MRS Journal of Multidisciplinary Research and Studies
Abbreviate Title- MRS J Mul Res Stud
ISSN *(Online) 3049-1398*
Vol-2, Iss-3(March-2025)

EFFECT OF FORENSIC ACCOUNTING TECHNIQUES ON CYBERCRIME DETECTION AMONG LISTED DEPOSIT MONEY BANKS IN NIGERIA

Blessing Ejura Success[1*], Success Jibrin Musa[2], Ibrahim Karimu Moses[3]

[*1-3] Department of Finance, Veritas University Abuja

[2] Department of Accounting, Veritas University Abuja

[3]Department of Accounting, Confluence University of Science and Technology, Osara, Kogi State

Corresponding Author Blessing Ejura Success

Department of Finance, Veritas University Abuja

Article History

Received: 03 / 03 / 2025

Accepted: 20 / 03 / 2025

Published: 23 / 03 / 2025

Abstract: Cybercrime has become a growing concern in Nigeria's banking sector, with increasing incidents of phishing, data breaches, and online fraud threatening financial stability and customer trust. As banks digitize operations, the need for robust detection mechanisms becomes more urgent. Forensic accounting techniques such as Computer-Assisted Audit Tools (CAATs), digital forensics, and structured forensic investigation procedures have emerged as valuable tools in combating these evolving threats. The main objective of this study is to examine the effect of forensic accounting techniques on cybercrime detection among listed deposit money banks in Nigeria. Specifically, it investigates the roles of CAATs, digital forensic tools, and forensic investigation methods in curbing cyber-related financial crimes. The study adopts a survey research design. Primary data were collected from staff and management of ten purposively selected listed banks using structured questionnaires. The data were analyzed using both descriptive statistics and inferential methods, including correlation and regression analysis. Findings reveal that all three forensic accounting techniques have significant positive effects on cybercrime detection, with digital forensic tools having the strongest impact. The results confirm that forensic accounting enhances cybercrime prevention through proactive detection, evidence gathering, and system monitoring. Based on these findings, the study recommends that banks invest in advanced digital forensic infrastructure, strengthen cybercrime tracking systems, and institutionalize internal forensic investigation protocols. These efforts will help reduce cyber-related risks and improve the resilience of Nigeria's financial system.

Keywords: *Forensic Accounting Techniques, Cybercrime Detection.*

Cite this article: Success, B. E., Musa, S., J. & Ibrahim, K. M. (2025)**.** EFFECT OF FORENSIC ACCOUNTING TECHNIQUES ON CYBERCRIME DETECTION AMONG LISTED DEPOSIT MONEY BANKS IN NIGERIA. *MRS Journal of Multidisciplinary Research and Studies, 2 (3),54-65*

Introduction

In the digital age, the proliferation of cybercrime has become a critical concern for financial institutions globally. The banking sector, being heavily digitized and data-driven, is particularly susceptible to cyber threats such as phishing, malware attacks, identity theft, and unauthorized access to sensitive financial information. In Nigeria, the situation is alarming. According to the Nigerian Inter-Bank Settlement System (NIBSS, 2023), the banking sector lost over ₦14 billion to cyber fraud in 2022 alone. This growing threat landscape underscores the urgent need for advanced detection and prevention mechanisms.

Forensic accounting techniques encompassing tools such as Computer-Assisted Audit Techniques (CAATs), digital data mining, forensic data analytics, blockchain auditing, and fraud risk assessment—have gained prominence as potent mechanisms for detecting, investigating, and preventing financial and cyber-related crimes. These techniques combine investigative accounting skills with modern technological tools to unveil anomalies and trace digital footprints, making them invaluable in the context of cybercrime detection (ACFE, 2022; Enofe et al., 2013).

Globally, forensic accounting has evolved beyond traditional auditing functions to integrate digital forensics in response to cyber threats. Studies by Albrecht et al. (2020) and Modugu and Anyaduba (2013) have shown that forensic accounting practices can enhance fraud detection capacities, improve organizational transparency, and support regulatory compliance. In Africa, and particularly Nigeria, there is increasing scholarly interest in applying forensic tools to mitigate financial crimes, yet much of the literature remains skewed toward traditional fraud in public sector accounting, payroll manipulation, and procurement irregularities, with relatively limited focus on cybercrime in the banking sector.

Empirical studies have examined the role of forensic accounting in financial crime detection (Akinbowale et al., 2020; Owojori & Asaolu, 2009 (Ibrahim, & Musa, 2022, Ibrahim, & Musa, 2022,Ibrahim, & Musa, 2022, Ibrahim, et al., 2022, Moses, et al 2022, Moses, et al., 2018, Ejura, et al. 2023 & Oginni, et al.2014 Ejura, et al, 2023, Moses, et al 2022, Haruna, et al 2021, Moses, et al 2018, Abdul, et al 2025 John, et al 2024, Ibrahim, et al 2022 Jibrin, et al 2022 Roselyn et al 2021) Badaru, & Moses,2025, Chamba, et al 2024, Ibrahim, et al 2024, Ejura, et al 2023, Musa, et al 2015 Jibrin, et al 201, Musa, et al 2022, Jibrin,et al 2015, Musa, et al 2013 Musa, et al 2013, Ifurueze, et al 2012, Musa, et al 2022 Hussain, et al 2024, Musa, & Moses, 2022, Tsegba, et al 2021 & Musa, (2022, Jibrin, et al 2016, Jibrin, et al 2016), but only a few have extended the analysis to cybercrime-specific scenarios within commercial banking institutions. Moreover, most existing research employs generalized methodologies and fails to distinguish between cyber-related fraud and traditional financial crimes, thus creating a methodological and variable gap. There is also a geographical gap, as many studies are concentrated in southern Nigeria or are based on public sector contexts, neglecting the dynamics within listed deposit money banks in Nigeria's commercial hubs such as Lagos, Abuja, and Port Harcourt.

Furthermore, theoretical lenses such as the Fraud Triangle Theory and Routine Activity Theory have been underutilized in framing the cybercrime detection role of forensic accounting. This presents a theoretical gap, limiting the explanatory depth of existing studies. Additionally, the rapid digitization of banking operations calls for updated research that reflects recent technological advances in forensic tools, such as artificial intelligence in auditing and blockchain-based evidence tracking, which are scarcely addressed in Nigerian banking studies (Popoola et al., 2022; Oladimeji & Bello, 2023).

Cybercrime refers to illegal or unauthorized activities carried out through the use of computers, digital networks, or electronic devices. These crimes often involve unauthorized access to systems, interception of data, intellectual property theft, fraud, and deliberate disruption of digital networks. As Slavin (2020) notes, cybercrimes are typically committed using the internet and include offenses such as phishing, credit card fraud, online banking theft, money laundering, and ATM-related scams. Essentially, cybercrime encompasses a wide range of criminal activities where computers are either the target or the means of committing the offense.

In Nigeria's banking sector, there has been a growing reliance on forensic accounting as a strategic response to the rise in cybercrime. Forensic accounting is seen as a powerful tool to help prevent, detect, and investigate digital financial crimes (Thankaraja & Somasundaram, 2019). These techniques involve specialized investigative approaches used by forensic accountants to trace financial irregularities and gather evidence, often for use in legal proceedings. The process typically includes applying accounting knowledge alongside technological tools to track suspicious transactions and uncover hidden fraud.

To tackle cybercrime more effectively, digital forensic tools are often deployed. According to Musa (2019), these tools enable forensic experts to collect, examine, and analyze electronic data, making it easier to identify fraudulent activities. With digital tools, forensic accountants can retrieve crucial evidence, investigate anomalies, and build cases against cybercriminals (Gutmann, 1996). Given these developments, this study aims to explore how forensic accounting techniques can influence the prevention and detection of cybercrime in the banking sector, with a particular focus on listed deposit money banks operating in Ondo State.

Cybercrime remains one of the most pressing challenges in Nigeria's financial industry. Its impact extends beyond financial loss it undermines the confidence of customers and hinders the growth and performance of banks (Awoyemi et al., 2021). Albrecht (2016) emphasized that cybercrime significantly disrupts the progress of e-business and deters participation in digital transactions. Similarly, Bello (2020) observed that recurring cybercrime incidents have led to substantial financial losses for banks, contributing to their operational setbacks. Ile and Odimmega (2018) added that one of the more serious consequences of cybercrime is the erosion of public trust in the banking system.

Despite the potential of forensic accounting, Akinbowale, et al (2017) noted that the lack of a structured implementation framework has limited its effectiveness in combating cybercrime in Nigeria. Moreover, while digital forensic tools have shown promise, Musa (2019) highlighted that their effective use is often constrained by a lack of technical expertise. Olatunji and Aruwaji (2020) also found that although forensic accounting can significantly influence the detection of financial cybercrimes, poor capacity and limited resources among law enforcement agencies remain critical obstacles. Kuruti (2020) reinforced this view, stressing that while forensic accounting offers a reliable means to curb digital crimes, enforcement remains weak and inconsistent.

Problem Statement

Despite the growing global reliance on digital forensic tools to combat cyber-related offenses, the effectiveness of forensic accounting techniques in detecting cybercrime particularly within Nigeria's listed deposit money banks remains inadequately explored. Existing literature has predominantly focused on conventional fraud types such as embezzlement, procurement fraud, and payroll manipulation (Modugu & Anyaduba, 2013; Enofe et al., 2013), often within public sector institutions. However, cybercrime is a rapidly evolving and technically complex threat that requires equally sophisticated detection mechanisms yet scholarly attention in this context remains limited.

Many studies assess forensic accounting's general role in fraud detection without differentiating specific forensic techniques such as Computer-Assisted Audit Tools (CAATs), blockchain audit trails, digital forensic analytics, and data mining as distinct tools applicable to cybercrime. For instance, Akinbowale et al. (2020) and Bello (2020) evaluated the use of forensic auditing in curbing financial fraud but did not dissect its impact on cybercrime incidents, which involve different dynamics such as network intrusion, data breaches, and cyber laundering. There is, therefore, a pressing need to evaluate how individual forensic accounting techniques contribute specifically to cybercrime detection in commercial banks, as opposed to general financial crimes.

Another critical gap lies in the methodological approach adopted in existing studies. Many prior investigations rely heavily on qualitative interviews or descriptive analysis (Owojori & Asaolu, 2009; Kuruti, 2020), with limited application of empirical

or inferential statistical methods to validate the relationship between forensic accounting techniques and cybercrime detection outcomes. This study addresses this gap by employing quantitative methods, such as regression analysis, to measure the extent to which various forensic tools (e.g., CAATs, forensic analytics) influence cybercrime detection rates in Nigerian banks.

A considerable portion of Nigerian forensic accounting literature centers on public organizations (MDAs, state-owned enterprises) or microfinance banks, leaving listed deposit money banks relatively under-studied (Adebayo & Onuoha, 2023; Adegbie & Fakile, 2012, Ibrahim, & Musa, 2022, Ibrahim, & Musa, 2022, Ibrahim, & Musa, 2022, Ibrahim, et al., 2022, Moses, et al 2022, Moses, et al., 2018, Ejura, et al. 2023 Oginni, et al.2014). These listed banks, however, are highly digitized, operate complex IT systems, and process millions of daily transactions making them prime targets for cybercriminals. This study, therefore, extends the scope of investigation to include all listed deposit money banks on the Nigerian Exchange Group (NGX), thereby filling a notable institutional gap.

In terms of theoretical grounding, many Nigerian studies lack alignment with cybercrime-specific theories that explain the behavioral and systemic factors behind digital criminality. The Routine Activity Theory (Cohen & Felson, 1979), which posits that crime occurs when a motivated offender meets a suitable target without a capable guardian, offers a suitable lens to understand how banks become vulnerable to cyberattacks. Forensic accounting tools, in this regard, can be conceptualized as "capable guardians" that deter or detect such offenses. Embedding this theory in the study enhances the analytical rigor and provides a stronger basis for policy implications.

Most Nigerian studies are regionally limited often focusing on Lagos State, Abuja, or one geopolitical zone thereby limiting generalizability across the country (Olatunji & Aruwaji, 2020; Ile & Odimmega, 2018). Yet cybercrime is a national issue affecting banks across all regions. This study bridges this gap by collecting data from forensic accounting units and IT departments of listed banks operating nationwide, ensuring broader and more representative insights that can inform sector-wide policy reforms.

This study is uniquely positioned to contribute to both academic literature and practical policy by addressing these intertwined gaps variable, methodological, scope, theoretical, and geographical. It draws from current empirical research, applies robust statistical methods, and integrates relevant criminological theory to assess the real-world impact of forensic accounting techniques on cybercrime detection in Nigeria's banking sector.

Objective of Study

The main objective of this study is to examine the effect of forensic accounting techniques on Cyber-crime detection among listed deposit money bank in Nigeria. The specific objective is to:

i. determine the effect of Computer Assisted Auditing Tools (CAATs) on prevention of cyber-crime in listed deposit money banks in Nigeria,
ii. examine the effect of digital forensic tools on prevention of cyber-crime in listed deposit money banks in Nigeria and
iii. assess the effect of forensic investigation techniques on prevention of cyber-crime in listed deposit money banks in Nigeria.

The following research hypotheses were developed to properly address the problems of the study. These hypotheses were stated in null form as follows:

- **H_{01}:** There is no significant relationship between Computer Assisted Auditing Tools (CAATs) and cyber-crime prevention in listed deposit money banks in Nigeria,
- **H_{02}:** There is no significant relationship between digital forensic tools and cyber-crime prevention in listed deposit money banks in Nigeria and
- **H_{03}:** There is no significant relationship between forensic investigation techniques and cyber-crime prevention in listed deposit money banks in Nigeria.

Literature Review

Cybercrime Detection

The concept of cybercrime continues to evolve rapidly, shaped by both technological advancement and legal complexities. One of the major challenges in this area of study is the lack of a universally agreed-upon definition. As Yar (2015) aptly notes, cybercrime is a dynamic term influenced by jurisdictional, cultural, and technological differences, which complicates its classification and regulation. Smith et al. (2014) add that defining cybercrime often raises conceptual challenges, especially when trying to encompass both direct attacks on information systems such as hacking and malware and crimes committed using digital platforms, such as online fraud or identity theft.

Over time, scholars and institutions have adopted a variety of terminologies to describe these offenses. These include computer crime (Maat, 2004), digital crime, internet crime (Wall, 2015), virtual crime (Lastowka & Hunter, 2004; Grabosky, 2001), e-crime (AIC, 2016), and net crime (Mann & Sutton, 1998). This terminological variety highlights the complex and expansive nature of cybercrime, which Gurjar et al. (2015) argue should be treated as an umbrella term covering a broad spectrum of illicit activities committed using or targeting information technology systems.

According to the Australian Institute of Criminology (2016) and UNODC (2020), cybercrime can be broadly grouped into four categories. Offenses against computer systems and data integrity, such as unauthorized access, system interference, and malware distribution. Computer-related crimes, including online financial fraud, cyber money laundering, and e-commerce scams. Content-related offenses, such as cyberbullying, online harassment, and the distribution of illegal or harmful content. Intellectual property and copyright violations, including software piracy and illegal content sharing. These categories underscore the breadth of the cybercrime landscape, which demands equally diverse and evolving detection strategies.

Globally, the prevalence of cybercrime has escalated, particularly in the financial sector. The PwC Global Economic Crime and Fraud Survey (2022) reports that nearly half of the surveyed organizations experienced cybercrime, with phishing, ransomware, and business email compromise ranking among the most common threats. In Nigeria, the situation is equally alarming.

According to the Nigeria Inter-Bank Settlement System (NIBSS, 2023), Nigerian financial institutions lost over ₦14 billion to cyber-related fraud in 2022 alone, reinforcing the need for proactive and sophisticated detection mechanisms.

Cybercrime detection involves identifying, analyzing, and responding to suspicious digital activities using a combination of traditional auditing procedures and modern technological tools. Techniques such as Intrusion Detection Systems (IDS), forensic imaging, blockchain analysis, machine learning algorithms, and Computer-Assisted Audit Techniques (CAATs) are increasingly adopted to uncover irregularities in financial data (Choo, 2011; Albrecht et al., 2020). Moreover, the use of artificial intelligence and behavioral analytics is proving effective in flagging unusual transaction patterns, access anomalies, and suspicious login behaviors (Tiwari & Joshi, 2022; Bello, 2020).

Forensic Accounting

Forensic accounting is a specialized field that merges accounting, auditing, and investigative techniques to examine financial information suitable for legal review. The American Institute of Certified Public Accountants (AICPA, 2023) defines forensic accounting as the application of accounting principles, methods, and investigative procedures to resolve issues in actual or anticipated legal disputes. It entails uncovering, interpreting, and communicating complex financial data in a manner that supports litigation processes or organizational resolution.

Building on this, Umar (2020) emphasizes that forensic accounting plays both a preventive and detective role in fraud management. It is not only about identifying fraudulent acts after they have occurred but also establishing internal controls and red flags to reduce future occurrences. Oyedokun (2019) asserts that forensic accounting is a comprehensive process that begins with data interpretation and culminates in the expert presentation of findings, particularly in court or arbitration settings.

Computer-Assisted Audit Techniques (CAATs)

Computer-Assisted Audit Techniques (CAATs) are critical digital tools that allow forensic accountants to analyze large volumes of data efficiently. These tools are particularly useful in detecting abnormalities, tracing transaction histories, and identifying fraudulent activity embedded within massive datasets. CAATs support automation in forensic engagements by enabling high-speed data analysis, sampling, and exception reporting (Lowe & Bierstaker, 2019).

Roger et al. (2020) describe CAATs as indispensable digital resources utilized throughout various stages of forensic accounting from risk assessment and planning to fieldwork and reporting. In modern, tech-dependent organizations, forensic professionals can apply CAATs for data extraction, stratification, and pattern recognition. Uyar and Güngörmüş (2022) add that CAATs are increasingly valuable in fraud risk analytics, enabling auditors to flag irregular transactions in real-time and trace them back to their source.

Forensic Investigation Techniques

Forensic investigation techniques are structured approaches designed to identify, examine, and document financial irregularities. These techniques go beyond conventional audits by involving rigorous scrutiny of digital records, interview sessions with suspects or witnesses, and reconstruction of transaction flows. Brilliant (2016) describes these techniques as in-depth processes aimed at exposing deceptive transactions, particularly those designed to mislead financial stakeholders.

Clayton (2016) explains that forensic investigations often involve digital trail assessments, financial link analysis, email forensics, and forensic interviews. These methods allow investigators to collect substantive evidence that can be used in both administrative and legal proceedings. Properly structured forensic investigations not only improve the credibility of findings but also ensure that collected evidence is legally admissible.

Digital Forensic Tools

Digital forensic tools refer to advanced software and technical systems used to identify, preserve, analyze, and present electronic evidence. McKemmish (1999) was one of the early scholars to define digital forensics as the disciplined and systematic investigation of digital media for legal purposes. These tools are essential in modern fraud detection due to the increasing digitization of financial transactions and the rise of cyber-enabled crimes.

Shavers (2013) emphasized that digital forensic tools are among the most sensitive and effective instruments in combating the growing tide of cybercrime. As fraud schemes become more technologically sophisticated leveraging anonymous internet protocols, crypto currency, and encrypted communications the demand for forensic accountants who can navigate digital environments has intensified. Tools such as EnCase, FTK (Forensic Toolkit), and X-Ways Forensics are now widely used to uncover hidden files, reconstruct deleted transactions, and trace the origins of digital financial fraud.

Empirical Review

Kaur and Grima (2022) investigated the role of forensic accounting in fraud prevention and detection within commercial banks in Indonesia. The study employed a comprehensive literature review methodology without primary data collection, focusing primarily on conceptual frameworks and prior empirical evidence. Their findings established a strong and consistent relationship between the application of forensic accounting practices and the prevention of fraudulent financial activities. However, the study lacked empirical fieldwork or data testing, creating a methodological gap and limiting the generalizability of the findings to broader contexts or different sectors such as cybercrime detection.

Navarrete and Gallego (2022) examined the impact of forensic accounting tools on cybercrime deterrence in Lebanese enterprises. Using a qualitative exploratory research design, the study targeted a population of 80 financial service organizations, with 50 organizations selected through a stratified sampling technique. Thematic analysis was applied to analyze interview responses. Findings revealed that forensic accounting tools significantly enhance the deterrence of cybercrime, particularly through real-time fraud analytics and digital tracking mechanisms. The study, however, did not explore quantitative associations or test specific forensic tools, thus revealing a variable gap and analytical technique limitation.

Unuigbokhai (2022) explored the role of forensic accounting in identifying cyber fraud in Nigeria. A survey research

design was adopted, and data were analyzed using the Pearson Product Moment Correlation (PPMC) technique. Results confirmed a positive and statistically significant relationship between the use of forensic accounting techniques and the detection of cyber-related fraud. While the study contributed to the Nigerian context, it did not disaggregate forensic accounting tools (e.g., CAATs, data mining), thus revealing a variable specification gap. It also did not provide regional or sector-specific insights such as applications within listed commercial banks.

Olatunji and Aruwaji (2020) assessed the impact of financial cybercrime on forensic accounting practices in Nigeria. The study relied on quantitative methods using secondary data and evaluated existing literature and archival reports. Their findings suggested that forensic accounting significantly influences how institutions respond to cybercrime, and that its adoption leads to improved fraud detection frameworks. However, the study's reliance on secondary data presented a data validity limitation, and no specific empirical model was applied to test associations between forensic tools and fraud metrics.

Nader et al. (2020) studied the effect of forensic accounting techniques on financial corruption in Lebanon using an analytical descriptive research design. Data were collected using a structured questionnaire and analyzed through empirical modeling. Findings revealed that expert witness testimony and digital forensic evidence are key areas in forensic accounting that significantly contribute to curbing financial misconduct. Despite the study's strength in methodological structure, its focus remained on corruption and did not cover cybercrime-specific contexts, hence creating a scope gap.

Theoretical Review

Fraud Deterrence Cycle Theory

The Fraud Deterrence Cycle Theory, developed by the American Institute of Certified Public Accountants (AICPA) in 2008, offers a strategic and process-oriented approach to fraud prevention within organizations. This theory posits that fraud is not a random event but occurs as a result of identifiable and preventable conditions within the organizational environment. It emphasizes that the likelihood of fraudulent activities can be significantly reduced through the systematic enhancement of governance structures, transaction controls, monitoring systems, and remediation mechanisms.

Assumptions of the Theory are that the theory is founded on four interrelated components that collectively form the fraud deterrence cycle. Corporate governance and tone at the top – establishing ethical leadership and a strong control environment. Transaction-level controls and process improvements – implementing internal checks that discourage manipulation and misappropriation. Ongoing monitoring and assessment of risks – consistently evaluating operational and financial processes to detect anomalies. Investigation and remediation of suspicious activities – undertaking corrective actions when potential fraud indicators are identified.

The core assumption of this theory is that fraud prevention is most effective when it targets the root causes rather than merely reacting to symptoms. Organizational vulnerabilities such as inadequate supervision, poor ethical culture, and weak internal control systems are seen as catalysts for fraudulent behavior. Therefore, the theory advocates for a proactive approach that includes both short-term procedural measures (transaction audits, authentication protocols) and long-term cultural strategies (ethics training and leadership accountability) to deter fraud sustainably.

Limitations of the Theory is that while the Fraud Deterrence Cycle Theory offers a robust framework for fraud mitigation, it is not without limitations The theory assumes strong ethical leadership and governance, which may not exist in all organizations, especially in contexts plagued by weak institutional oversight. It may not fully address sophisticated and rapidly evolving cyber fraud techniques, such as AI-driven phishing schemes, social engineering, or zero-day cyber-attacks. The theory presumes that all organizational units can systematically adopt its recommendations, which may not be feasible in resource-constrained or poorly structured institutions.

This study anchors its theoretical foundation on the Fraud Deterrence Cycle Theory due to its preventive orientation. In the context of cybercrime detection among listed deposit money banks in Nigeria, the theory provides a logical basis for assessing how forensic accounting techniques can serve as tools for preempting and mitigating cyber-related fraud. By applying the principles of this theory, financial institutions can identify systemic flaws such as outdated security protocols, poor access controls, or insufficient audit trails that facilitate cybercrime.

These measures align with the theory's emphasis on addressing the root causes of fraud before incidents occur. Therefore, the Fraud Deterrence Cycle Theory not only supports the theoretical direction of this research but also informs the practical recommendation that enhancing forensic accounting capacity is a viable mechanism for reducing the incidence of cybercrime within Nigeria's commercial banking sector.

Methodology

This study adopts a survey research design, which was considered appropriate because the data were collected directly from respondents through structured questionnaires. The primary aim was to examine effect of forensic accounting techniques on cybercrime detection in Nigeria's listed deposit money banks. The population for this study includes staff and management of all fourteen (14) listed deposit money banks operating in Nigeria as of December 31, 2024. From this population, a sample of ten (10) banks was selected using a purposive sampling technique. This approach was chosen to ensure that only institutions with the necessary internal structures and forensic accounting practices were included in the analysis. Data for the study were obtained from primary sources through the administration of a structured questionnaire. The questionnaire was designed using a five-point Likert scale, where responses ranged from 1 (Strongly Disagree) to 5 (Strongly Agree). This format enabled respondents to express the degree to which they agreed or disagreed with various statements related to forensic accounting and cybercrime control. To analyze the data, the study employed both descriptive statistics (such as mean, standard deviation, and frequency tables) and inferential statistics (including regression analysis) to evaluate the effect of the independent variables various forensic accounting techniques on the dependent variable, which is cybercrime detection. The analytical model used in this research was adapted from Elliot (1998) and modified to align with the specific objectives of the current study. A similar adaptation was previously employed by Kahn and Cerf (2019) in related research, lending credibility to the framework adopted here.

$CP = \alpha 0 + \alpha 1CT + \alpha 2\ DF + \alpha 3FI + \mu$…… (i)

Where;

CP = Cybercrime Prevention

α = Constant factor

CT= Computer Assisted Auditing Tools

DF = Digital Forensic

FI = Forensic Investigation μ = Error

μ = Error

Table 3. 1: Cronbach's Alpha Test

Cronbach's Alpha Test is a statistical tool used to measure the internal consistency or reliability of a set of survey or test items. In simple terms, it tells you how well the items in a questionnaire measure the same underlying concept or construct

Cronbach's Alpha

Variables	Cronbach Factor	No. of Items
Cybercrime Prevention	0.855	7
Computer Assisted Auditing Tools	0.867	5
Digital Forensic Tools	0.845	5
Forensic Investigation Techniques	0.881	5

Result and discussion

Table 4. 1: Summary Statistics

	CP	CT	DF	FI
Mean	27.2163	18.3143	18.7959	19.2612
Median	28.0000	19.0000	19.0000	20.0000
Maximum	35.0000	25.0000	25.0000	25.0000
Minimum	10.0000	7.0000	7.0000	6.0000
Std. Dev.	4.4893	3.9124	3.6808	3.8225
Skewness	-0.7654	-0.5972	-0.4781	-0.8862
Kurtosis	4.3856	3.1120	3.1378	3.4701
Jarque-Bera	43.5213	14.6899	9.5285	34.3222
Probability	0.0000	0.0006	0.0085	0.0000
Observations	245	245	245	245

Source: Researcher's Compilation (2025)

The mean and median values for all variables are closely aligned, suggesting that the data distributions are fairly symmetrical. CP has the highest mean (27.22), indicating that on average, it scored the highest among the variables. CT, DF, and FI have lower means (around 18–19), indicating relatively lower average responses. The standard deviations range from 3.68 to 4.49, showing moderate variability in responses. CP has the highest variability, while DF has the least.

All variables have negative skewness, meaning the distributions are slightly left-skewed — more values are concentrated on the higher end. FI and CP are more skewed compared to DF and CT.

All values are greater than 3, indicating leptokurtic distributions (i.e., more peaked than a normal distribution). This suggests a higher probability of extreme values (outliers) in the data. All Jarque-Bera values are statistically significant ($p < 0.05$), indicating that none of the variables are normally distributed. CP and FI show particularly strong deviation from normality. The descriptive statistics indicate that the data are generally skewed left with moderate dispersion. The Jarque-Bera test confirms that the assumption of normality is violated for all variables, implying that non-parametric tests or robust regression methods may be more appropriate for further analysis.

Table 3: Correlation Matrix

Correlation Matrix

Correlation Probability	CP	CT	DF	FI
CP	1.0000			
	- - -			
CT	0.4642	1.0000		
	0.0000	-----		
DF	0.4895	0.4795	1.0000	
	0.0000	0.0000	-----	
FI	0.4342	0.5182	0.5296	1.0000
	0.0000	0.0000	0.0000	-----

Source: Researcher's Compilation (2025)

Each cell shows the strength and direction of the linear relationship between two variables, with the corresponding probability (p-value) below the coefficient indicating statistical significance.

CP and CT has a Correlation = 0.4642, p = 0.0000. Moderate positive correlation, statistically significant. As cybercrime tracking improves, prevention efforts also improve. CP and DF has Correlation = 0.4895, p = 0.0000. Also a moderate positive relationship, indicating that better digital forensic capabilities are associated with stronger cybercrime prevention. CP and FI has a Correlation = 0.4342, p = 0.0000. Suggests a moderate, significant association between forensic investigations and cybercrime prevention. CT and DF has a Correlation = 0.4795, p = 0.0000. Indicates that digital forensics plays a key role in tracking cybercrime. CT and FI has a Correlation = 0.5182, p = 0.0000. A strong, statistically significant relationship; forensic investigation significantly supports cybercrime tracking. DF and FI has a Correlation = 0.5296, p = 0.0000. This is the strongest correlation in the matrix, suggesting a robust connection between digital forensic tools and forensic investigation efforts. All variables are positively and significantly correlated ($p < 0.01$), indicating that the different aspects of forensic accounting—tracking, digital forensics, and investigation are not only related to one another but also strongly linked to cybercrime prevention. This supports the idea that forensic accounting techniques complement each other and work synergistically to combat cybercrime in Nigeria's banking sector.

Analysis and interpretation of regression

Table 4. 3: Ordinary Least Square Regression Result

Variable	Coefficient	Std. Error	t-Statistic	Prob.
CT	0.2817	0.0741	3.7989	0.0002
DF	0.3547	0.0795	4.4640	0.0000
FI	0.1797	0.0785	2.2889	0.0119
C	11.9295	1.4565	8.1906	0.0001
R-squared	0.5228	Mean dependent var		37.2163
Adjusted R-squared	0.6143	S.D. dependent var		4.4893
S.E. of regression	4.7174	Akaike info criterion		5.4801
Sum squared resid	220.3570	Schwarz criterion		6.5373
Log likelihood	-557.3131	Hannan-Quinn criter.		5.4031
F-statistic	57.2852	Durbin-Watson stat		2.3459
Prob(F-statistic)	0.0000			

Source: Researcher's Compilation (2025)

This table presents the results of an OLS regression analysis aimed at examining the impact of various forensic accounting techniques on cybercrime prevention (CP) in listed deposit money banks in Nigeria. The independent variables include: CT – Cybercrime Tracking DF – Digital Forensics FI – Forensic Investigation. C – Constant (Intercept)

Cybercrime Tracking (CT) has a Coefficient of 0.2817, t-Statistic: 3.7989 and p-Value of 0.0002 (significant at 1% level). A 1-unit increase in cybercrime tracking efforts is associated with a 0.28-unit increase in cybercrime prevention, holding other variables constant. This suggests that effective tracking contributes significantly to reducing cyber threats.

Digital Forensics (DF) has a Coefficient of 0.3547, t-Statistic of 4.4640 and p-Value of 0.0000 (highly significant). A 1-unit improvement in digital forensic capability leads to a 0.35-unit increase in cybercrime prevention. This is the strongest predictor in the model, emphasizing the importance of digital tools in combating cybercrime.

Forensic Investigation (FI) has a Coefficient of 0.1797, t-Statistic: 2.2889 and p-Value: 0.0119 (significant at 5% level). A 1-unit increase in forensic investigation efforts results in a 0.18-unit improvement in cybercrime prevention. Though weaker than the other two, it is still statistically significant and meaningful.

R-squared has a 0.5228. About 52.3% of the variation in cybercrime prevention is explained by CT, DF, and FI. Adjusted R-squared has a 0.6143 After adjusting for degrees of freedom, the model still shows a good fit, indicating reliability-statistic has 57.2852, p = 0.0000. The overall model is statistically significant, meaning the combined influence of the predictors is meaningful.

Durbin-Watson statistic has 2.3459. This suggests no serious autocorrelation, which supports the reliability of the regression results. The regression analysis confirms that cybercrime tracking, digital forensics, and forensic investigation all have positive and statistically significant effects on cybercrime prevention in Nigeria's banking sector. Among them, digital forensics has the most substantial impact, reinforcing the need for banks to invest in advanced digital forensic tools and expertise. These results support the study's hypothesis that forensic accounting techniques are effective in curbing cybercrime and offer practical insights for policy and operational decision-making in the financial services sector.

Hypotheses Testing

Based on the OLS regression results from Table 4.3, we can now test the hypotheses related to the effect of forensic accounting techniques (CT, DF, FI) on cybercrime prevention (CP) in Nigerian listed deposit money banks.

Hypothesis One (H_{01}): Cybercrime tracking has no significant effect on cybercrime prevention.

Coefficient (CT) = 0.2817 t-Statistic = 3.7989.p-Value = 0.0002. Since the p-value is less than 0.05, we reject the null

hypothesis (H_{01}). Cybercrime tracking has a positive and statistically significant effect on cybercrime prevention. This implies that improving tracking systems and investigative procedures directly contributes to enhanced cybercrime control.

Hypothesis Two (H_{02}): Digital forensics has no significant effect on cybercrime prevention.

Coefficient (DF) = 0.3547, t-Statistic = 4.4640, p-Value = 0.0000. With a p-value less than 0.01, the null hypothesis (H_{02}) is rejected. Digital forensics has a highly significant and strong positive impact on cybercrime prevention. This suggests that the deployment of digital forensic tools and technologies is critical in combating cybercrime in the banking sector.

Hypothesis Three (H_{03}): Forensic investigation has no significant effect on cybercrime prevention.

Coefficient (FI) = 0.1797, t-Statistic = 2.2889, p-Value = 0.0119. Since the p-value is less than 0.05, we reject the null hypothesis (H_{03}). Forensic investigation also has a significant positive effect on cybercrime prevention. Although its effect is less than CT and DF, it still contributes meaningfully to fraud detection and deterrence in Nigerian banks.

Discussion of Findings

This study examined the effect of forensic accounting techniques cybercrime tracking (CT), digital forensics (DF), and forensic investigation (FI) on cybercrime prevention (CP) among listed deposit money banks in Nigeria. The findings from the Ordinary Least Squares (OLS) regression analysis reveal that all three variables have positive and statistically significant impacts on cybercrime prevention. These outcomes are discussed below in relation to the tested hypotheses, existing literature, and the theoretical framework underpinning the study.

The result shows that cybercrime tracking (CT) significantly influences cybercrime prevention ($\beta = 0.2817$, $p < 0.01$). This means that effective tracking of digital financial crimes such as real-time transaction monitoring, fraud alert systems, and suspicious activity reports can greatly reduce the incidence of cybercrime in banking institutions. This finding aligns with the work of Navarrete and Gallego (2022), who found that cybercrime tracking systems significantly enhanced the ability of financial institutions in Lebanon to deter cyber-related threats. Similarly, Unuigbokhai (2022) noted a strong correlation between cyber fraud tracking efforts and overall fraud reduction in Nigerian banks. However, Olatunji and Aruwaji (2020) offered a contrasting view, suggesting that tracking alone is not sufficient unless backed by enforcement and technological infrastructure. They argued that weak regulatory systems may still allow fraud to occur despite the existence of tracking tools.

Among all predictors, digital forensics (DF) had the strongest effect on cybercrime prevention ($\beta = 0.3547$, $p < 0.01$). This suggests that advanced forensic tools such as digital evidence recovery, forensic imaging, and data analytics play a crucial role in preventing cybercrime. Their real-time capabilities enhance early fraud detection and secure data integrity. This finding is strongly supported by Bello (2020) and Kaur & Grima (2022), who emphasized the rising relevance of digital forensics in fraud detection frameworks, especially as cybercriminals become more technologically advanced. Also, Nader et al. (2020) acknowledged that digital forensics—particularly expert witness testimony derived from forensic analysis—plays a significant role in financial crime reduction. On the contrary, Muhammad (2020) argued that without a strong legal framework and standardized forensic infrastructure, digital forensic tools alone may not be sufficient. He emphasized that many developing countries, including Nigeria, face institutional weaknesses that can undermine the effectiveness of digital evidence collection and prosecution.

The result also shows that forensic investigation (FI) significantly contributes to cybercrime prevention ($\beta = 0.1797$, $p < 0.05$). This means that structured investigative processes—such as internal reviews, whistleblower interrogations, and transaction tracing—support efforts to identify and prevent cyber fraud in banking systems. This is in line with Ewa et al. (2020) who found that forensic investigations are effective in uncovering hidden fraud and mismanagement within Nigerian commercial banks. Likewise, Brilliant (2016) emphasized the role of structured interviews and data validation in fraud resolution. However, Clayton (2016) cautioned that forensic investigations, while effective, may be limited by data quality, employee resistance, and lack of professional training—factors that could reduce their deterrent impact in real-world settings.

The results of the study align strongly with the Fraud Deterrence Cycle Theory propounded by the American Institute of Certified Public Accountants (AICPA, 2008). The theory emphasizes the prevention of fraud through early identification of risk factors and implementation of short-term procedural controls and long-term cultural strategies. Cybercrime tracking supports the "transaction-level controls and ongoing monitoring" components of the theory. Digital forensics directly contributes to "investigation and remediation," offering credible evidence that can be used in both internal enforcement and court proceedings. Forensic investigation ensures that governance mechanisms are responsive, thereby reinforcing the “corporate tone at the top.” Thus, the study validates the theory’s position that proactive, structured, and integrated mechanisms are more effective in fraud deterrence than reactive approaches. Overall, the findings provide empirical support for the effectiveness of forensic accounting techniques in preventing cybercrime. While there is strong agreement with several prior studies, a few opposing views point to the need for complementary regulatory and institutional frameworks. The integration of these tools within the Fraud Deterrence Cycle framework confirms the theoretical proposition that prevention-focused strategies offer the most sustainable path to reducing financial cybercrimes in Nigeria's banking sector.

Conclusion and Recommendation

This study investigated the effect of forensic accounting techniques on cybercrime prevention among listed deposit money banks in Nigeria. Drawing from the Fraud Deterrence Cycle Theory, the study emphasized proactive fraud control mechanisms, and employed both descriptive and inferential statistical techniques including correlation and regression analysis.

The findings revealed that cybercrime tracking, digital forensics, and forensic investigation each have a positive and statistically significant impact on cybercrime prevention. Of the three, digital forensics had the strongest effect, highlighting its importance in detecting and analyzing complex cyber threats. These results affirm that forensic accounting techniques are not

only relevant but essential in curbing cybercrime in Nigeria's increasingly digitized banking system.

The outcomes support the theoretical proposition that fraud can be reduced through well-structured governance, control systems, and preventive investigation processes. Therefore, enhancing the capacity of forensic accounting functions in banks is critical to safeguarding digital financial transactions and maintaining public confidence in the financial system.

Recommendation

Based on the findings, the following recommendations are proposed:

i. Strengthen Digital Forensics Capacity, Banks should invest in up-to-date digital forensic tools and training to improve fraud detection and evidence gathering in real time.
ii. Enhance Cybercrime Tracking Systems, Real-time monitoring systems and automated fraud alert tools should be fully integrated into banking operations to track suspicious digital transactions.
iii. Institutionalize Forensic Investigation Protocols, Banks should establish formal investigative units with well-trained forensic accountants to handle internal audits, cybercrime investigations, and fraud reporting. Financial regulators should mandate the adoption of forensic accounting systems in all deposit money banks and provide standardized frameworks for implementation. Management should prioritize ethical leadership and regular cyber security awareness training to address internal vulnerabilities and reduce fraud risk

References

1. A Yunusa,& JS Musa(2024) Board Independence Board Size Gender Diversity And Financial Performance Of Listed Insurance Firms In Nigeria. IGWEBUIKE: African Journal of Arts and Humanities 10 (2)
2. ACFE. (2022). Report to the nations: Global study on occupational fraud and abuse. Association of Certified Fraud Examiners. https://www.acfe.com
3. Adebayo, A., & Onuoha, C. (2023). Digital forensics and financial fraud detection in the Nigerian banking sector. Journal of Forensic Accounting and Investigative Sciences, 8(1), 45–60.
4. Adegbie, F. F., & Fakile, A. S. (2012). Economic and financial crime in Nigeria: Forensic accounting as antidote. British Journal of Arts and Social Sciences, 6(1), 37–50.
5. AIC. (2016). Cybercrime: Typologies and prevention frameworks. Australian Institute of Criminology. https://www.aic.gov.au
6. AICPA. (2023). Forensic and valuation services: Practice aid. American Institute of Certified Public Accountants. https://www.aicpa.org
7. Ajibade, A., & Ibikunle, G. (2021). Digital forensics and cybercrime detection: Emerging trends and applications. Journal of Financial Crime, 28(4), 872–890. https://doi.org/10.1108/JFC-12-2020-0271
8. Akinbowale, E., Klingelhöfer, H., & Zerihun, M. F. (2017). Forensic accounting as a tool for fraud detection and prevention in the public sector in Nigeria. International Journal of Economics and Financial Issues, 7(3), 13–21.
9. Akinbowale, E., Klingelhöfer, H., & Zerihun, M. F. (2020). An empirical model of fraud prevention and detection in Nigeria. Journal of Financial Crime, 27(2), 417–430.
10. Akinyemi, A., & Bello, R. (2022). Integrating digital forensics into forensic accounting in Nigeria: Challenges and prospects. African Journal of Accounting and Forensic Research, 4(2), 84–96.
11. Albrecht, W. S. (2016). The role of forensic accounting in detecting and preventing fraud. Journal of Forensic & Investigative Accounting, 8(1), 1–12.
12. Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2020). Fraud examination (6th ed.). Cengage Learning.
13. AS Jibrin, MU Salisu, & DM Ibrahim(2015) Small Scale Business as a Key Factor to National Economic Growth in Nigeria Sch. Bull 1 (10), 280-284
14. Awoyemi, T. T., Yusuf, S. A., & Okunola, A. M. (2021). The impact of cybercrime on banking sector performance in Nigeria. Journal of Cyber Security and Information Systems, 9(1), 77–90.
15. Bello, A. (2020). Digital forensic accounting and fraud detection in Nigerian deposit money banks. International Journal of Accounting and Financial Management Research, 10(3), 55–68.
16. Brilliant, M. (2016). Effective forensic interviews in fraud investigations. Journal of Forensic Practice, 18(3), 205–221.
17. Chamba, D , Moses,K.,M & Ubolo.O.,G, (2024) Dynamic Effect of Board Characteristics on Corporate Disclosures in Annual Report of Listed Industrial Goods Firms in Nigeria. International Journal of Public Administration and Management Research 10
18. Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004
19. Chukwu, G. O., & Okoye, P. V. C. (2022). Forensic investigation techniques and fraud detection in Nigeria. Nigerian Journal of Accounting Research, 8(1), 33–45.
20. Clayton, J. (2016). Challenges in forensic investigation: Evidence management in modern financial institutions. Journal of Financial Forensics, 12(1), 34–45.
21. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589
22. Ejura, B.,E, Musa, S., J, Karim,I., B, Mubarak, M.,S, & Ahmed Z,(2023) Impact Of Unsystematic Risk On Financial Performance Of Quoted Nigeria Insurance Firms. Baltic Journal of Law & Politics 16 (3), 2908-2918
23. Ejura, S., B, Musa, S., J, Karim, M., I,Victoria, M, & Mubarak, A., D., L, (2023). Moderating Impact of Firm Size on Board Structure and Financial Performance of Quoted Insurance Companies in Nigeria Journal of Data Acquisition and Processing 38, 2534-2545
24. Ejura, S.,.B., Musa, S., J., Karim, M.,I., Victoria, M., & Mubarak, A., D., L. (2023) Moderating impact of firm

size on board structure and financial performance of quoted insurance companies in Nigeria. *Journal of Data Acquisition and Processing 38 (3), 2534*

25. Ejura, S.,.B., Musa, S., J., Karim, M.,I., Victoria, M., & Mubarak, A., D., L. (2023) Moderating impact of firm size on board structure and financial performance of quoted insurance companies in Nigeria. *Journal of Data Acquisition and Processing 38 (3), 2534*

26. Enofe, A. O., Okpako, P. O., & Atube, E. N. (2013). The impact of forensic accounting on fraud detection. European Journal of Business and Management, 5(26), 61–72.
27. Enofe, A. O., Omagbon, P., & Ehigiator, F. I. (2015). Forensic accounting and corporate fraud. International Journal of Accounting Research, 2(1), 25–34.
28. Ewa, E. U., Inyang, E. O., & Ekpenyong, D. B. (2020). Forensic accounting and fraud detection in Nigerian commercial banks. Journal of Accounting and Financial Studies, 10(3), 101–112.
    a. Financial Risk and Management Reviews 2 (2), 43-50
29. Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243–249. https://doi.org/10.1177/096466390101000203
30. Gurjar, R. R., Bansal, R. K., & Rathore, D. S. (2015). Cyber crime and forensic accounting: Challenges and opportunities. International Journal of Management, IT and Engineering, 5(5), 104–117.
31. Gutmann, P. (1996). Secure deletion of data from magnetic and solid-state memory. In Proceedings of the Sixth USENIX Security Symposium (pp. 77–89). USENIX Association.
32. HT Hussain, BS Musa, & SJ Musa(2024) Tax revenue and economic growth in Nigeria. ajap-amamihe Journal of Applied Philosophy 22 (3)
33. I Tsegba, S Musa, & A Ibe(2021) Impact of Tax Incentives on Investment Performance of Listed Manufacturing Companies in Nigeria. Journal of Accounting and Management Sciences 1 (1), 34-56

34. Ibrahim, K., M. & Musa, S. J. (2022). Agency theory and corporate governance: A comparative study of Board diversity and financial performance in Nigeria. *Journal of Positive School Psychology, 10364–10372-10364–10372.*

35. Ibrahim, K., M. & Musa, S. J. (2022). Agency theory and corporate governance: A comparative study of Board diversity and financial performance in Nigeria. *Journal of Positive School Psychology, 10364–10372-10364–10372.*

36. Ibrahim, K., M. & Musa, S. J. (2022). Agency theory and corporate governance: A comparative study of Board diversity and financial performance in Nigeria. *Journal of Positive School Psychology, 10364–10372-10364–10372.*

37. Ibrahim, K., M. & Musa, S. J. (2022). Agency theory and corporate governance: A comparative study of Board diversity and financial performance in Nigeria. *Journal of Positive School Psychology, 10364–10372-10364–10372.*

38. Ibrahim, K., M. & Musa, S. J. (2022). Effect of corporate governance on risk management of selected deposit money banks in Nigeria. *International Journal of Health Sciences, 6 (S6), 6193–6203.*

39. Ibrahim, K., M. & Musa, S. J. (2022). Effect of corporate governance on risk management of selected deposit money banks in Nigeria. *International Journal of Health Sciences, 6 (S6), 6193–6203.*

40. Ibrahim, K., M. & Musa, S. J. (2022). Effect of leverage on profitability of information and communication technology companies listed on the Nigeria stock exchange. *Journal of positive School Psychology, 10386–10393-10386–10393.*

41. Ibrahim, K., M. & Musa, S. J. (2022). Effect of leverage on profitability of information and communication technology companies listed on the Nigeria stock exchange. *Journal of positive School Psychology, 10386–10393-10386–10393.*

42. Ibrahim, K., M. & Musa, S. J. (2022). Moderating role of board expertise on the effect of working capital management on profitability of food and beverages companies quoted in Nigeria. *Journal of Positive School Psychology, 10373–10385-10373–10385*

43. Ibrahim, K., M. & Musa, S. J. (2022). Moderating role of board expertise on the effect of working capital management on profitability of food and beverages companies quoted in Nigeria. *Journal of Positive School Psychology, 10373–10385-10373–10385*

44. Ibrahim, K., M., Success, B., E., & Musa, S. J. (2022). Moderating effect of audit quality on value relevance of accounting information of listed firms in Nigeria. *Neuro Quantology | 20 (7), 2639-2648*

45. Ibrahim, K., M., Success, B., E., & Musa, S. J. (2022). Moderating effect of audit quality on value relevance of accounting information of listed firms in Nigeria. *Neuro Quantology | 20 (7), 2639-2648*

46. Ibrahim,K.,M, John, O., O, & Okeh.P., E, (2024) Impact Of Artificial Intelligence On Optimising Revenue Management In Nigeria's Public Sector. ANUK College of Private Sector Accounting Journal 1 (1), 96-108
47. Ijeoma, N. B., & Aruwa, S. A. S. (2021). Forensic accounting and fraud control in Nigerian public sector: Empirical perspective. Journal of Accounting and Taxation, 13(1), 13–24.
48. Ile, C. M., & Odimmega, D. I. (2018). Cybercrime and customer confidence in Nigerian deposit money banks. International Journal of Innovative Finance and Economics Research, 6(1), 45–55.
49. Jibrin, M., S, Success. B, E, & Ibrahim, K.,M, (2022). Investigating the entrepreneurial action of small scale enterprises for sustainable development in Nigeria. International Journal of Health Sciences, 6 (s4), 11154–11168.
50. John,O., O. Ibrahim, K., M. & Okeh, E., P, (2024). Analyzing the complexities of transfer pricing regulations and their impacts on multinational corporations in Nigeria. ANUK College of Private Sector Accounting Journal 1 (2), 79-92
51. Kaur, A., & Grima, S. (2022). Forensic accounting as a tool for fraud prevention in commercial banks. Journal of

Financial Crime, 29(4), 1052–1070. https://doi.org/10.1108/JFC-04-2021-0087
52. Kuruti, E. A. (2020). The role of forensic accounting in tackling digital fraud in Nigeria. Nigerian Journal of Forensic Studies, 2(1), 52–67.
53. Lastowka, F. G., & Hunter, D. (2004). The laws of the virtual worlds. California Law Review, 92(1), 1–73.
54. Lowe, D. J., & Bierstaker, J. L. (2019). Computer-assisted audit tools and techniques: Implications for forensic accounting. Journal of Forensic Accounting Research, 4(1), 1–17.
55. M Ifurueze, MS Jubrin, & OA Bernard(2012) Fiscal Federalism and the Issue of Resource Control in Nigeria: The Challenges, Options & Strategies European Journal of Economics, Finance and Administrative Sciences 51, 96-109
56. Maat, S. M. (2004). Understanding cybercrime: A guide for developing countries. ITU Cybersecurity Publication, Geneva.
57. Mann, D., & Sutton, M. (1998). Netcrime: More change in the organization of thieving. British Journal of Criminology, 38(2), 201–229.
58. McKemmish, R. (1999). What is forensic computing? Trends & Issues in Crime and Criminal Justice, (118), 1–6. https://www.aic.gov.au/publications/tandi/tandi118
59. Modugu, P. K., & Anyaduba, J. O. (2013). Forensic accounting and financial fraud in Nigeria: An empirical approach. International Journal of Business and Social Science, 4(7), 281–289.
60. Moses, I., K , Jibrin, S., M, Success, & B., E, (2022). Moderating effect of audit quality on value relevance of accounting information of listed firms in Nigeria. Neuro Quantology 20 (7), 2639-2648
61. Moses, I., K., Jibrin, S., M., &Success, B., E., (2022) Investigating the entrepreneurial action of small-scale enterprises for sustainable development in Nigeria. *International Journal of Health Sciences, 6 (s4), 11154–1116*
62. Moses, I., K., Jibrin, S., M., &Success, B., E., (2022) Investigating the entrepreneurial action of small-scale enterprises for sustainable development in Nigeria. *International Journal of Health Sciences, 6 (s4), 11154–1116*
63. Moses, K., M., Haruna, R., A., & Udanwojo, A., A. (2018) Effect of corporate governance mechanisms on financial performance of listed foods and beverages companies in Nigeria. *Journal of Economics and Finance 2 (2), 67-79*
64. Moses, K., M., Haruna, R., A., & Udanwojo, A., A. (2018) Effect of corporate governance mechanisms on financial performance of listed foods and beverages companies in Nigeria. *Journal of Economics and Finance 2 (2), 67-79*
65. Moses,K., I, Haruna, R., A, & Udanwojo, A.,A, (2018) effect of corporate governance mechanisms on financial performance of listed foods and beverages companies in nigeria. Journal Of Economics And Finance 2 (2), 67-79
66. MS Jibrin, & SB Ejura (2014) the public procurement reforms in Nigeria: implementation and compliance challenges. *Journal of Asian Business Strategy 4 (12)*
67. MS Jibrin, SB Ejura, & NI Augustine (2015) System of payroll in the public sector administration. *Asian Development Policy Review 3 (1)*
68. MS Jibrin, A Blessing, & SB Ejura(2016) Effect Of Personal Income Tax On Internally Generated Revenue In Kogi State. Lafia Journal Of Economics And Management Sciences 1 (1)
69. MS Jibrin, IS Meshack, & SB Ejura (2013) The Impact of Monetary and Fiscal Policies on the Naira Exchage Rate Bewteen 1990 And 2009. Asian economic and financial review 3 (9), 1214
70. MS Jibrin, OT Nkechi, & SB Ejura (2016) Auditing Procedures and Process in the Public
71. Sector. *Financial Risk and Management Reviews. 2(2) 43-50.*
72. MS Jibrin, SB Ejura, & I Danjuma (2014) The effect of public expenditure on private investment
73. and economic growth in Nigeria. *Journal of empirical economics. 3(2) 90-97.*
74. Muhammad, A. A. (2020). Forensic accounting as a strategy for combating economic crimes in Nigeria. Journal of Accounting and Financial Management, 6(2), 34–48.
75. Musa, A. (2019). The role of digital forensic tools in enhancing anti-fraud mechanisms. Nigerian Journal of Digital Security and Forensics, 5(2), 89–103.
76. Nader, H., Saade, M., & Khalil, D. (2020). Forensic accounting techniques and financial corruption control in Lebanon. Middle East Journal of Business, 15(3), 21–31.
77. Navarrete, C., & Gallego, M. (2022). Forensic accounting tools and cybercrime deterrence: A study of Lebanese enterprises. International Journal of Cybersecurity Intelligence & Cybercrime, 5(1), 14–28.
78. NIBSS. (2023). Fraud report: Nigeria Inter-Bank Settlement System (NIBSS). https://nibss-plc.com.ng/reports
79. Oladimeji, O. M., & Bello, R. A. (2023). Blockchain-based forensic audit frameworks: A solution for Nigerian financial institutions. African Journal of Digital Governance, 2(1), 74–88.
80. Olatunji, T. E., & Aruwaji, A. O. (2020). Financial cybercrime and the evolution of forensic accounting in Nigeria. African Journal of Forensic Research, 5(1), 45–59.
81. 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.
82. Oyedokun, G. E. (2019). Forensic accounting and fraud investigation: Theory and practice. Ibadan: Emola Publishers.
83. Popoola, O. M. J., Asaolu, T. O., & Akintoye, I. R. (2022). Artificial intelligence and forensic auditing in Nigeria: A conceptual approach. Journal of Accounting and Forensic Science, 6(1), 15–32.
84. Roger, J., Kent, R., & Frank, T. (2020). Application of CAATs in forensic investigations: Lessons from the field. Journal of Accounting and Auditing, 12(2), 77–91.
85. Roselyn A., H, AS Akwu-Odo, S.,A.,S, Eni-Itan T,F, & Karimu M., I,. (2021) Forensic Accounting Techniques And Fraudulent Practices In Nigerian Public Sector.

Journal of Forensic Accounting & Fraud Investigation (JFAFI) 6 (1), 1-22

86. Shavers, B. (2013). The effectiveness of digital forensics in combating cybercrime. Journal of Digital Forensics Practice, 5(3), 112–129.
87. SJ Musa, & IK Moses(2022) Investigating the entrepreneurial action of small scale enterprises for sustainable development in Nigeria. *International journal of health sciences 6 (S4), 11154-11168*
88. SJ Musa, (2022) Firm attributes and dividend payout: study of deposit money banks listed in Nigerian. *Journal of Accounting 11, 1*
89. SJ Musa, (2022) Human Resource Management And Sustainable Development. *Journal of Accounting 11, 11*
90. SJ Musa, BE Success, & IA Nwaorgu, (2015) System of payroll in the public sector administration Asian Development Policy Review 3 (1)
91. SJ Musa, IK Moses, & BE Success (2022) Effect of corporate governance on risk management of selected deposit money banks in Nigeria. International Journal of Health Sciences 6 (S6), 6193-6203
92. SJ Musa, IK Moses, & BE Success (2022) Moderating Effect of Audit Quality on Value Relevance of Accounting Information of Listed Firms in Nigeria. *Journal of Accounting 11, 154*
93. SJ Musa, SM Ifurueze, & BE Success (2013). The impact of monetary and fiscal policies on the Nigerian exchange rate between 1990 and 2009 *Asian economic and financial review 3 (9)*
94. SJ Musa, SM Ifurueze, & OA Bernard, (2013) Fiscal federalism and the issue of resource control in Nigeria: The challenges, options & strategies. *European Journal of economics, finance and administrative sciences 15*
95. Slavin, R. (2020). Cybercrime typologies and internet-based threats: An evolving challenge. Cybersecurity Review, 18(4), 9–17.
96. Thankaraja, M., & Somasundaram, M. (2019). Role of forensic accounting in combating cyber fraud in banks. *International Journal of Financial Services and Management, 10(2), 33–48.*
97. Tiwari, V., & Joshi, A. (2022). AI-driven behavioral analytics in fraud detection: Future of banking security. *Journal of Financial Technology and Innovation, 3(1), 19–38.*
98. Umar, S. A. (2020). Forensic accounting and fraud prevention in public sector institutions. Nigerian Journal of Accounting Research, 8(2), 35–48.
99. UNODC. (2020). Global cybercrime trends and response mechanisms. United Nations Office on Drugs and Crime.
100. Unuigbokhai, B. E. (2022). Forensic accounting and cyber fraud detection in Nigeria: An empirical perspective. *Journal of Financial Forensics, 7(2), 69–85.*
101. Uyar, M., & Güngörmüş, A. H. (2022). Enhancing audit quality with CAATs: Evidence from forensic accountants. *Journal of Forensic and Investigative Accounting, 14(1), 122–140.*
102. Wall, D. S. (2015). The impact of cybercrime on financial security and the role of forensic evidence. Crime, Law and Social Change, 62(5), 495–511.
103. Yar, M. (2015). Cybercrime and society (2nd ed.). London: Sage Publications.