). The things that will be operating above 0. 7 were retained. In which case (s) of a removed item (s), the data were retested for another reliability and validity test. Overall, the data were still put into tests of construct reliability and convergent validity, adding a new dimension of discriminant validity to consider. Discriminant validity is usually applied to test that the construct and its indicators are different from other constructs and their indicators in the outer model (Lee & Chen, 2013). Discriminative validity was tested through the use of HTMT and MTMD horizontal plots as a particular analysis test.

The Discriminatory Features of AVE are another way to build discernment. Heterotrait and Monotrait can be the ways this can be done. To show discriminant validity, the square root of the AVE must be greater than the correlation with the other latent variables (Garson, 2016). In the table of correlations where it is seen (read: seen being) values (of 'AVE' squared are higher than other latent variables' correlations) data will be assumed to test discriminant validity, using Heterotrait and

Monotrait criteria. It is presumed that the data cleansing and screening are performed before moving further customarily into the analysis of these data. This resulted in the next phase. Data from the second stage were used to test the preliminary suppositions of the study.

Data Presentation

Table 1.1Analysis of the Response Rate

Questionnaire	**Frequency**	**Rate %**
Retrieved	**71**	**88.75**
Not Retrieved	**9**	**11.25**
Total Distributed	**80**	**100**

Source: Researcher's Field Survey Result, (2023)

Table 1.1 depicted that out of the 80 questionnaires distributed, 71 was retrieved from the respondents. This number was considered sufficient to achieve the objectives of the study.

Analysis of Research Objectives

Table 1.2 Frequency Distribution for Distributed Ledger Technology

S/N	**Distributed Ledger technology (DLT) (Block Chain)**	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	TOTAL
1	Distributed ledger technology is used to locate fraudulent activity in my bank.	21 (29.9%)	42 (59.2%)	5 (7.0%)	3 (4.2%)	0 (0%)	71 (100%)
2	We use distributed ledger technology to detect fraudulent practice	20 (28.2%)	43 (60.6%)	8 (11.3%)	0 (0%)	0 (0%)	71 (100%)
3	We use specific ledger software to detect suspicious fraudulent transactions.	34 (47.9%)	33 (46.5%)	3 (4.2%)	1 (1.4%)	0 (0%)	71 (100%)

Source: Field Survey Results (2023)

In the survey conducted, we gathered data on three statements regarding the use of distributed ledger technology to detect fraudulent activity in banks. Let's dive into the findings:

Statement 1: Distributed ledger technology is used to locate fraudulent activity in my bank. The results showed that a majority of respondents (89.1%) either agreed or strongly agreed with this statement. Among them, 59.2% agreed and 29.9% strongly agreed. A smaller portion, 7.0%, remained undecided, while only 4.2% disagreed.

Statement 2: We use distributed ledger technology to detect fraudulent practice. Similar to the previous statement, a significant majority (88.8%) of respondents agreed or strongly agreed that their bank utilizes distributed ledger technology for detecting fraudulent practices. Specifically, 60.6% agreed and 28.2% strongly agreed with this statement. A small portion of respondents (11.3%) remained undecided, with no one expressing disagreement or strong disagreement.

Statement 3: We use specific ledger software to detect suspicious fraudulent transactions. For this statement, the responses were as follows: Strongly Agree - 47.9%, Agree - 46.5%, Undecided - 4.2%, Disagree - 1 respondent (1.4%). No respondent strongly disagreed with this statement. These findings indicate a positive sentiment towards the use of distributed ledger technology and specific ledger software in detecting fraudulent activity within banks among the surveyed individuals

The statement received a varied response, with no clear consensus among the respondents. Around half of the participants (47.9%) expressed strong agreement, while a similar number (46.5%) agreed that their bank utilizes specialized ledger software to identify potentially fraudulent transactions. A small portion (1.4%) disagreed with the statement, and 4.2% were unsure.

These detailed findings revealed that most respondents held a positive view of distributed ledger technology (DLT) and its role in uncovering and preventing fraudulent activities within their bank. The significant agreement percentages demonstrate confidence in the effectiveness of DLT and dedicated ledger software for detecting fraud.

It's vital to remember that these results indicate a diverse range of opinions among the participants, suggesting a nuanced understanding of the topic at hand.

Table 1.3 Frequency on Artificial Intelligence

S/N	**Artificial Intelligence**	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	TOTAL
1	Artificial intelligence (AI) has improved the detection of fake payment.	32 (45.1%)	38 (53.5%)	1 (1.4%)	0 (0%)	0 (0%)	71 (100%)
2	Artificial Intelligence is used in our bank to identify frauds	36 (50.7%)	31 (43.7%)	3 (4.2%)	1 (1.4%)	0 (0%)	71 (100%)
3	AI is used in the bank to give quick identification of customers' identity	43 (60.6%)	25 (35.2%)	1 (1.4%)	2 (2.8%)	0 (0%)	71 (100%)

Source: Field Survey Results (2023)

In the aspect of detecting fake payments, the effectiveness of artificial intelligence (AI) is showcased in Table 1.3. The data revealed that AI has significantly improved the detection of fraudulent transactions. A staggering 98.6% of respondents either agreed or strongly agreed with this notion. Among them, 45.1% expressed strong agreement, while 53.5% simply agreed. Merely a minute fraction (1.4%) remained uncertain, and there were no dissenting voices.

Moving on to Statement 2, it pertains to the utilization of AI in identifying frauds within our bank. A resounding majority (94.4%) of respondents either agreed or strongly agreed with this statement's accuracy. Among them, 50.7% exhibited strong agreement, while 43.7% expressed agreement without utmost conviction. A small percentage (4.2%) remained unsure about the matter, and only a negligible portion (1.4%) disagreed.

Lastly, Statement 3 highlights the use of AI in swiftly verifying customers' identities within the bank's operations. Once again, an overwhelming majority (94%) either agreed or strongly agreed with this statement's validity as well. Among these respondents, a significant proportion (60.6%) showed strong agreement and another portion (35.2%) merely agreed without absolute certainty. A slight fraction (1.4%) remained uncertain about this aspect while an even smaller proportion (2.8 %) disagreed.

Overall, the results demonstrated that AI has played a crucial role in enhancing payment security and fraud prevention within financial institutions like banks. The

majority of respondents acknowledged its positive impact on detecting fake payments, fraud identification, and quick customer identity verification

Based on the feedback received, an overwhelming majority (95.8%) of respondents either strongly agreed or agreed that their bank utilizes AI to swiftly verify customers' identities. Of those surveyed, 60.6% strongly agreed, while 35.2% simply agreed with this statement. A small proportion (1.4%) expressed uncertainty, and 2.8% disagreed.

These detailed findings indicate that most respondents held a positive perception of how AI has impacted the banking industry. They believe that AI has enhanced the detection of fraudulent transactions, plays a crucial role in identifying and preventing frauds, and facilitates prompt verification of customers' identities. The high agreement percentages reflect a level of confidence in the effectiveness of AI in these domains.

The data further revealed that respondents view the use of AI favorably when it comes to enhancing payment security, detecting frauds, and expediting customer identity verification processes. There is a general consensus among participants that AI holds immense potential in these areas and its integration into banking operations is widely accepted by the majority who partook in this survey.

Table 1.4 Frequency on Machine Learning

S/N	**Machine Learning**	SA	A	U	D	SD	TOTAL
1	We use machine learning in monitoring transactions within and outside the country	25 (35.2%)	36 (50.7%)	10 (14.1%)	0 (0%)	0 (0%)	71 (100%)
2	We use machine learning to store customers' information properly	29 (40.8%)	33 (46.5%)	9 (12.7%)	0 (0%)	0 (0%)	71 (100%)
3	We use machine learning to improve our payment process	39 (54.9%)	24 (33.8%)	7 (9.9%)	1 (1.4%)	0 (0%)	71 (100%)

Source: Field Survey Results (2023)

The survey data revealed that machine learning plays a crucial role in monitoring transactions, both domestically and internationally. Out of the total respondents, 85.9% either agreed or strongly agreed with this statement. Among them, 50.7% expressed strong agreement, while 35.2% simply agreed. A smaller portion of the

respondents (14.1%) remained undecided, with no one expressing disagreement or strong disagreement.

In addition to transaction monitoring, machine learning is also utilized to effectively store customer information. Of the respondents, 40.8% agreed and 46.5% strongly agreed with this statement, making it clear that they recognize the importance of using machine learning for proper information management. Similarly, a small percentage (12.7%) remained undecided on this matter.

These findings highlight the widespread acceptance and understanding among respondents regarding the significant role played by machine learning in monitoring transactions and securely storing customer information.

When it comes to properly storing customers' information, the findings revealed that a large majority of respondents (87.3%) either agreed or strongly agreed with the utilization of machine learning for this purpose. Specifically, 46.5% strongly agreed and 40.8% agreed with the statement. A smaller percentage (12.7%) remained undecided, while there were no respondents who disagreed or strongly disagreed.

Regarding Statement 3, which pertains to the use of machine learning to improve the payment process, the results show that 39 respondents (54.9%) agreed and 24 respondents (33.8%) strongly agreed with this statement. Additionally, there were 7 respondents (9.9%) who remained undecided, and only 1 respondent (1.4%) disagreed, with no respondents strongly disagreeing.

Based on these responses, it can be concluded that a significant majority of participants (88.7%) either agreed or strongly agreed with the notion that machine learning is employed to enhance the payment process. Among them, 54.9% expressed agreement while 33.8% expressed strong agreement. A smaller portion of participants (9.9%) remained undecided, while only a negligible percentage (1.4%) disagreed.

In summary, when analysing the data in detail, it becomes apparent that a substantial number of participants held a positive perception regarding the usage of machine learning in various banking operations such as monitoring transactions within and outside the country, proper storage of customer information, and improvement of payment processes. The high percentages indicating agreement suggest a level of confidence in the effectiveness of machine learning in these areas.

Overall, it is evident from survey results that people generally have a favorable view towards employing machine learning for monitoring transactions effectively as well as ensuring proper storage of customer information and enhancing payment processes - particularly when considering their descending order: improving payment process.

Table 1.5 Frequency on X-way Forensic

S/N	X-way Forensic	SA	A	U	D	SD	TOTAL
1	We use X-way forensic to extract digital investigation from digital devices.	26 (36.6%)	34 (47.9%)	11 (15.5%)	0 (0%)	0 (0%)	71 (100%)
2	We use X-way forensic to offer flexible reporting options to document and present findings.	17 (23.9%)	40 (56.3%)	14 (19.7%)	0 (0%)	0 (0%)	71 (100%)
3	We use X-way forensic to extract uncover hidden information and detect malicious activity.	27 (38.0%)	32 (45.1%)	12 (16.9%)	0 (0%)	0 (0%)	71 (100%)

Source: Field Survey Results (2023)

The findings of the survey revealed that there was a moderate level of agreement among respondents regarding the use of X-way forensic for extracting digital investigations from digital devices.

In response to Statement 1, a total of 26 respondents (36.6%) agreed, while 34 respondents (47.9%) strongly agreed. A smaller group of 11 respondents (15.5%) remained undecided, with no respondent expressing disagreement or strong disagreement.

According to the data, it is evident that a significant majority (84.5%) either agreed or strongly agreed with the use of X-way forensics for extracting digital investigations from digital devices. Among the respondents, 47.9% strongly agreed, and 36.6% simply agreed with this statement. A smaller proportion of participants (15.5%) remained uncertain about their stance, while none expressed any form of disagreement.

Moving on to Statement 2, which focuses on the utilization of X-way forensics for offering flexible reporting options to document and present findings, the participants also demonstrated a notable degree of consensus.

Out of all those who responded, 17 individuals (23.9%) agreed with this statement, while an even larger number - 40 participants (56.3%) - strongly agreed with it. Similarly, to before, there were some who were undecided about this matter - specifically 14 individuals (19.7%). However, just like in Statement 1's case; no one disagreed or strongly disagreed.

In terms of flexible reporting options provided by X-way forensic software; an overwhelming majority (80%) either agreed or strongly agreed that this feature existed and was utilized effectively by users within their organization.
Among the participants who responded; a staggering amount - specifically; (56%) - expressed strong agreement towards this notion whereas another sizable portion (23%) simply stated they agree with it. The remaining percentage (19.7%) claimed indecisiveness but no participants expressed disagreement or strong disagreement in regards to this matter.
The survey results revealed that a large majority of respondents (83.1%) either agreed or strongly agreed with the notion that X-way forensics is utilized to uncover hidden information and detect malicious activity. Among the participants, 45.1% strongly agreed, while 38.0% simply agreed with this statement. A smaller portion (16.9%) remained undecided, and there were no respondents who disagreed or strongly disagreed.
In summary, the detailed analysis of the data indicates that a considerable amount of participants held a positive view for x-way forensic in digital investigations. They believe that this method allows for the extraction of valuable information from digital devices, provides flexible reporting options, and aids in uncovering hidden information and detecting malicious activity. The high agreement percentages suggest that X-way forensic is widely regarded as a valuable tool in these domains.
However, it is important to note that there are varying levels of agreement or disagreement among respondents when it comes to the usefulness and effectiveness of X-way forensics in different areas. Despite some consensus on certain aspects, a considerable portion remains undecided or expresses disagreement regarding its application in these contexts. This suggests potential variations in experiences or perceptions among the participants on this particular matter.

Preliminary Analysis

It is imperative to conduct preliminary research before applying the well-known structural equation modelling (Hair et al., 2014). Screening of data for missing values, outlier detection, data normality, multicollinearity, nonresponse bias and common method bias was something I conducted. Details are presented below.

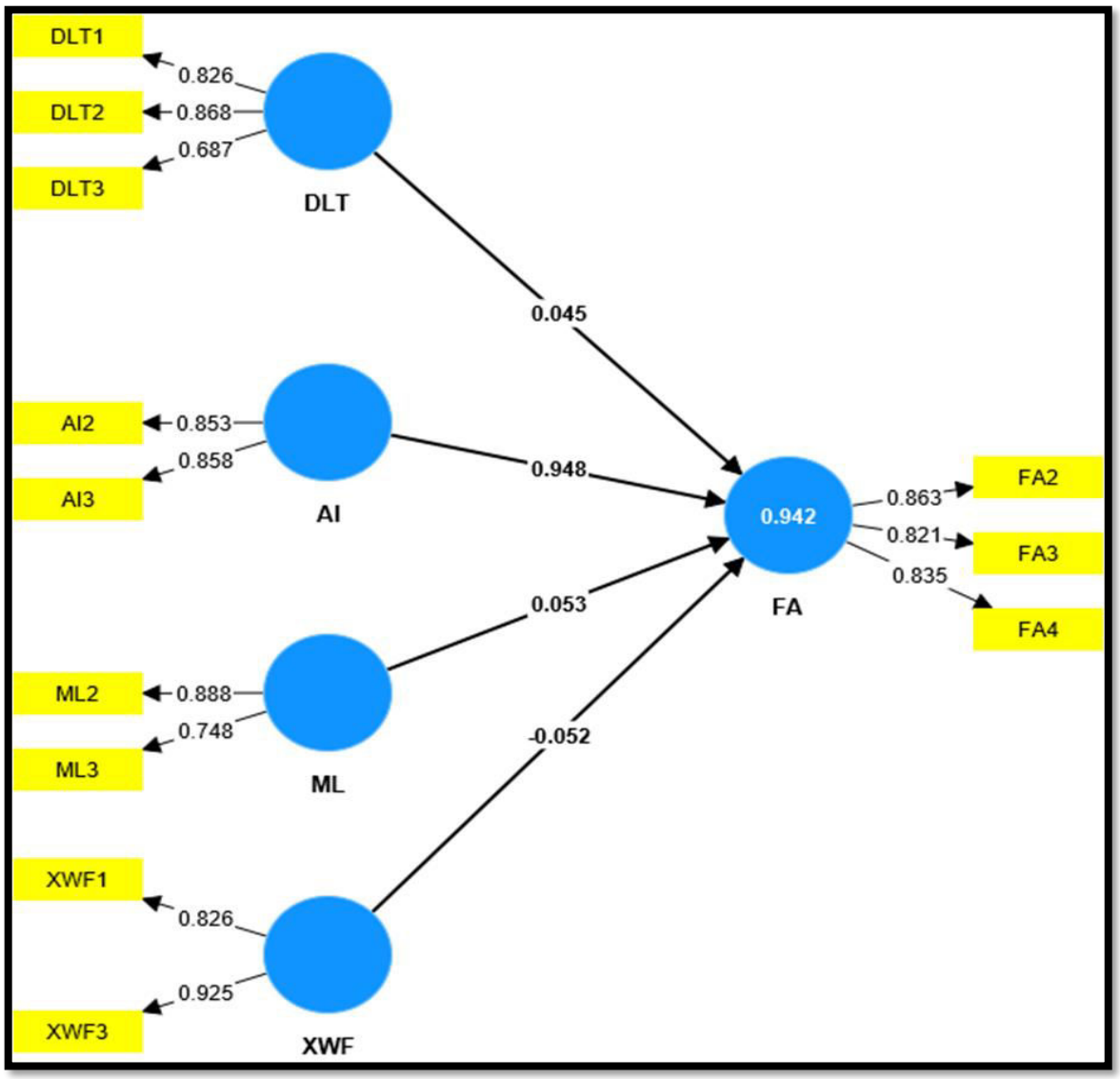
4.5.1 Missing Values

A common challenge faced by data analysts is missing data (Tabachnick&Fidell, 2013). It is crucial to ensure that the data set is complete without any missing values. According to Hair et al. (2014), researchers suggest a threshold of 10% for missing values, yet the data collected from the field in this instance contains no missing values.

Normality Test

The data were also assessed for normality, which is crucial to ensure that the collected data exhibit a normal distribution. Normality was evaluated using skewness and kurtosis statistics. Kurtosis indicates how peaked or flat a distribution is relative to a normal distribution (Hair et al., 2014), while skewness measures the symmetry of the distribution (Tabachnick&Fidell, 2013). According to the results shown in Table 4.2, the variables in the study fall within the ±1.96 range, which is the most commonly used threshold (Hair et al., 2014). Consequently, the data demonstrated some normality.

Result of Data on PLS-SEM



Source: The Research ran PLS-SEM

Fig 1.1

Table 1.6 Construct Reliability and Validity

Construct	Items	F-Loading	AVE	CR
Distributed ledger Technology	DLT1 DLT2 DLT3	0.826 0.868 0.687	0.636	0.838
Artificial Intelligence	AI2 AI3	0.853 0.858	0.731	0.845
Machine Learning	ML2 ML 3	0.888 0.748	0.674	0.804
X-ways forensic	XWF1 XWF3	0.826 0.925	0.769	0.869

Note: μ<0.7 The data were removed as a result of insufficient loadings. AVE stands for Average Variance Extracted, and CR is the abbreviation for Composite Reliability.

In the table above, all constructs have a Cronbach's Alpha coefficient above 0.7, except for AI1, ML1, XWF2, and FA1, which have coefficients below 0.7. Garson (2016) notes that Cronbach's alpha can be biased against short scales with only two items, as seen with the variables mentioned. However, Garson (2016) suggests this can be overlooked for a single construct. Hair et al. (2014) similarly state that a construct with a Cronbach's Alpha below 0.7 can be disregarded if other constructs in the model have coefficients above 0.7. All constructs met the minimum benchmarks for composite reliability and AVE, which are 0.7 and 0.5, respectively. Despite Fornell&Larcker's (1981) recommendation to reject constructs with a Cronbach's Alpha below 0.6, Garson (2016) advises using a threshold of 0.7.
The loading process should not be lower than 0.7 (Hair et al., 2014). In the table above, all things that measure the modern forensic technology and fraud management loaded well, as they loaded above 0.7. As a result, all items measuring the modern forensic technology and fraud management were retained. On the other hand, variables under artificial intelligence 1, machine learning 1, X-way forensic 2 and forensic awareness 1 loaded < 0.7, therefore were deleted, while other variables loaded > 0.7

Table 1.7 *Discriminant Validity using Heterotrait and Monotrait (n=71)*

	AI	**DLT**	**FA**	**ML**	**XWF**
AI					
DLT	**0.318**				
FM	1.357	**0.310**			
ML	0.504	0.303	**0.485**		
XWF	0.160	0.440	0.132	**0.576**	***

Note: The highlighted diagonal values reflect the square root of each latent construct's AVE.

The following table shows the outcome of discriminant validity. The numbers that are bolded indicate the square root of AVE for each latent variable. The AVE of distributed ledger technology is 0.318. Similarly, fraud awareness, the AVE is 0.310. Likewise, for the machine learning with AVE coefficient of 0.485. Finally, X-ways forensic having AVE coefficient of 0.576. According to the Heterotrait and Monotrait discriminant validity criteria, the data is discriminant (Garson, 2016). To this stage, the data has been tested for factor loadings, convergent validity, and discriminant validity, and it has passed all tests.

Test of Hypotheses for Direct Relationships

It is important to determine the direct effect of modern forensic technology on fraud management in Nigeria. This will help test hypotheses. Thus, it's presented below.

Table 1.8

Original Sample (O)	**Beta**	**Standard Deviation (STDEV)**	**T Statistics**	**P-Values**	**Label**
AI->FA	0.948	0.946	0.017	0.000	Accepted
DLT->FA	0.045	0.040	0.032	0.168	Rejected
ML->FA	0.053	0.048	0.032	0.102	Rejected
XWF->FA	-0.052	-0.038	0.044	0.238	Rejected

Direct Path Coefficient

From above, it can be deduced that artificial intelligence toward the fraud awareness has a positive effect on fraud management, significant at P value <.0.000. This means a unit change in artificial intelligence will lead to 17. % change in the fraud awareness. As a result, the null hypothesis (H_0) that states there is no significant effect on modern forensic technology on fraud awareness among international authorized banks in Nigeria is rejected.

But, distributed ledger technology has no positive significant value on fraud awareness at P value > our alpha (0.05). This means a unit change in distributed ledger technology will lead to 32. %. Thus, H_0 that states there is no significant effect on modern forensic technology on fraud awareness among international authorized banks in Nigeria is supported.

Similarly, machine learning has no positive significant value on fraud awareness at P value > our alpha (0.05). This means a unit change in machine learning will lead to 32. %.

And finally, X-ways forensic has no positive significant value on fraud awareness at P value > our alpha (0.05). This means a unit change in distributed ledger technology will lead to 44. %.

Table 1.9

	R-Square R^2	**R-Square Adjusted**
FM	0.942	0.938

Adjusted R square is 93%, meaning 93% variance in fraud awareness is been explained by the variation in AI, DLT, ML, XWF while the remaining 7% are the variable that are not explained in this work. This thus establish, that there exists a direct relationship between artificial intelligence and fraud awareness.

Conclusion

This study examines the impact of innovative forensic technology and management, particularly artificial intelligence (AI), on fraud management in Nigerian commercial banks. Economic crimes, especially recent corruption and white-collar crimes, have led to corporate collapses, making forensic accounting crucial. AI-powered systems offer real-time analysis of vast data, identifying fraudulent patterns and anomalies swiftly. Advanced machine learning, predictive analytics, and customer behavior monitoring help mitigate risks. AI-driven authentication methods, such as biometric identification, enhance security and reduce identity theft. Collaboration with cybersecurity firms and data sharing foster robust AI models and comprehensive prevention strategies. Regular updates and employee training ensure effective use of AI tools. Ethical considerations and regulatory compliance are essential for transparency and data protection. The study highlights AI's potential to revolutionize fraud management, improve customer trust, and mitigate financial risks in Nigerian banks.

References

1. *Abdulrahman, S. (2019). Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper. International Journal of Accounting & Finance Review, 4(2), 13-21.*
2. *Adeniran, T. A. M., Muftau A. Ijaiya, Damilola S. (2017). Fraud And Bank Performance Nexus.Evidence From Nigeria Using Vector Error Correction Model.J.Bus.Finance, 3(1).*
3. *Adesina, K., Erin, O., Ajetunmobi, O., Ilogho, S., &Asiriuwa, O. (2020a). Does forensic audit influence fraud control? Evidence from Nigerian deposit money banks.Banks and Bank Systems, 15(2), 214–229.*
4. *Adesina, K., Erin, O., Ajetunmobi, O., Ilogho, S., &Asiriuwa, O. (2020b). Does forensic audit influence fraud control? Evidence from Nigerian deposit money banks.Banks and Bank Systems, 15(2), 214–229.*
5. *AICPA. (2010). FVS Practice Aid 10-1: Serving as an Expert Witness or Consultant. New York: American Institute of Certified Public Accountants.*
6. *Akande, Folorunso&Egwakhe, Johnson & Benjamin, R. &Umukoro, Jones. (2024). Fraud And Financial Performance Of Banks In Nigeria. Fraud And Financial Performance Of Banks In Nigeria. 30. 10.53555/kuey.v30i5.1249.*
7. *Ayorinde, A. O., Toyin, A., &Leye, A. (2013). International Journal of Management Sciences and Business Research, 2013, ISSN (2226-8235) vol-2, issue 9. International Journal of Management Sciences and Business Research, 2(9).*
8. *B.V., P. (2016). Cyber Forensic Technology: A Review. International Journal of Engineering Trends and Technology (IJETT), 41(5).*
9. *Babarinde, Gbenga&Onwumere, Josaphat&Idera, Abdulmajeed. (2024). Bank Fraud and its Impact on Deposit Mobilisation: The Case of Nigerian Deposit Money Banks.*
10. *Bassey, B., Eyo, B., Ahonkhai, A., &Ebahi, O. (2017).Effect of forensic accounting and litigation support on fraud detection of banks in Nigeria.IOSR Journal of Business and Management, 19(06), 56–60.*
11. *Bhasin, M.L. (2007), Forensic Accounting and Auditing – Perspectives and Prospects, Accounting world magazine, www.iupindia.in.*
12. *Bondaruk, T. &Bohrinovtseva, L. &Bondaruk, O.. (2023). Fraud Using Bank Payment Cards: A Way for Financing of Terrorism and Separatism. Statistics of Ukraine. 101.*
13. *Bushman, M. R. 7 Smith, J.A. (2003). Transparency, Financial Accounting Information, and Corporate Governance" FRBNY Economic Policy Review forthcoming.Centre for Forensic Studies (2010): Nigerian Institute of Advanced Legal Studies Lagos, Nigeria Roundtable on the Role of Forensic and Investigative Accounting: Challenges For the Banking Industry 19th July, 2010.*

14. *Choo, K. K. R., Smith, R. G., McCusker, R., &Choo, K. K. R. (2007). Future directions in technology-enabled crime: 2007-09. Canberra: Australian Institute of Criminology.*
15. *Clark-Carter, D. (2004). Quantitative psychological research: A student's handbook. Hove: UK: Psychology Press. www.brookings.edu .*
16. *Cotton, M.P. (2000). Corporate Fraud Prevention, Detection and Investigation: A practical Guide of Dealing with Corporate Fraud, Australia: Price water house coopers*
17. *Crumbley, D. L (2003) "What is Forensic Accounting". Retrieved ON 24TH March from: www.edwardspub.com.*
18. *Crumbley, D. L (2006): Forensic Accountants Appearing in the literature. Retrieved on March 23, 2012 from www.forensicaccounting.com.*
19. *Crumbley, D. L. (2001) Forensic Accounting: Older than you think, JFA, 2 (2) 181*
20. *Crumbley, D. L. (2009). So What Is Forensic Accounting? The ABO Reporter Fall (9)*
21. *Deepika, B. (2014). Forensic Technology used in Digital Crime Investigation Forensic Service. Forensic Science,4(5).*
22. *Degboro, D. and J. Olofinsola, 2007. Forensic accountants and the litigation support engagement. Niger. Account., 40(2): 49-52*
23. *Dhar, P. and A. Sarkar, (2010). Forensic accounting: An Accountant's Vision. Vidyasagar University Journal of Commerce, 15(3): 93-104.*
24. *Electronic fraud and performance of deposit money banks in Nigeria: 2008-2018. International Journal of Business and Management, 15(6), 126.*
25. *EmekaNwobia, C., AnayojAdigwe, P., KasieEzu, G., &NonsoOkoye, J. (2020a).*
26. *EmekaNwobia, C., AnayoAdigwe, P., KasieEzu, G., &NonsoOkoye, J. (2020b). Electronic fraud and performance of deposit money banks in Nigeria: 2008-2018. International Journal of Business and Management, 15(6), 126.*
27. *Emmanuel, O., Prof.., &Nwoka, N., Ee. (2019). Forensic Accounting and Fraud Prevention in Manufacturing Companies in Nigeria.International Journal of Innovative Finance and Economics,7(1).*
28. *Enoch, Y. S., John, A. K., &Olumuyiwa, A. E. (2013).Mitigating Cyber Identity Fraud using Advanced Multi Anti-Phishing Technique.International Journal of Advanced Computer Science and Applications (IJACSA), 4(3), 156-164. Retrieved from: thesai.org.*
29. *Erick Oyier, O. (2013). The Impact Of Forensic Accounting Services On Fraud Detection And Prevention Among Commercial Banks In Kenya. International Journal of Management Sciences and Business Research, 7(13).*
30. *Ezejiofor, R. A., Nkiru Peace, N., & Jane, O., F. N. (2016). Impact Of Forensic Accounting On Combating Fraud In Nigerian Banking Industry.International Journal of Academic, 1(2).*

31. *Fabian C., O., Ph. D., J.K.J., O., Ph. D., &Oluranti, A, A. (2022).Forensic Accounting Services and its effect on Fraud Prevention in Health Care Firms in Nigeria.World Journal of Finance and Investment, 6(1).*
32. *Fornell, C., &Larcker, D. (1981).Evaluating structural equation modela with unobservable variables and measurement error.Journal of marketing research, 181(1), 39-50.*
33. *Garson, D. (2016). Partial Least Squares: Regression & Structural Equation Models. USA: Statistical Associates Publishing.*
34. *Gitau, E. W., & Samson, N. G. (2016). Effect of financial fraud on the performance of commercial banks: a case study of tier 1 banks in Nakuru town, Kenya. International Journal of Economics, Commerce and Management, 4(20), 142-157.*
35. *Govil, J., &Govil, J. (2007, May).Ramifications of cybercrime and suggestive preventive measures.2007 IEEE International Conference on Electro/Information Technology.*
36. *Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., &Ishfaq, M. (2022). Distributed ledger technology technology: benefits, challenges, applications, and integration of distributed ledger technology technology with cloud computing. Future Internet, 14(11), 341.*
37. *Hair, J., Black, W., Babin, B., & Anderson, R. (2014).Multivariate data analysis (7th ed.). UK: Pearson New International Edition.*
38. *Howard S. and Sheetz, M. (2006): Forensic Accounting and Fraud Investigation for non-Experts, New Jersey, John Wiley and Sons Inc*
39. *docplayer.net.*
40. *cointelegraph.com.*
41. *techcabal.com.*
42. *techpoint.africa.*
43. *www.hyperverge.co.*
44. *Izedonmi, F.I. &Mgbame, C.O. (2011).Curbing financial frauds in Nigeria, a case for forensic accounting. African Journal of humanities and society, 1(12), 52-56.*
45. *J. Inyada, S., Olopade, D. O., &Ugbede, J. (2019a). Effect of forensic audit on bank fraud in Nigeria.American International Journal of Contemporary Research, 9(2).*
46. *J. Inyada, S., Olopade, D. O., &Ugbede, J. (2019b). Effect of forensic audit on bank fraud in Nigeria.American International Journal of Contemporary Research, 9(2).*
47. *Joshi, M. S. (2003): "Definition of Forensic Accounting" www.forensicaccounting.com.*

    Joshi, P., Bremser, W., Hemalatha, J. and Al-Mudhaki, J. (2007), Non-audit services and auditor independence: empirical findings from Bahrain

,International Journal of Accounting, Auditing and Performance Evaluation, 4(1), pp. 57-89

48. *Kaur, B., Sood, K., &Grima, S. (2022). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. Journal of Financial Regulation and Compliance, 31(1), 60-95.*
49. *Kennedy, M. P., & J.O. Anyaduba, Dr. (2013). Forensic Accounting and Financial Fraud in Nigeria: An Empirical Approach. International Journal of Business and Social Science, 4(7).*
50. *Lee, K., & Chen, S. (2013). Introduction to partial least square: Common criteria and practical considerations. Advanced Materials Research, 1766-1769. www.scientific.net.*
51. *Manyo, Takon& Walter, Mboto& Obo, Ekpenyong&Wonah, Ogar&Omang, Bekom&Ekpo, Nkamare&Emefiele, &Chike, Charles. (2023). Effect of Fraud on Commercial Banks' Performance in Nigeria. 2. 69-78.*
52. *Manyo, Takon& Walter, Mboto& Obo, Ekpenyong&Wonah, Ogar&Omang, Bekom&Ekpo, Nkamare&Emefiele, &Chike, Charles. (2023). Effect of Fraud on Commercial Banks' Performance in Nigeria. 2. 69-78.*
53. *Mohamed, I. (2020). Exploring The Role Of Forensic Accounting In Law Enforcement A Case Study From The UK.International Journal of Psychosocial Rehabilitation, 24(06).*
54. *Musa, Dumbulu&Enock, Zikusooka& University, Metropolitan. (2024). A Study On*
55. *(Ms.C), Dr. A. O. E. A. U.; E. J. D. (Ms. C., Mr. (n.d.).The Role Of Forensic Accounting In Mitigating Financial Crimes.*
56. *Examining Internal Audit Practices On Fraud Management In Organizations, A Case Study Of Centenary Bank. 3. 169-175.*
57. *Niyi, O. (2021). Forensic Accounting as a Tool for Fraud Detection and Prevention in Public Sector: Moderating on MDAs. International Business Management, 15(1).*
58. *O.J, A. (2021).Examination of fraud in the Nigerian banking sector and its prevention.Asian Journal of Management Research,3(01).*
59. *O.J., A. (2021). Examination of fraud in the Nigerian banking sector and its prevention.Asian Journal of Management Research,3(6).*
60. *Ojaide, F. (2000). Fraud detection and prevention: the case of pension accounts ICAN NEWS January/March.*
61. *Okoye, E.I. &Akamobi, N.L. (2009). The role of forensic accounting in fraud investigations and litigation support.The Nigerian Academic Forum 17 (1).*
62. *Owojori, A.A. &Asaolu T.O. (2009).The role of forensic accounting in solving the vexed problem of corporate world. European Journal of Scientific Research.29 (2), 183-187*

63. Ojaide.(2013). Forensic evidence and crime scene investigation.Journal of Forensic Investigation, 01(02).
64. Ojianwuna, Chukwuekwu. (2024). Fraud and Performance of Listed Deposit Money Banks in Nigeria: Exploring the Combined Effects of Fraud Triangle and Fraud Diamond Theories. Journal of Business and Econometrics Studies.1-8. 10.61440/JBES.2024.v1.27.
65. Okoye E.I and Akamobi N.L (2009): The Role of Forensic Accounting in Fraud Investigation and Litigation Support. The Nigerian Academic Forum Vol 17 No1.
66. Okpara, G. C. (2009), "Bank failure and persistent distress in Nigeria: a discriminant Analysis". Nigerian Journal of Economic and Financial Research.2(1).
67. Okunbor.J.A and Obaretin. O (2010): Effectiveness of the Application of Forensic Accounting Services in Nigerian Corporate Organisations. AAU JMS Vol. 1, No. 1.
68. Olorunsegun, S. (2010). The impact of electronic banking in Nigeria banking system: Critical appraisal of Unity Bank PLC. Unpublished MBA project, LadokeAkintola University of Technology, Ogbomoso, Oyo State Nigeria
69. Olurotimi, O. N. O. and A. S. (2021). Forensic accounting as a tool for fraud detection and prevention in public sector: Moderating on mdas. International Business Management, 15(1).
70. Osuagwu, P., &Umeh, J. (2018). Rising wave of e-frauds puts economy at risk. Retrieved from www.vanguardngr.com.
71. Rezaee, Z, Crumbley, D. L and Elmore, R C (2006): Forensic Accounting Education: A Survey of Academicians and Practitioners. Advances in Accounting Education, Forthcoming. Available at SSRN: ssrn.com.
72. Skousen, C.J. and C.J. Wright.(2008). Contemporaneous risk factors and the prediction of Financial statement fraud.Journal of Forensic Accounting, 9: 37-62
73. Success Ikechi, K., & Anthony, N. (2020). Fraud theories and white collar crimes: Lessons for the Nigerian banking industry. International Journal Of Management Science And Business Administration, 6(6), 25–40.
74. Tabachnick, B.G., &Fidell, L.S. (2013).Using multivariate statistics (5th ed.). Boston: Pearson.
75. Udegbunam, R. I. (1998), "Bank Failure in Nigeria since Deregulation: Underlying Causes and Implication for Policy". Benin Journal of Social Sciences, Volume 6 & 8, No. 1 & 2.
76. Urbach, N., &Ahlemann, F. (2010).Structural equation modeling in information systems research using partial least squares.Journal of Information Technology Theory, 11(2), 5–40. Retrieved from aisel.aisnet.org.
77. Wallace, A. (1991): The Role of the Forensic Accountant. Retrieved on 20th march from: www.ssrn.com.

78. *Williams, Harley &Adeyanju, David. (2021). The Impact of Fraud on Financial Performance of Deposit Money Banks: Evidence from Nigeria. Sumerianz Journal of Business Management and Marketing. 4. 12-16.*
79. *Wisdom, O., OlamideOgunleye, O., &Ibidunni, O. M. (2018).Forensic accounting and fraud prevention and detection in Nigerian banking industry introduction.COJ Reviews and Research, 1(1).*
80. *Yiye, J., Mustapha, R., Ahmad, A. M., &Bassi, H. (2022).Digital Forensic Investigation of Cyberstalking and Social Media Harassment using Network Forensic Analysis.Journal of Science Technology and Education, 10(3).*
81. *Zawoad, S., &Hasan, R. (2015, June).FAIoT: Towards building a forensics aware eco system for the internet of things. 2015 IEEE International Conference on Services Computing.objects.scraper.bibcitation.com.*
82. *Zhang, M. (2022). Forensic imaging: A powerful tool in modern forensic investigation. Forensic Sciences Research, 7(3), 385–392.*
83. *Zysman, A. (2004), "Forensic Accounting Demystified", world investigators network Standard practice for investigative and forensic accounting engagements, Canadian Institute of Chartered Accountant, Nov 2006*