DELSU Journal of Management Sciences
Abbr. Title: Deljoms, FMS
ISSN: *(Online)* **: 2756-3731**
OPEN ACCESS
Research Article
Volume 7 Number 1 June, 2025

Forensic Accounting and Cybercrime: Evidence from Nigerian Banking Industry

OGBOTOR, Maxwell Smith Ph.D
Department of Accounting,
Faculty of Management Sciences,
Delta State University, Abraka, Nigeria

Publication Date: 2025/06/30

Abstract
This paper explores the relationship between forensic accounting and cybercrime in Nigeria's banking sector, utilizing secondary data and qualitative analysis. Grounded in fraud prevention and perceived pressure/incentive/motive theories, the study reveals a concerning rate of cybercrime, resulting in substantial financial losses and compromised customer data. To combat this, the study advocates for the integration of forensic accounting, robust cyber security measures, and effective regulatory implementation. Recommendations include investing in cyber security infrastructure and enforcing regulations like the Cybercrime Act. Furthermore, promoting digital financial services, financial literacy, and good corporate governance can help mitigate cybercrime's impact. The study also highlights the importance of engaging forensic accountants and building capacity in cyber security and digital forensics to stay ahead of emerging threats.

Keywords: *Forensic accounting, Cybercrime, Nigerian banking industry, Cybercrime investigation, Digital forensics*

Introduction

Nigeria's banking industry is under siege from a new breed of thieves: cybercriminals. These digital outlaws can drain your bank account, steal your identity, and shake the very foundations of our financial systems. But there's a beacon of hope in this dark landscape: forensic accounting. These financial detectives use their expertise to track down the culprits and bring them to justice. The banking sector plays a pivotal role in sustaining economic stability. However, Nigerian banks have faced a decade-long surge in fraudulent activities through cyber space, eroding public trust and threatening financial stability, ultimately harming shareholders' interests (Adeyemi & Fagbemi, 2023).

The accounting profession's shift towards forensic accounting, as seen in countries like the US, UK, and Malaysia (Hassan & Sanni, 2023), presents an opportunity for Nigeria to bolster its banking sector's integrity and public trust. Unlike conventional accounting methods, which have proven inadequate in detecting and preventing fraud (Okoye, 2013), forensic accounting offers a specialized approach to addressing financial crimes. With their advanced technical expertise, forensic accountants can complement traditional auditing roles (Crumbley, 2012), filling the gap in detecting and preventing fraud, and ultimately contributing to a stable financial system. By adopting forensic accounting practices, Nigeria can potentially mitigate the impact of fraudulent activities and restore confidence in its financial sector.

The integration of forensic accounting tools is essential for financial institutions to meet stakeholder expectations and prevent fraudulent activities (Krstic, 2009). Forensic accounting plays a critical role in detecting and investigating financial crimes, such as embezzlement and complex transactions (Marianne, 2005). By adopting robust forensic accounting practices, financial institutions can promote a culture of accountability and transparency, reducing the risk of financial crimes.

In Nigeria's banking sector, the surge in fraudulent activities has underscored the importance of forensic accounting (Adeyemi & Fagbemi, 2023). Traditional audit methods are no longer sufficient to detect and prevent fraud, given the complexity of modern banking transactions (Centre for Forensic Studies, 2010). This study highlights the significance of forensic accounting in uncovering and mitigating cybercrime in Nigeria's banking industry, ultimately contributing to a safer and more secure banking environment. By leveraging forensic accounting, financial institutions can better protect themselves and their customers from the devastating effects of cybercrime.

Literature Review

Forensic Accounting

The field of forensic accounting has its roots in the mid-20th century, when Peloubet (1946) first conceptualized it as a means to apply accounting expertise to legal issues. Since then, forensic accounting has evolved to incorporate a range of skills and techniques, including accounting, auditing, and investigation (Dada, Owolabi & Okwu, 2013; Zysman, 2004). This field plays a critical role in detecting and preventing financial crimes, and its applications are diverse.

Forensic accounting is a multifaceted discipline that involves analyzing financial data, identifying irregularities, and providing expert testimony (Oyedokun et al., 2019). It requires specialized skills and knowledge, including the ability to interpret financial transactions and identify potential fraud (Enofe, Utomwen, & Danjuma, 2015). By combining accounting, auditing, and investigative techniques, forensic accountants can help resolve legal disputes and promote financial integrity (ACFE, 2008; AICPA, 2006). Ultimately, forensic accounting is a powerful tool for preventing and detecting financial crimes, and its importance cannot be overstated (Umar, 2020).

Cybercrime

Cybercrime involves using computers, electronic devices, and networks to commit unauthorized acts, such as data theft, fraud, and system sabotage (Slavin, 2020). This encompasses various crimes, including phishing, credit card fraud, and online money laundering (Oloruntoba & Oyedokun, 2023). To combat cybercrime, forensic accounting procedures are employed, utilizing digital forensic tools to collect, examine, and analyze data (Thankaraja & Somasundaram, 2019). These tools enable forensic accountants to investigate cybercrime cases effectively and gather evidence to support potential fraud or cybercrime cases (Gutmann, 1996). By leveraging these techniques, forensic accountants can help mitigate the effect of cybercrime.

Cybercrime refers to criminal activities that utilize computers or networks as tools, targets, or platforms, encompassing a range of offenses from hacking and denial-of-service attacks to traditional crimes facilitated through technology. These crimes can have significant impacts, such as disrupting critical infrastructure, compromising sensitive information, and crippling systems (Nayak, 2013). Various types of cybercrime exist, including hacking, virus dissemination, phishing, cyberstalking, identity theft, and software piracy, among others (Goni et al., 2022). These crimes can cause widespread

disruption and harm to individuals, organizations, and societies.

The advent of information and communication technology (ICT) has given rise to cybercrime, as individuals, organizations, and governments increasingly rely on digital systems (Onuora et al., 2017). This dependence on technology has created vulnerabilities, allowing criminals to exploit digital platforms for illicit activities (Ebelogu et al., 2019). Cybercrime can be categorized into two main types: cyber-dependent crimes, which require the internet or ICT systems to function, and cyber-enabled crimes, which are traditional offenses amplified by technology (Europol, 2019; Alvarez, 2021).

Cyber-dependent crimes include activities like malware creation, hacking, and service denial attacks, while cyber-enabled crimes encompass a range of offenses, such as economic crimes, malicious communications, and child exploitation (Europol, 2019; Alvarez, 2021). Individuals, organizations, and governments face various cybercrime threats, including cyber-theft, cyber-terrorism, hacking, and malware attacks (Ibikunle & Odunayo, 2013; Bandakkanavar, 2020; Kaspersky, n.d.; Kumudenee, 2021; Love, 2018; Muhammad & Kiru, 2017). These threats can result in significant financial and reputational damage.

Theoretical Framework

The paper hinged on two (2) theories- fraud preventive theory and perceived pressure/incentive/motive theory

Fraud Preventative Theory

The Fraud Preventative Theory, introduced by Ajzen & Fishbein (1980), suggests that understanding the intentions behind an individual's behaviour can help predict and thwart fraudulent undertakings. According to this theory, intentions are the best predictor of planned behaviour, and identifying the antecedents of these intentions can provide valuable insights into preventing fraud (Ajzen & Fishbein, 1980). In the context of banking, forensic accounting services play a crucial role in preventing and detecting fraud. These services provide litigation support, helping to quantify economic damages and resolve disputes (Akintoye, 2008; Kankpang et al., 2018). Bank statements are essential in maintaining accountability and serving as an audit trail for transactions (Goosen, Beaver & Landsman, 1999). By leveraging forensic accounting facilities and maintaining accurate records, banks can reduce the risk of deceitwith protect their customers' interests. This proactive approach can help prevent fraudulent behaviour and promote a secure banking environment.

Forensic litigation support provides assistance in legal disputes, helping to quantify economic damages and resolve conflicts (Akintoye, 2008). Digital forensics involves the preservation, collection, and analysis of digital evidence to facilitate the reconstruction of events (Carrier, 2003). Studies have explored the responsibilities of forensic accounting with the use of information technology in auditing and financial investigations (Moorthy et al., 2011). However, the impact of forensic ICT on the financial performance of commercial banks in Nigeria remains a distinct area of research, warranting further investigation through field surveys and primary data collection.

The Fraud Prevention Theory offers valuable insights into the human side of cybercrime in Nigeria's banking industry. By understanding what drives individuals to engage in cybercrime, forensic accountants can develop effective strategies to prevent and detect these crimes. This theory highlights the benefits of considering the human factor in cybercrime prevention, allowing forensic accountants to create targeted training programs that educate bank employees on cybercrime risks and security protocols. By combining technical expertise with an understanding of human

motivations, forensic accountants play a very important role in protecting the integrity of Nigeria's banking system. This approach can help reduce the risk of cybercrime and promote a safer banking environment. Ultimately, the theory provides a framework for forensic accountants to proactively address the root causes of cybercrime and develop practical solutions to mitigate its impact.

Perceived Pressure/Incentive/Motive Theory

Pressure is a significant factor in committing fraud, and it can manifest in various forms. The motivations behind fraudulent behaviour can be diverse and complex. Research suggests that pressure can stem from various sources, including personal, professional, and external factors (Lister, 2007; Vona, 2008). Financial difficulties, personal greed, addiction, and other issues can create an environment where individuals may feel pressured to commit fraud (Vona, 2008). Additionally, pressure can be driven by financial, social, or political factors (Murdock, 2008), and can also be linked to employee motivation and personal gain (Rae and Subramanian, 2008). Studies have categorized these pressures into different types, such as economic, job-related, and personal pressures (Albrecht et al., 2008), or as stemming from obligations, personal issues, or corporate pressures (Chen & Elder, 2007).

These pressures can contribute to an individual's likelihood of committing fraud. Pressure can have a dual effect, driving creativity and efficiency when goals are achievable, but potentially leading to misconduct when goals seem unattainable (Hooper & Pornelli, 2010).When pressure becomes an all-consuming force, individuals may resort to questionable activities, including fraud. Personal pressures, such as financial strain, can push individuals to steal. Organizational pressures, including incentives like bonuses and share price targets. This also facilitates pressure to dishonest behaviour (Singleton et al., 2006; Kenyon & Tilton, 2006). These pressures can take many forms, and understanding their impact is crucial in preventing and detecting fraud.

Understanding what drives individuals to commit cybercrime is crucial in the fight against cybercrime in Nigeria's banking industry. Forensic accountants can use the Perceived Pressure/Incentive/Motive Theory to recognize pressures that may push someone to involve in cybercrime, such as financial difficulties or personal greed. By recognizing these pressures, they can develop targeted strategies to prevent and detect cybercrime. This might involve analyzing financial transactions for suspicious patterns or using digital forensics to investigate incidents.

By understanding the motivations behind cybercrime, forensic accountants can also create effective training programs to educate bank employees on cybercrime risks and security protocols. By applying this theory, forensic accountants can play a vital role in keeping Nigeria's banking system safe and protecting customers' sensitive information. This approach can help reduce the risk of cybercrime and promote a safer banking environment.

Methodology

This research utilized a qualitative methodology to examine the intersection of forensic accounting and cybercrime investigation within Nigeria's banking sector. A comprehensive review of existing literature was conducted, drawing from prominent databases such as Google Scholar, JSTOR, and ScienceDirect, as well as industry reports and research publications. The search strategy employed relevant keywords to identify pertinent studies and reports.

The collected data underwent thematic analysis, revealing key patterns and relationships that shed light on the role of

forensic accounting in combating cybercrime. The study's findings offer valuable insights into the development of effective strategies for investigating and preventing cybercrime, with implications for both practice and future research. Although the study's scope is limited to the Nigerian banking industry, its findings can inform context-specific solutions and provide a foundation for further investigation into the application of forensic accounting in cybercrime investigation.

Analysis and Discussion

Cybercrime in the Nigerian Banking Industry

The banking industry's increasing reliance on technology has brought about a new wave of threats - cybercrime. Imagine someone hacking into your online banking account, stealing your hard-earned money, or identity. This is a harsh reality many face today. Cybercrime in banking refers to the use of technology to commit crimes such as hacking, phishing, and malware attacks. These crimes can compromise sensitive customer data, disrupt banking services, and cause significant financial losses.

Nigeria's banking sector has undergone significant transformations, including a major restructuring exercise in 1986 that led to an increase in commercial banks and improved services (Ifokobonk, as cited in Ogunwale, 2020). The introduction of internet banking in the late 1990s revolutionized financial services, enabling transactions such as online payments, electronic fund transfers, and automated teller machine payments (Ogunwale, 2020). However, the widespread adoption of internet banking has also led to a rise in cybercrime activities, with Nigerian banks facing attacks from cybercriminals who steal or transfer funds without authorization (Ogunwale, 2020).

Nigeria's financial institutions have seen a surge in cybercrime threats due to their increased reliance on the internet and technology. This has led to various crimes such as theft, phishing, hacking, and fraud, resulting in significant losses. In 2018, Nigerian financial institutions lost over ₦15 billion to cybercrime and electronic fraud, with annual customer deposit losses estimated at ₦1.9 billion. It's projected that by the year 2030; about $6 trillion will be lost to cybercrimes globally, including Nigeria, mainly through phishing and identity theft (Ogbonnaya, 2020).Fraudulent undertakings led to significant financial losses for Nigerian banks, with N3.5 billion lost in just three months of 2020, marking a considerable rise from the previous year (Eleanya, 2021). The widespread adoption of digital technologies has fueled the surge in cybercrime, including spamming, credit card scams, and phishing attacks, which pose substantial threats to the banking sector's stability and customer trust (Eze, 2021).

The Nigerian banking sector is vulnerable to the adverse effects of cybercrime, according to recent studies. Research by Fadairo-Cokers and Ibrahim (2021) revealed that cybercrime hinders online banking and ATM transactions, often due to inadequate financial knowledge and limited understanding of digital platforms. Furthermore, Muhammad and Kiru (2017) emphasized the need for Nigeria to strengthen its anti-cybercrime efforts, identifying factors such as low literacy rates and ineffective governance as significant contributors to the issue.

To combat identity duplication and fraudulent activities, the Central Bank of Nigeria implemented the Bank Verification Number (BVN) initiative, which aimed to address losses totaling N203 billion over a 14-year period. Despite this effort, Nigerian banks still suffered significant losses, with N12.30 billion lost to internet fraud between 2014 and 2018 (Ogunwale, 2020). While existing research has extensively examined cybercrime threats in the banking sector, there remains a knowledge gap regarding the dynamics

between bank insiders and external cybercriminals. This study seeks to investigate the nexus between bank employees and outside perpetrators in cybercrime, as well as the efficacy of current prevention and detection measures (Faboyede et al., 2023).

Cybercrime significantly impacts the banking system, affecting both financial losses and customer trust. To combat this, banks must invest in robust cyber security measures, including security protocols, transaction monitoring, and customer education (Faboyede et al., 2023). Effective implementation of regulations, such as Nigeria's Cybercrimes Act 2015, can also help reduce cybercrime rates (Ogunwale, 2020).

Forensic Accountants and Auditors in Cybercrime Investigation

Forensic accountants and auditors play a crucial role in cybercrime investigation by utilizing specialized techniques to identify and analyze digital evidence. They extract and analyze data from digital sources like emails, transaction logs, and network traffic, using advanced data analytics and digital forensic tools to uncover fraudulent activities and patterns indicative of financial crimes (Ali, 2024). This expertise is essential in tackling cyber-enabled crimes, which involve sophisticated techniques and advanced technology.

Forensic auditing involves in-depth investigation of financial and non-financial data to identify and evaluate suspected fraud or illegal activity. This process leverages various analytical techniques, such as statistical analysis, predictive analytics, and machine learning, to detect suspicious patterns or evidence of fraud (Bierstaker, Brody& Pacini, 2006). Forensic auditors collect data from various sources, including financial transactions, emails, and digital logs, which are then analyzed using forensic software and advanced technologies.

Forensic accountants possess expertise in conducting detailed interviews and analyzing complex financial transactions to uncover the truth (Okpo & Simeon, 2023). They provide services to corporations, attorneys, and government, helping to estimate losses, identifies perpetrators, and track down assets (Coenen, 2005). Their primary goal is to determine where money went, how it got there, and who was responsible for it (Degboro & Olofinsola, 2007).

The application of technology during forensic accounting has revolutionized the uncovering and substantiation of monetaryscam. Artificial intelligence (AI) enables efficient data analysis and automation of routine tasks, such as document review and transaction matching. Blockchain technology provides a transparent and immutable digital ledger, ensuring the integrity and accuracy of financial data (Bierstaker et al., 2006). This technology allows forensic auditors to analyze big data quickly and accurately, detect suspicious patterns, and identify anomalies that may indicate fraud.

Forensic accountants and auditors are vital in preventing and detecting fraud and corruption within organizations, essentially acting as financial crime scene investigators (Honigsberg, 2020). They collaborate with law enforcement agencies to investigate and prosecute cases (Rahman et al., 2023). By leveraging their skills and expertise, forensic accountants can help bring financial criminals to justice and prevent future crimes.Effective fraud prevention strategies are crucial to protect organizations from financial and reputational losses. Implementing strong policies and procedures related to financial management, payments, and monitoring of financial transactions is essential (KPMG, 2013). Regular internal controls and division of responsibilities, where financial tasks are undertaken by different individuals, can help reduce the risk of fraud (PricewaterhouseCoopers, 2016). By

combining these elements with technology, such as data security systems and anomaly detection systems, organizations can reduce the menace of fraud and protect their assets and reputation (Deloitte, 2019; BCA, 2021).

Conclusion

The threat of cybercrime looms large over Nigeria's banking sector, with devastating financial consequences and erosion of customer confidence. The industry has witnessed a surge in cyber-attacks, resulting in substantial monetary losses, with a notable example being the over ₦15 billion lost to cybercrime and electronic fraud in 2018 (Ogunwale, 2020). The increasing reliance on digital banking has created an environment conducive to cybercrime activities, including hacking and malware attacks, which can compromise sensitive data and disrupt financial services (Ogunwale, 2020).

Forensic accountants and auditors are essential in the fight against cybercrime, employing specialized skills to identify and analyze digital evidence (Ali, 2024). By harnessing advanced data analytics and digital forensic tools, these professionals can uncover patterns indicative of financial crimes and detect anomalies that may indicate fraud (Bierstaker, Brody & Pacini, 2006). The integration of technologies like artificial intelligence and blockchain can enhance the efficiency and accuracy of forensic audits, enabling the detection of suspicious patterns and anomalies (Bierstaker et al., 2006).

To effectively combat cybercrime, banks must prioritize robust cyber security measures, including security protocols and customer education (Faboyede et al., 2023). The effective implementation of regulations, such as Nigeria's Cybercrimes Act 2015, can also contribute to reducing cybercrime rates (Ogunwale, 2020). By establishing strong policies and procedures, organizations can mitigate the risk of fraud and protect their assets and reputation (KPMG, 2013; PricewaterhouseCoopers, 2016).

Recommendations

A comprehensive approach is necessary to protect Nigeria's banking industry from cyber threats. This involves investing in robust cyber security measures, including advanced threat detection systems and customer education initiatives. Collaboration between the government and banking industry is crucial in implementing effective regulations and staying ahead of emerging threats (Sanusi, 2012).

Digital financial services can play a vital role in promoting financial inclusion in Nigeria, particularly in rural areas. By leveraging mobile phones and other digital platforms, the Central Bank of Nigeria can reach underserved populations and promote economic growth. Financial literacy programs are also essential in educating citizens on safe online banking practices and reducing the risk of cybercrime (Nkechika, 2022).

Promoting good corporate governance is critical for the stability and growth of Nigeria's banking industry. This involves addressing broader societal issues like corruption and poor leadership, while implementing strong policies and procedures related to financial management and transaction monitoring. By combining these efforts with technology, banks can reduce the risk of fraud and protect their assets (Adegbite, 2012).

To effectively combat financial crimes, forensic accountants and auditors should be engaged to utilize specialized techniques and analyze digital evidence. Building capacity and expertise in cyber security and digital forensics is essential for the government and banking industry to stay ahead of cyber threats and promote a safer financial system. This requires a collaborative effort to develop and implement effective strategies for detecting and preventing financial crimes.

References

Adegbite, E. (2012). Corporate governance in the Nigerian banking industry: towards governmental engagement. *Int. J. Business Governance and Ethics*, 7(3), 209-231.

Adeyemi, O.S.& Fagbemi, T. O. (2023). Forensic accounting techniques and fraud control in Nigerian banks. *International Journal of Accounting and Financial Reporting*, *13*(2), 115-133.

Ajzen, I.& Fishbein, M. (1980). Understanding attitudes and predicting social behaviour>Englewood Cliff, NJ: Prentice-Hall.

Akintoye I.R (2008). *The basics of environmental and forensic accounting*. Unique Educational Publishers.

Akintoye, I.R. (2008).*The basics of environmental and forensic accounting.* Unique Educational Publishers, ISBN 987-8047-61-0

Albrecht, W.S., Albrecht, C. & Albrecht, C.C. (2008). Current trends in fraud and its detection: A global perspective. *Information Security Journal*, *17*. Available at www.ebscohost.com.

Ali, X. (2024). Role of Forensic Accounting in the Era of Cyber Scam: New approaches and Techniques. *Int J Account Res*. 12:390.

Al-Shaikh, A, & Al-Adeem, K. (2023). Exploring the current state of forensic accounting in Saudi Arabia and possible ways of elevating it to assist the government fighting corruption. *Journal of forensic Accounting Profession*, 3(1), pp. 1-37.

Alvarez, R. (2021, Sept 2). Cyber-enabled crime vs. Cyber dependent crime. IPProbe.Global. Available athttps://ipprobe.global/2021/09/02/cyber-enabled-crime-vs-cyber dependentcrime/#:~:text=#:~:text=%E2%80%9CCyber%2Denabled%20crime%20is %20traditional,ransomware%2C%20DDoS%20attacks%20and%20malware.

American Institute of Certified Public Accountants (AICPA). (2006). Audit risk exposure standards. Statements of Auditing Standard.

Association of Certified Fraud Examiners. (2008). Report to the nation on occupational fraud abuse. Austine: Tax Association of Certified Fraud Examiners.

Bandakkanavar, R. (2020, June 19). Causes of cybercrime and preventive mechanism. Krazytech. Available from https://krazytech.com/technical-papers/cyber-crime

BCA. (2021). Pokok-Pokok Pedoman Penerapan Strategi Anti Fraud. Available at https://www.bca.co.id/-/media/Feature/Report/File/S8/Kebijakan-GCG/Pokok-Kebijakan -Anti-fraud.pdf

Bierstaker, J. L., Brody, R. G., & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. Managerial Auditing Journal, 21(5), 520-535. Available athttps://doi.org/10.1108/02686900610667283

Brytting, T., Minogue, R. & Morino, V. (2011). The Anatomy of Fraud and Corruption: Organizational Causes and Remedies. [Online]. Gower Publishing Ltd.

Carrier, B. (2003). Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers.*International Journal of Digital Evidence, Volume 1, Issue 4.*

Centre for Forensic Studies. (2010). Nigerian Institute of Advanced Legal Studies Lagos, Nigeria

Roundtable on the Role of Forensic and InvestigativeAccounting:

Challenges For The Banking Industry 19th July.
Chen, K. Y. & Elder, R. J. (2007). Fraud Risk Factors and the Likelihood of Fraudulent Financial Reporting: Evidence from Statement on Auditing Standards No. 43 in Taiwan, Working paper.
Coenen, T. (2005). *Forensic accounting, a new twist on bean counting*.
Crumbley, D. L. (2012). Forensic accounting older than you think. *Journal of Forensic Accounting, 4(*3):132-41.
Crumbley, D.L., Heitger, L.E., & Smith, G.S. (2005). Forensic and investigative accounting. CCH Group, Chicago, IL
Dada, Samuel O., & Owoeabi, S.A. (2013). Forensic Accounting a Panacea to Alleviation of Fraudulent Practices in Nigeria. *International Journal Business Management Economic Research,* 4 (5).
Degboro, D. & Olofinsola, J. (2007). Forensic accountants and the litigation support engagement. *Nigeria Accountant*, 40 (2), 49-52.
Deloitte. (2019). Fraud Risk Management. Deloitte Insights. https://doi.org/10.1108/DELOITTE-01-2019-0003
Dhar, P. & Sarkar, A. (2010). Forensic accounting: An accountant's vision. *Vidyasagar University J. Commerce*, 15(3), 93-104.
Ebelogu, C. U., Ojo, S. D., Andeh, C. P.,& Agu, E. O. (2019). Cybercrime, its adherent negative effects on Nigerian youths and the society at large: Possible solutions. *International Journal of Advances in Scientific Research and Engineering (IJASRE)* 5(12), 155-164.
Eleanya, F. (2021 Feb 16). Cyber fraud rises 534% as Nigerian banks lose ₦3.5 billion. BUSINESSDAY. Available atwww.businessday.ng/banking-finance/article/cyber- fraud rises-534-as-Nigerian-banks-lose-n3-5bn/
Enofe, A. O., Utomwen, & Danjuma (2015). The role of forensic accounting in mitigating financial crimes. International Journal of Advanced Academic Research.*International Journal of Economics and Business Management*, 1(7)1-10.
Europol. (2019, Oct 9). Internet Organized Crime Threat Assessment. Available at internet-organized-crime-threat-assessment-iocta-2019
Eze, P. A. U. (2021). Challenges of cybercrime on online banking in Nigeria: A review. International Digital Organization for Scientific Research (IDOSR).*Journal of Art and Management* 6(1), 63-69.
Faboyede, O. S., Ogunniyi, O., Atanda, O., Dahunsi, O. & Balogun, Z. (2023). Cybercrime Threats in the Nigerian Banking Sector and the Way Forward. *Ilorin Journal of Criminology and Security Studies* Vol.1, No.2, December, pp. 31-48.
Fadairo-Cokers, O. A. & Ibrahim, G. U. (2021). Impact of cybercrime on selected Deposit Money Banks (DMBS) in the Federal Capital Territory (FCT). *International Journal of Advanced Research in Statistics, Management and Finance* 8(1)
Goni, O., Ali, H., Showrov, Alam, M., &Shameem, A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, 1(2), pp. 29-39. Available athttps://doi.org/10.5281/zenodo.6499991
Goosen, G. Beaver, W., & Landsman, W. (1999). The relevance of the value of relevance literature for financial accounting standard setting: another

review. *Journal of Accounting and Economic,*. 31, 77-104.
Gutman, G. S. (1996). *Preventing financial fraud through forensic accounting*. The Chartered
Hassan, M. M., & Sanni, A. M. (2023). Enhancing Fraud Detection in Nigerian Banks Through Forensic Accounting. *Journal of Banking Regulation*, 24(3), 243-259.
Honigsberg, C. (2020). Forensic Accounting. *Annual review of law and social science*, 16(1), pp. 147-164.
Hooper, M. J,. & Pornelli, C. M. (2010). Deterring and detecting financial fraud: A platform for action. Available athttp://www.thecaq.org/docs/reports-and- publications/deterring-and-detectingfinancial-reporting-fraud-a platform-for- action.pdf?
Ibikunle, F. & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: Challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE)* 1(1), 100-110.
Kankpang, A. K., Nkiri, J. E., & Uket, E. E. (2018). Effect of employee dishonesty and fraud on profitability of manufacturing firms in Nigeria. *Asia Pacific Journal of Research in Business Management* 9 (7), 1 - 13.
Kaspersky (n.d.). *Black hat, White hat, and Gray hat hackers – Definition and Explanation*. Available atfrom https://www.kaspersky.com/resource center/definitions/hacker-hat- types
Kenyon, W. and Tilton, P. D. (2006). Potential red flags and fraud detection techniques: A Guide to Forensic Accounting Investigation, First Edition, John Wiley & Sons, Inc, New Jersey.
KPMG. (2013). Managing the Risk of Fraud and Misconduct. *KPMG Report*, 1(1), 1-24. Available athttps://doi.org/10.1108/KPMG-05-2013-0001
Krstić, J. (2009). The role of forensic accountants in detecting frauds in financial statements. *Economic and Organization* 6(3), 295-302.
Kumudenee, A. (2021, Nov 2). Malware Analysis Report. Researchgate. Retrieved from Available athttps://www.researchgate.net/publication/ 356406682_Malware_Analysis_ Report
Lister, L. M. (2007). *A Practical Approach to Fraud Risk:* Internal Auditors.
Love, J. (2018b, April 5). A Brief History of Malware – Its Evolution and Impact. Lastline. Available athttps://www.lastline.com/blog/history-of-malware-its-evolution and-impact/
Marianne O (2011). Forensic accounting and the law: The Forensic Accountant in the Marion hecht and Maryellen Redmond (2010) Unveiling the Mystery of Forensic Accounting. Oregon Society of Certified Public Accountants. Published by Accounting Today
Moorthy, K.M., Seetharaman, A., Mohamed, Z., Gopalan, M., & Lee Har San, L.H. (2011). The Impact of Information technology on Internal auditing. *African Journal of Business Management,* Vol. 5(8), pp.3523-3539.
Muhammad, S. I. & Kiru, M. U. (2017). A situational analysis of cybercrime and its economic impact in Nigeria. *International Journal of Computer Applications* 169(7), 19-29.
Muhammad, S. I. & Kiru, M. U. (2017). A situational analysis of cybercrime and its economic impact in Nigeria.

International Journal of Computer Applications 169(7), 19-29.
Murdock, H. (2008). The Three Dimensions of Fraud: Internal Auditors. Available at www.emerald.com.
Nayak, S. D. (October 2013). Impact of Cyber Crime: Issues and Challenges. 6(2).
Nkechika, C. G. (2022). Digital Financial Services and Financial Inclusion in Nigeria: Milestones and New Directions. *Economic and Financial Review Volume* 60/4 December, pp. 151-170.
Ogbonnaya, M. (2020, Oct 19). *Nigeria: Cybercrime in Nigeria Demands Public-Private Action*. All Africa. Available at https://allafrica.com/stories/202010200103.html
Ogunwale, H. (2020). The Impact of Cybercrime on Nigeria's Commercial Banking System. Researchgate. Retrieved from www.researchgate.net/publication/347388290
Okoye, E. I. (2013). Forensic accounting: A tool for fraud detection and prevention in the public service. A study of selected ministries in Kogi State. *International Journal of Academic Research in Business and Social Sciences,* 3(4), 1–18.
Okpo, S. A., & Simeon, U. J. (2023). The role of forensic accounting in mitigating against cybercrimes during the covid-19 pandemic era: issues and perspectives. *GPH-international journal of social science and humanities research*, 6(07), 09-23.
Oloruntoba, S. R., &Oyedokun, O. I. (2023). Forensic Accounting and Cybercrime Prevention in Listed Deposit Money Banks in Nigeria. *The Akungba Administrators and Management Scientists (TAAMS),* Volume 1, Issue, pages 15-26.
Onuora, A. C., Uche, D. C., Ogbunude, F. O., & Uwazuruike, F. O. (2017). The challenges of cybercrime in Nigeria: An overview. *Akanu Ibrahim Federal Polytechnic Unwana, Ebonyi (AIPFU) Journal of School of Sciences* (AJSS), 1(2), 6-11.
Oyedokun, G. E., Enyi, E. P., Dada, Ajibade, A. T., Igbaraola, A. F.,& Waluyo, W. (2019). Financial Statements' Integrity and Forensic Accounting Techniques. *Journal of business ethics* 139, 197-214.
PricewaterhouseCoopers. (2016). Global Economic Crime Survey. PwC, 6(3), 1-40. Available athttps://doi.org/10.1108/PWC-09-2016-0002
Rahman, M.J., Xuan, J., Zhu, H. & Hossain, M.M. (2023). Accounting fraud and corporate sustainability: Chinese listed companies. Journal of Financial Crime, Vol. ahead-of-print. doi:Available at https://doi.org/10.1108/JFC-02-2023-0035.
Sanusi, L. S. (2012). Banking Reform and its Impact on the Nigerian Economy. Being a Lecture delivered at the University of Warwick's Economic Summit, UK 17th February. *CBN Journal of Applied Statistics* Vol. 2 No.2.
Singleton, T. W., Bologna, G. J., Lindquist, R. J., & Singleton, A. J. (2006). *Fraud auditing and forensic accounting,* 3rd Ed., John Wiley & Sons, Inc, New Jersey.
Slavin, N. B. (2020). Empirical analysis on the use of forensic accounting techniques in curbing creative accounting. *International Journal of Economics Commerce and*

Management United Kingdom, 3(1): 1-15.
Thainkaraya, D. & Somasundaram, J. (2019). Forensic accountants and the litigation support engagement. *Niger Account*,40(2): 49-52.
Vona, I. W. (2008). *Fraud Risk Assessment: Building a Fraud Audit Programme*. Hoboken, New Jersey: John Wiley and Sons.
Zysman, A. (2004). *Forensic Accounting Demystified*. World Investigators Network Standard Practice for Investigative and Forensic Accounting Engagements.