



## Prevalence of Cyber Fraud and Economic Security in Nigeria: Issues and Perspective, Crosssectional Analysis

BATURE Sunday Ali<sup>1</sup>, Prof. UMAR Shehu Usman<sup>2</sup> &, Mohammed Ayuba Oche<sup>3</sup>

*Institute of Governance and Development Studies, Nasarawa State University, Keffi<sup>1</sup>, Department of Political Science, Nasarawa State University, Keffi<sup>2</sup>, Department of Sociology, Federal University, Lafia, Nasarawa State<sup>3</sup>*

Date of Submission: 14-02-2026

Date of Acceptance: 27-02-2026

### ABSTRACT

This study is to examine the impact of cyber fraud on economic security in Abuja, Nigeria, existing literature, literature was reviewed thematically, the study was anchored on the fraud diamond theory. The study identified massive youth unemployment as the push for the proliferation of cyber fraud in Nigeria. The study concluded that the existing literature on the effectiveness of regulatory bodies in combating advance fee fraud, particularly in Nigeria, reveals several key gaps. While there is extensive analysis of legal frameworks and regulatory provisions, there is limited exploration of the actual implementation and enforcement of these laws. Comparative analyses of regulatory bodies, especially with international counterparts, are lacking, as are studies on the impact of corruption within regulatory bodies themselves. The study recommends that government should reviewed existing and new development policies and programmes to be youth friendly as this would enable the youth to develop sense of belonging and adhere to the dictates of the respective social institutions in Nigeria.

**Keywords:** Trend, Cyber, Cyber Fraud, Economic, Economic Security

### I. Introduction

Globally, cyber fraud has resulted in billions of dollars in financial losses, severely impacting businesses and governments alike. In response, nations are making significant efforts to fortify their cybersecurity systems, recognizing that unchecked cyber fraud can destabilize economies, destroy critical infrastructures, and lead to substantial losses in national revenue (Fischer, 2009; Babayo et al., 2021). The electronic market is now open to everybody, including criminals. It was projected that by 2020, global Cyber security spending will reach \$170 bn, a 126% increase from \$75bn in 2015. According to the World Economic Forum's report

Globalization 4.0, "More organizations than ever are conducting business online" (Broeders, 2021). However, alongside these benefits, the rise of the Internet has also introduced significant security challenges, one of the most concerning being cyber fraud. Cyber fraud involves illegal activities such as identity theft, hacking, online scams, and financial fraud perpetrated digitally. It is a subset of cybercrime that specifically targets economic systems, causing substantial financial harm to individuals, organizations, and nations.

Nigeria, as the most populous country in Africa, is particularly vulnerable to cyber fraud. With over 200 million people and a rapidly growing digital economy, the country has witnessed a surge in cybercriminal activities that directly threaten its economic security. The proliferation of internet in Nigeria has indeed come with unintended consequence, as a haven for criminals. Cybercrime has remained a challenging issue despite increasing awareness and attention to addressing the menace in Nigeria and across the globe. Nigeria is ranked among the top countries in the world for internet fraud, which has contributed to massive financial losses and a significant loss of investor confidence (Federal Bureau of Investigation, 2022).

In 2021, Nigeria's estimated loss to cyber fraud was over \$649 million, a figure that continues to rise annually (Adeniyi, 2021). The consequences of this are multifaceted: the country's financial institutions are continually targeted, sensitive data is compromised, and critical infrastructures essential to the economy are at risk. Moreover, Nigeria's global reputation has been tarnished, as it is often associated with infamous "419" fraud schemes and other cyber-related crimes (Adomi & Igun, 2008). For instance, Cybercrime accounted for about 43% of total monetary loss due to fraud in 2016. These losses have negative impacts on individuals, businesses and the government in terms of welfare losses, business disruption, profit reduction/rising operating cost and revenue losses.



However, several factors has been adjudged to contribute to the prevalence of cyber fraud in Nigeria, including high unemployment rates, widespread poverty, and weak governance structures. These economic challenges have driven many young Nigerians to engage in cybercrime as a means of survival (Idowu, 2021). Despite efforts by the Nigerian government to address these issues such as the establishment of the National Cybersecurity Policy, the Economic and Finanacial Crime Commission, and the National Information Technology Development Agency (NITDA) cyber fraud remains a critical challenge. The Nigerian government has also implemented legislative frameworks aimed at curbing cybercrime, including the 2015 Cybercrime Act, which outlines strict penalties for cybercriminal activities. However, the effectiveness of these measures is often hampered by inadequate cybersecurity infrastructure, limited enforcement, and a lack of public awareness.

#### Statement of Problem

Over time, Nigeria has become a hotspot for cybercrime in Africa, with the nation experiencing a sharp rise in the frequency and sophistication of cyberattacks. Cybercriminals engage in various illicit activities, including phishing, hacking, identity theft, and the notorious "419" advance fee fraud scams. According to Mphatheni and Maluleke (2022), Nigeria consistently ranks among the top African countries impacted by cyberattacks, with hundreds of millions of incidents reported annually. The financial toll of these crimes is substantial; for instance, Nigeria lost an estimated N198.6 billion (\$649 million) in 2017 alone due to cyber fraud (Adepetun, 2018), and by 2018, the losses had escalated to around \$800 million (Week, 2019, as cited in Ali, 2025).

Scholars such as Adepetun (2018), Ohwovorirole (2019), and Akinyetun (2021) have highlighted the country's vulnerability to cyberattacks, pointing to hundreds of millions of incidents each year. These attacks have caused significant financial setbacks, including an average annual loss of N127 billion by 2019. Available statistics indicated that cybercrime in Nigeria has recorded 174% increase from 2022 till date. It further revealed that phishing and scam top the ranking. Nigeria now occupies the 5<sup>th</sup> position in the global cybercrime index, there is 65% increase in data breaches in the first quatre of 2023. The report further indicate that cybercrime losses are estimated to reach \$10.5 trillion annually by the last quatre of 2025 with Nigeria's growing digital economy vulnerable to these threats. Small and medium scale enterprises are

the major victims of cyber-attacks. With 87% experiencing phishing attacks in 2022, compared to 37% in 2021. It was further added that 71% of Nigeria's firms were hit with ransomware in 2021 with businesses paying an average of \$706,452 in ransom to cybercriminals (BusinessDay, 2022, Global Cybercrime Index, 2025). While this challenge persists, policies and strategies has failed to reversed the trends, there is paucity of empirical studies on the subject matter.

#### Research Questions

- i. What is the trend and causes of cyber fraud in Abuja?
- ii. What is the impact of cyber fraud on economic development in FCT Abuja?
- iii. What are the efforts of government in curbing cyber fraud in Abuja?

#### Research Objective

The major objective of this study is to examine the impact of cyber fraud on economic security in Abuja. The specific objective is to:

- i. Determine the causes and trends of cyber fraud in Abuja
- ii. To ascertain the impact of cyber fraud on economic development in FCT Abuja
- iii. To determine the efforts of government in curbing cyber fraud

#### Concept of Cyber Fraud

Cyber fraud refers to the deceptive use of computers or the internet to mislead individuals, steal their money, or cause other detrimental effects. This form of fraud encompasses a wide range of tactics aimed at defrauding users online by stealing their personal information or financial assets (Ali, 2025). Cyber fraud can be categorized into two main types: **direct** and **indirect** fraud. **Direct fraud** involves immediate actions such as employee theft, unauthorized use of credit or debit cards, and using false identities to conceal illicit financial activities. In contrast, **indirect fraud** includes more complex schemes, such as tricking individuals into willingly sharing their personal information through phishing emails, or hacking into computer systems to steal data. Although both types of fraud result in financial losses, they differ in the method of execution and the level of interaction between the victim and the fraudster (Holt & Lampke, 2020). However, this paper conceived cyber fraud as the manipulation of digital resource for personal gain against individual, and or group.

#### Economic Security



Economic security is a multifaceted economic concept influenced by the dynamic environment of material production and the external and internal threats to the economy. It is a fundamental component of national security, which is the primary responsibility of the state, executed in close collaboration with economic agents. National security reflects the capability of the state's political, legal, and economic institutions to safeguard the interests of key entities within the framework of national economic traditions and values. Consequently, its development should be considered within the broader context of forming a secure national state (Litvinenko, 2013). Absolute economic security, free from any external or internal threats to the national economy, is unattainable. The main factors contributing to a country's economic security include its geographical location, natural resources, industrial and agricultural potential, socio-demographic development, and the quality of public administration. Nations such as Russia, the United States, Japan, China, and members of the European Union possess significant industrial potential, agricultural production, and natural resources, alongside advantageous geographic positions, all of which bolster their economic security (Grigoreva & Fesina, 2013). In this study economic security, "economic security" refers to the state of a country's economy characterized by stability, resilience, and the ability to withstand external shocks. Economic security encompasses various aspects, including but not limited to the protection of individuals, businesses, and the government from financial risks and vulnerabilities posed by fraudulent activities.

### Economic Causes of Cyber Fraud

Hassan et al. (2012) contends that high unemployment, urbanisation, lack of awareness of cybersecurity, poverty, the proliferation of cybercafes, corruption and inadequate enforcement of existing laws against cyber criminals by law enforcement agencies coupled with weak judicial systems which do not deter potential offenders from engaging in illegal activities online are factors contributing to the proliferation of cybercrime in Nigeria.

Unemployment, coupled with poverty, is a major factor contributing to the prevalence of cybercrime in Nigeria. The problem of unemployment in Nigeria is complex and multifaceted. The formal job sector in Nigeria is small and cannot accommodate many job seekers. This has resulted in a situation in which many individuals are underemployed or unemployed. Statistic has revealed that the youth are

disproportionately affected, with many graduating from schools and universities with computer and internet competency but without lacking employment prospects (Olowu, 2009; Bello, 2018). Hence, Nigeria has a low standard of living and people living below the poverty line. In this context, the Internet has become a source of optimism for many young Nigerians. Numerous individuals use the Internet to establish businesses, sell products, and offer services, thereby providing an avenue for entrepreneurship and self-employment (Adesina 2017; Bello, 2018). However, the dearth of formal employment opportunities, poverty and the high cost of establishing a business makes some young people resort to cybercrime as subsistence (Makeri, 2017).

Ibrahim (2016) in a study noted that the causations of crimes that are relevant in the cyberspace concurrently impact in the physical space and vice versa. This paper aims to explore parents' perceptions of the factors that cause socioeconomic cybercrime in Nigeria. Despite a long-standing view that the juvenile offenders of today could become the hardened criminals of tomorrow, and the conclusions of a number of developmental theories on the stability of delinquency across the life course, the existing data on cybercrimes in Nigeria have principally been derived from studies involving university students. Yet, individuals' moral-standard-levels, which shape their offending capacities, are mostly developed in childhood. The empirical basis for this paper is face-to-face interviews with 17 Nigerian parents regarding children's vulnerability to involvement in cybercrime. Drawing upon qualitative data, this paper argues that a complex web of familial factors and structural forces, alongside cultural forces, explains the degree of cybercrime involvement on the part of Nigerian youths.

In another study, Molokwo (2022) conducted an investigation into some socioeconomic predictors of cybercrimes among Nigerian youths in Ibadan Metropolis. Descriptive research design of survey type was adopted. Participants were one hundred and fifty youths within the age range of 18-35 selected through convenience sampling. Four hypotheses guided the study. Socioeconomic Predictors of Cybercrime Questionnaire (SOPOC-Q) designed and validated by the researcher was used to collect data for the study. Data collected were subjected to analysis using frequency count, percentage and analysis of variance (ANOVA). Results shows that internet [ $F_{(1,148)}=9.617$ ;  $p<.002$ ] is the most significant contributor to cybercrime followed by peer influence [ $F_{(1,148)}=1.768$ ;  $p<.186$ ] and unemployment [ $F_{(1,148)}=1.829$ ;  $p<.176$ ] were significant contributors to cybercrime among the



participants while economic hardship [ $F_{(1,148)}=.66$ ;  $p<.79$ ] was not significant. Stringent measures to curtail the activities of internet fraudsters, early orientation of children on the need to avoid bad and wayward peers and the need for government and non-governmental organization to provide jobs for unemployed individuals were recommended.

In a similar vein, Wall (2013) proposed seven different motivational subsets, based on: self-satisfaction; the need for peer respect; to impress potential employers; criminal gain or commercial advantage; revenge; distance from victim; politically motivated protest. These motivational signposts help to illustrate that the specific motivations behind cybercrime are diverse.

### Trends and Patterns of Cyber Fraud

Cyber fraud remains a lucrative and illegal business in cyberspace. In Nigeria, weblinks are designed to unlawfully access users' data (PINs and personal details) by requesting naive computer users to fill online forms (Unini, 2019). In Nigeria, cyber fraudsters send emails through conventional messages and social media platforms to claim that a potential victim has been named as a beneficiary for the will of an estranged relative and stands the chance of inheriting millions of naira and large property. An individual may also be phished through online charity, where fraudulent people host websites of charity organizations soliciting monetary donations and materials to these organizations that do not exist. Fraudsters also host fake charity social network pages built for soliciting money from unsuspecting individuals. Sometimes, they claim that a particular person is sick and needs money for medical bills. They even go as far as displaying pictures evidencing the sick condition of the person on fake websites. Hence, the donation from kind-hearted individuals, who get unknowingly exploited, profits the cybercriminals.

The Western Union money transfer scheme has also been used to perpetrate cyber fraud in Nigerian banks (Wall, 2007). Western Union money transfer is an online money transfer service that allows customers to send and receive money from all over the world via Western Union Agent locations. Fraudsters use foreign names that are not recognised by any bank and align with compromised banking staff to access funds. A successful fraud cannot be easily executed without an insider within the bank. This is because the facilitation of payment is dependent upon the insider who does not alert the relevant security agencies. For every successful fraudulent transaction, the insiders also get their share. It was in a bid to checkmate such

fraudulent practices that the Central Bank of Nigeria (CBN) introduced the Bank Verification Number (BVN) scheme in 2014, to prevent cyber theft and other crimes. Notwithstanding such policy intervention, the perpetration of such illegal activities continues (Ebem et al., 2017).

In 2014, Dzomira, there are numerous ways to commit identity theft. Identity theft involves stealing credit card information during legitimate transactions, according to Pal, Herath, and Rao (2019). When a customer's credit card information is concealed during a transaction, these fraudulent transactions typically take place in those businesses. The card will be scanned by the con artists using a "wedge" or review device, an electronic gadget that captures all the data on the magnetic stripe. Criminals can trick victims into providing credit card information or steal merchant information as sophisticated ways to obtain credit card details. However, Dzomira (2014) contends that even though losses to businesses and banks resulting from credit card fraud continue to rise, there aren't enough laws in place to stop this crime. The majority of people will suffer from technology in order to gain from it. Phishers create websites that look like legitimate websites so that victims can enter sensitive data like usernames, passwords, and credit card numbers. Frequently, emails are sent to recipients asking for the disclosure of sensitive information or the opening of investigations, and when that information is revealed, criminals alter the online environment. Phishing and phishing are two variations on phishing that deceive targets through text messages and phone calls (Dzomira, 2014).

Businesses and other traders may also be the targets of this scam type. Depending on the type of business, e-commerce sites are frequently targeted because, depending on the content, they may contain valuable information or payment information that can be used for fraudulent purchases (Tendülkar, 2013). Internal fraud is typically committed by corporate con artists using "pen and paper". However, as the business world became more computerized, the same criminals started using computer scams to pull off the same con.

According to Onodi, Okafor, and Onyali (2015), embezzlement entails using funds or assets that have been entrusted to employees for their own use (for instance, employees may use the company's computer payment system to transfer data or money from the company's bank account to a personal account). Furthermore, financial institutions might grant authorized staff members access to private customer data that they can use to log into online customer accounts. Employee fraud is made more



convenient as a result. The salami technique is a technique that scammers sometimes use to steal small sums of money. Long-term changes to the program are gradual and difficult to notice. This type of fraud, which involves the monthly withdrawal of several dollars from the accounts of numerous customers, is an example (Tendelkur, 2013).

#### **Impact of cyber fraud on economic development**

Amughoru et al. (2022) examined the impact of advanced fee fraud and money laundering control on the economic performance of Nigeria from 1987 to 2020. Data on advanced fee fraud, money laundering, and financial performance indicators (gross domestic product, foreign direct investment, and balance of payment) were collected from the Central Bank of Nigeria statistical bulletin, National Bureau of Statistics, and World Bank Indicators. The data were analyzed using the Auto Regressive Distributed Lag (ARDL) Bound test. The results showed that advanced fee fraud and money laundering control significantly and negatively affect economic performance. This negative impact may be attributed to the poor fraud control systems implemented by the government, which are inadequate to prevent fraudulent activities. Based on the study's findings, it was recommended that policymakers institute more effective and proactive advanced fee fraud control mechanisms aimed at preventing fraudulent activities and taking legal action against fraudsters in the country.

Lawal et al. (2017) investigates the link between fraud and the business cycle in Nigeria using primary data sourced from questionnaires administered to both fraudsters and fraud managers. The study is based on the premise that Nigeria is in a recession and has been recently described as "fantastically corrupt." Understanding the link between fraud and economic behavior would provide an in-depth understanding of fraud levels in different phases of the Nigerian economy and help improve the fraud management system in Nigeria, which is believed to have significant consequences on the nation's economy.

The results show that although there is a significant relationship between fraud and the business cycle in Nigeria, the level of fraud committed does not solely depend on the presence of either expansion or recession in the economy. Instead, there is an identified range of fraud that might increase during adverse economic conditions. Sarriá et al. (2019) examines the abusive practices within the financial system over recent decades that constitute fraud. The study aims to compare the prevalence of psychological distress and health-related quality of life based on exposure to financial

fraud and its economic impact on family finances. The City of Madrid Health Survey 2017 included specific questions on exposure to financial fraud, administered to half of the participants ( $n = 4425$ ). Mental health need was defined by a score greater than two on the 12-item version of the Goldberg health questionnaire. Health-related quality of life was assessed using the Dartmouth Coop Functional Health Assessment Charts/WONCA (COOP/WONCA). The prevalence of financial fraud was 10.8%. The prevalence rate ratio for mental health need in those experiencing severe economic impact due to fraud was 1.62 (95% CI 1.17–2.25; reference: no fraud), after adjusting for age, sex, social class, and immigrant status. Women experienced a decreased quality of life even with a moderate impact of fraud, while men experienced a decreased quality of life with severe economic impact. This study contributes to the growing body of literature showing the effects of economic shocks on health as a result of financial fraud. Smith (2009) examines the current evidence on the cost, extent, and awareness of consumer fraud in Australia. In 2008, the ABS found that approximately five percent of the Australian population reported being victimized by consumer scams, with personal losses reaching almost \$1 billion. This paper compares the ABS survey findings with those gathered by the AIC during the annual fraud awareness-raising activities conducted by the Australasian Consumer Fraud Taskforce. In 2008, a self-selected sample of 919 respondents to the AIC's online survey reported being victimized by a wide variety of scams, including fictitious lotteries, phishing scams, financial advice scams, and other attempts to elicit personal information. Individuals from all age groups were targeted in these scams, with older Australians being victimized to a similar extent as those in their middle years. By understanding the nature and scope of these risks, consumer protection and regulatory agencies can tailor their fraud prevention activities to maximize their impact, thereby reducing consumers' susceptibility to offers that are too good to be true.

Abubakari (2021) explores the rapid and consistent growth of cybercrime and its economic consequences, which have garnered scholarly attention from organizations, governmental bodies, and researchers in academic environments. Cybercrime is recognized for its wide-ranging impact on the economic conditions of organizations, political economies, and individuals. The study's main objective is to systematically review and outline the current state of research on the determinants of cybercrime adaptation, the consequences of cybercrime, and the hindrances of cybercrime



policies in Anglophone West Africa. The database search was conducted between December 20, 2020, and January 9, 2021, across three electronic databases: Scopus, Sage, and Google Scholar. Articles were included if they were written in English and addressed the issue of cybercrime in Anglophone West Africa, focusing on either the consequences or reasons for cybercrime adaptation or the hindrances of cybercrime policies. A total of 24 articles were included in the study. Among these, 13 addressed cybercrime consequences, 6 tackled reasons for cybercrime adaptation, and 6 addressed hindrances of cybercrime policies and regulations. The finding reveals that cybercrime has micro-, meso-, and macroeconomic impacts in West Africa. At the micro level, citizens lose both financial resources and international travel opportunities. E-businesses at the meso level suffer financial and reputational victimization. At the macro level, countries with prevalent cybercrime experience reduced foreign investment, damage to international reputation, and financial challenges. Additionally, the review shows that cybercrime perpetrators lose focus on education. The study also indicates that the reasons for cybercrime adaptation are associated with economic strains and corruption at the governmental level. Hindrances of cybercrime policies revolve around corruption, government interference, ineffective implementation of cybercrime laws, and inconsistencies in cybercrime policy content. The author recommends further studies to include articles in different languages and to explore how cybercrime reflects in the lives of perpetrators and their perspectives on mitigative interventions. Additionally, future studies should aim to understand how cybercrime is organized in African societies to enhance the effectiveness of cybercrime mitigation processes in Africa.

#### **Efforts of government in curbing cybercrime in FCT Abuja**

Oriola (2005) examines the regulatory framework addressing fraudulent email scams, specifically advance fee fraud originating in Nigeria. The paper analyzes relevant provisions of the Criminal Code Act, the Advance Fee Fraud and Other Related Offences Act, the Financial Crimes Commission Act, and the Money Laundering Prohibition Act, which collectively aim to curb Internet scams. The term '419' has become synonymous with email scams, contributing to Nigeria's notoriety in this regard. The paper highlights loopholes and inadequacies in the legislation, noting that the boom in Internet scams in Nigeria is less due to insufficient regulation and more

due to the lack of enforcement of existing laws. Oriola emphasizes the need for international assistance in combating such crime, advocating for greater systemic transparency, enhanced legal enforcement, intensified public enlightenment campaigns, and technological approaches to address the menace of advance fee fraud on the Internet.

Smith et al. (1999) discuss the evolution of deceptive practices that trick individuals into parting with their money, focusing on a variant of the traditional "advance fee" scheme predominantly carried out by Nigerian nationals. This scheme, promising quick wealth to those willing to succumb to temptation, has led to an estimated \$5 billion being stolen worldwide over the past decade. The study analyzes the escalation of this phenomenon in terms of frequency, seriousness, and the nature of the criminality involved. It explores the reasons behind its development and the limited effectiveness of traditional law enforcement measures in controlling it. Despite extensive publicity on advance fee fraud, these offenses persist, driven by vulnerable and gullible victims and increasingly unscrupulous and violent organized criminals. What began as a simple adaptation of a traditional scheme has evolved into a sophisticated organized criminal operation with international links. Challenges in gathering evidence and prosecuting offenders in other jurisdictions have resulted in relatively few convictions. Nonetheless, global police services and governments are collaborating to address the issue. The use of electronic messaging complicates matters, enabling offenders to disguise their identities and reach larger numbers of potential victims. The authors suggest that effective education about the risks involved may be a more appropriate response than pursuing trans-jurisdictional criminal proceedings.

Abubakari (2021) explores the rapid and consistent growth of cybercrime and its economic consequences, garnering scholarly attention from organizations, governmental bodies, and researchers. Cybercrime significantly impacts the economic conditions of organizations, political economies, and individuals. The study systematically reviews and outlines the current state of research on the determinants of cybercrime adaptation, its consequences, and the hindrances of cybercrime policies in Anglophone West Africa. A database search conducted across Scopus, Sage, and Google Scholar included 24 articles addressing cybercrime in Anglophone West Africa. The findings indicate that reasons for cybercrime adaptation are linked to economic strains and governmental corruption. Hindrances of cybercrime policies revolve around corruption, government interference, ineffective



implementation of laws, and policy inconsistencies. The author recommends further studies to include articles in different languages and to explore how cybercrime affects perpetrators and their perspectives on mitigative interventions.

### **Theoretical Framework: Fraud Diamond Theory**

The Fraud Diamond Theory, proposed by Wolfe and Hermanson in 2004, expands on the Fraud Triangle (which includes pressure, opportunity, and rationalization) by adding a fourth element, capability, to provide a more comprehensive framework for understanding fraud (Wolfe & Hermanson, 2004). In the context of cyber fraud and its impact on economic security, the Fraud Diamond Theory is particularly relevant. Individuals may feel pressure due to financial difficulties, societal expectations, or personal circumstances, leading them to engage in fraudulent activities like cyber fraud. Economic hardships or the desire for quick wealth can create pressures that drive individuals to seek illicit means to alleviate their financial burdens. Cyber fraud thrives on the availability of opportunities, such as technological advancements that enable scammers to reach a global audience easily. The internet provides a platform for scammers to create deceptive schemes and target unsuspecting individuals, highlighting the importance of addressing vulnerabilities in systems and processes that allow for fraud to occur.

Scammers often rationalize their actions, believing that their behavior is justified or that they will not get caught. They may convince themselves that the victims are not actually being harmed or that the ends justify the means. Rationalization plays a significant role in perpetuating fraud and can be a barrier to deterring fraudulent behavior. The Fraud Diamond Theory introduces capability as a crucial element. It refers to the knowledge, skills, and resources needed to commit fraud successfully. In the context of cyber fraud, scammers must have the technical expertise to create convincing fraudulent schemes and the ability to execute them effectively, often leveraging digital technologies and sophisticated tactics. By considering these four elements together, the Fraud Diamond Theory provides a nuanced understanding of the factors contributing to fraud, including cyber fraud, and underscores the complexity of combating such crimes. Addressing these elements requires a multi-faceted approach that includes enhancing financial literacy, implementing effective fraud detection mechanisms, strengthening regulatory frameworks, and increasing awareness among the public to reduce the impact of cyber fraud on economic security.

## **II. Discussions**

Nigeria has become a hotspot for cybercrime in Africa, with the nation experiencing a sharp rise in the frequency and sophistication of cyberattacks. Cybercriminals engage in various illicit activities, including phishing, hacking, identity theft, and the notorious "419" advance fee fraud scams. According to Mphatheni and Maluleke (2022), Nigeria consistently ranks among the top African countries impacted by cyberattacks, with hundreds of millions of incidents reported annually. The financial toll of these crimes is substantial; for instance, Nigeria lost an estimated N198.6 billion (\$649 million) in 2017 alone due to cyber fraud (Adepetun, 2018), and by 2018, the losses had escalated to around \$800 million (Week, 2019). In 2022 cybercrime costs Nigeria's economy billions, with financial losses due to fraudulent operations reaching N273 billion (\$762 million). The banking sector is significantly affected, with phishing attacks and data breaches posing major threats. The economic impact of cyber fraud in Nigeria has been well-documented, with numerous studies focusing on the severe financial losses incurred by individuals, businesses, and government institutions. Scholars such as Adepetun (2018), Ohwovoriole (2019), and Akinyetun (2021) have highlighted the country's vulnerability to cyberattacks, pointing to hundreds of millions of incidents each year. These attacks have caused significant financial setbacks, including an average annual loss of N127 billion by 2019. Despite these broad assessments, there remains a distinct lack of research focusing on the specific impact of cyber fraud on key economic hubs like Abuja.

The Fraud Diamond Theory is highly relevant to the study on the impact of cyber fraud (CYBER FRAUD) on economic security. The theory's four elements—pressure, opportunity, rationalization, and capability—provide a comprehensive framework for understanding the dynamics of fraud, including cyber fraud, and its implications for economic security. In the context of the study, the theory can help explain why individuals engage in cyber fraud despite its illegal and unethical nature. For example, economic pressures, such as poverty or financial hardship, can drive individuals to seek quick and easy ways to make money, leading them to fall prey to cyber fraud schemes. Additionally, the internet and digital technologies provide scammers with the opportunity to reach a wide audience and execute fraudulent activities on a large scale, highlighting the role of opportunity in enabling cyber fraud. Rationalization may also play a part, as scammers may justify their actions by



believing that they are not causing harm or that their victims deserve to be deceived. Furthermore, the theory's emphasis on capability underscores the importance of scammers' skills and resources in carrying out cyber fraud effectively, particularly through the use of technology. Understanding these elements can inform strategies to prevent and combat cyber fraud, such as enhancing financial literacy, strengthening cybersecurity measures, and raising awareness about the risks of online fraud, ultimately contributing to greater economic security.

### III. Conclusion/Recommendations

The existing literature on the effectiveness of regulatory bodies in combating advance fee fraud, particularly in Nigeria, reveals several key gaps. While there is extensive analysis of legal frameworks and regulatory provisions, there is limited exploration of the actual implementation and enforcement of these laws. Comparative analyses of regulatory bodies, especially with international counterparts, are lacking, as are studies on the impact of corruption within regulatory bodies themselves. Additionally, there is a gap in understanding the technological capabilities and adaptation of regulatory bodies to combat evolving fraud techniques. The role of public-private partnerships, international cooperation, and the effectiveness of educational campaigns also require more in-depth investigation. Furthermore, there is a need for more quantitative assessments, longitudinal studies, and case studies to evaluate regulatory effectiveness over time and in specific contexts. Finally, the broader economic impacts of regulatory effectiveness on victims and society remain underexplored. Addressing these gaps could provide valuable insights into enhancing the effectiveness of regulatory bodies in combating advance fee fraud and other cybercrimes. Overall, while the Fraud Diamond Theory provides a useful framework for understanding fraud, it should be viewed as a starting point rather than a definitive explanation. Integrating insights from other theories and considering broader contextual factors can enhance its explanatory power and applicability. Consequently, this study recommends that government should reviewed existing and new development policies and programmes to be youth friendly as this would enable the youth to develop sense of belonging and adhere to the dictates of the respective social institutions in Nigeria.

### References

- [1]. Abubakari, Y. (2021): The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: a review. *Social Space Journal* pp 137-176
- [2]. Adeniyi, I.A. (2021). Cyber Security in Nigeria: Appraising Cybercrime, the Existing Legal Framework, the Challenges and the Way Forward. *SSRN Electronic Journal*. doi:<https://doi.org/10.2139/ssrn.3991151>.
- [3]. Ajoke, O. Z. (2014): Impact of Economic and Financial Crime Commission on the Economic Development of Nigeria. Bachelor's Thesis (Turku University of Applied Science) Degree Program in International Business International Business Management 2014
- [4]. Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, 27, 945-958.
- [5]. Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research*, 4(8), 1-19.
- [6]. Alao, D., Osah, G. and Eteete, A. (2019). Unabated Cyber Terrorism and Human Security in Nigeria. *Asian Social Science*, 15. doi:<https://doi.org/10.5539/ass.v15n11p105>.
- [7]. Amughoro, O. A. & Ijeoma, N. (2022): Advanced Fee Fraud, Money Laundering Controls and Economic Performance in Nigeria. *International Journal of Advances in Engineering and Management (IJAEM)* Volume 4, Issue 1 Jan 2022, pp: 719-728 www.ijaem.net ISSN: 2395-5252. DOI: 10.35629/5252-0401719728
- [8]. Babayo, S., Muhammad, Y., Usman, S. and Bakri, M. (2021). Cyber security and Cybercrime in Nigeria: the Implications on National Security and Digital Economy. 4(1), 27-61
- [9]. Bello, M. (2018). *Investigating Cybercriminals in Nigeria: a Comparative Study*. [online] 1library.net. Available at: <https://1library.net/document/y9mlr4jqinvestigating-cybercriminals-in-nigeria-a-comparative-study.html>.
- [10]. Bhasin, M. L. (2016). The role of technology in combatting bank frauds: perspectives and prospects. *Ecoforum Journal*, 5(2). <http://www.ecoforumjournal.ro/index.php/eco/article/view/412>
- [11]. Broeders, D. (2021). Private active cyber defense and (international) cyber security—



- pushing the line?. *Journal of Cybersecurity*, 7(1), tyab010.
- [12]. Button, M. Tapley, J. and Lewis, C. (2012). The fraud justice network and the infrastructure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice*, 13 (1), 37-61.
- [13]. Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of Information Law and Technology*.  
<http://go.warwick.ac.uk/jilt/2009//chawki>
- [14]. Chigozie-Okwum, C., Ugboaja, S., Micheal, D., & Osuo-Genseleke, M. (2017).
- [15]. Proliferation of cyber insecurity in Nigeria: a root cause analysis. *AFRREV STECH: An International Journal of Science and Technology*, 6(2), 53-60.  
<https://www.ajol.info/index.php/stech/article/view/161143>
- [16]. Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588 - 608.
- [17]. Drammeh, F. (2023): Trust and Fraud in Nigeria: A Comprehensive Analysis of Socioeconomic Factors and Regulatory Measures (June 10, 2023). Available at SSRN: <https://ssrn.com/abstract=4475135> or <http://dx.doi.org/10.2139/ssrn.4475135>
- [18]. Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, 4(2), 16-26.
- [19]. Ebem, D.U., Onyeagba, J.C. & Ugwuonah, G.E. (2017). Internet Banking: Identity Theft and Solutions -The Nigerian Perspective. *Journal of Internet Banking and Commerce*, 2 2(2), 1-15.
- [20]. Efiog, E. J., Inyang, I. O., & Joshua, U. (2016). Effectiveness of the mechanisms of fraud prevention and detection in Nigeria. *Advances in Social Sciences Research Journal*, 3(3).
- [21]. Glickman, H. (2005). The Nigerian "419" Advance Fee Scams: Prank or Peril? *Canadian Journal of African Studies / Revue Canadienne Des Etudes Africaines*, 39(3), 460-489.  
<https://doi.org/10.1080/00083968.2005.10751326>
- [22]. Grigoreva E., Fesina E., (2013). Economic Security as a Condition of Institutional Support of Economy Modernization. *World Applied Sciences Journal*, vol. 31, no. 5, pp. 940-948.
- [23]. Guariniello, C., and DeLaurentis, D., (2014). Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. *Procedia Computer Science*, 28, pp. 720-727.
- [24]. Hassan, A.B., Lass, F.D. and Makinde, J., (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology*, 2(7), pp.626- 631.
- [25]. Holt, T. J., & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, 1(1), 137-154.
- [26]. Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behaviour*, 35: 1, 20-40. DOI: 10.1080/01639625.2013.822209
- [27]. Hunton, P., (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), pp. 528-535.
- [28]. Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. In *2016 IEEE International Conference on cybercrime and computer forensic (ICCCF)* (pp. 1-9). IEEE. <https://ieeexplore.ieee.org/abstract/document/7740439/>
- [29]. Idowu, O.A. (2021). Cybercrimes and Challenges of Cyber-Security in Nigeria. 3(1), 1-12.
- [30]. Igwe, C. N. (2011) Socio-economic developments and the rise of 419 Advance-Fee Fraud in Nigeria. *European Journal of Social Sciences* March 2011 20(1):184-193.
- [31]. Ismagilov I.I., (2012). Strategic management of enterprise development in the conditions of formation of the network economy. *Kazan economic bulletin*, vol. 1, pp. 16-18.
- [32]. Lamensch, M. And Ceci, E. (2018): VAT fraud Economic impact, challenges and policy issues Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies: *PE 626.076 – October 2018 EN STUDY R*
- [33]. Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behaviour*, 126, 106979. doi:10.1016/j.chb.2021.106979
- [34]. Litvinenko A.N., (2013). Economic and national security: the problem of concepts correlating Scientific and technical statements,



- S.-Petersburg State Polytechnic University, *Economic sciences*, № 3 (173), pp. 9-15.
- [35]. Makeri, Y.A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), pp.315–321. doi:<https://doi.org/10.23956/ijarcsse/v6i12/01204>.
- [36]. Molokwu, A. N. (2022). Socioeconomic Predictors of Cybercrime among Nigerian Youths in Ibadan Metropolis. *Turkish International Journal of Special Education and Guidance & Counselling ISSN: 1300-7432*, 11(1), 61–68. Retrieved from <https://www.tijseg.org/index.php/tijseg/article/view/167>
- [37]. Nigeria Criminal Code, (2004), Federal Republic of Nigeria.
- [38]. Nissenbaum, H., (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, pp. 61-73.
- [39]. Ogham S. C. (2023): Scrutiny of the Legal and Regulatory Framework of e-commerce in Nigeria. *Nigerian Bar Journal*. [Ajol-file-journals\\_693\\_articles\\_254146\\_64](https://www.nigerianbarjournal.com/ajol-file-journals_693_articles_254146_64)
- [40]. Okpa, J. T., Ajah, B. O., & Igbe, J. E. (2020). Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology*, 14(2),460-478.<https://search.proquest.com/openview/dc68d59c9f55b14f96e5d089123de874/1?pq-origsite=gscholar&cbl=55114>
- [41]. Olowu, D. (2009). Cyber-Crimes and the boundaries of domestic legal responses: case for an inclusionary framework for Africa. *Journal of Information, Law & Technology*, 1.
- [42]. Oriola, T. A. (2005): Advance fee fraud on the Internet: Nigeria's regulatory response.
- [43]. *Computer Law & Security Review*, Volume 21, Issue 3, 2005, Pages 237-248, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2005.02.006>. (<https://www.sciencedirect.com/science/article/pii/S0267364905000701>)
- [44]. Pal, A., Herath, T., De', R., & Rao, H. R. (2021). Is the convenience worth the risk? An investigation of mobile payment usage. *Information systems frontiers*, 23, 941-961. <https://link.springer.com/article/10.1007/s10796-020-10070-z>
- [45]. Potts, M., (2012). The state of information security. *Network Security*, 2012, pp. 9-11.
- [46]. Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice [Electronic Resource]*, (420), [1]-6. <https://search.informit.org/doi/10.3316/ielapa.655572069982261>. Updated 2024 <https://doi.org/10.52922/ti268334>
- [47]. Seissa, I. G., Ibrahim, J., & Yahaya, N. (2017). Cyber terrorism definition patterns and mitigation strategies: A literature review. *International Journal of Science and Research (IJSR)*, 6(1), 180-186.
- [48]. Smith, R. G., Holmes, M. N., and Kauffman, P. (1999). Trends and issues in crime and criminal justice No. 121: Nigerian Advance Fee Fraud. *Australian Institute of Criminology*; Retrieved on 15.01.2005:<http://www.aic.gov.au/publications/tandi/ti121.pdf>
- [49]. Tendulkar, R. (2013). *Cyber-crime, securities markets and systemic risk*. CFA Digest, 43(4), 35- 43.UK: Oxford University Press.
- [50]. Udelue, M. C., Mathias, B. A., & Ezech, S. S. (2020). socioeconomic correlates of youths involvement in cybercrime: perceptions of residents in Onitsha south LGA, Anambra State, Nigeria. *International Journal of Social Sciences and Humanities Reviews*, 10(3), 66-79. <https://www.academia.edu/download/110084003/526.pdf>
- [51]. Unini, C. (2019). Cyber Defamation: Be Careful About What You Post Online. The Nigeria Lawyer. Available at: <https://thenigerialawyer.com/cyber-defamation-be-careful-about-what-you-post-online/>
- [52]. Vito, G.F. & Maahs, J.R. (2012). *Criminology: Theory, research and policy*. Sudbury: Jones and Bartlett Learning.
- [53]. Von Solms, R., and Van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, 38, pp. 97-102.
- [54]. Wall, D.S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press.
- [55]. Wolfe, D. & Hermanson, D.R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal*, 74 (12), 38 – 42.
- [56]. Xin, Q., Zhou, J., & Hu, F. (2018). The economic consequences of financial fraud: Evidence from the product market in China. *China Journal of Accounting Studies*, 6(1), 1–23.



<https://doi.org/10.1080/21697213.2018.1480005>

- [58]. Yakubu, M.A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(1), 315–321.  
doi:<https://doi.org/10.23956/ijarcsse/V6I12/01204>.