Afropolitan Journals

ISSN: 2780-5981X www.afropolitanjournals.com

The Effect of Online Fraud on the Adoption of Digital Economy in Nigeria: A Review

Bourdillon O. Omijeh

Nigerian Communications Commission, Professional Chair in University of Port-Harcourt.

Corresponding author: bourdillon.omijeh@uniport.edu.ng

Abstract

This research paper focuses on the different types of fraud and how it affects the acceptance of digital economy in Nigeria and the different techniques to help detect and mitigate these frauds. Digital technologies have the potential to open up new avenues for rapid economic growth, promote economic mobility, drive innovation, create jobs, and speed equal access to high-quality public services. This, combined with the convergence of multiple technologies and the emergence of global platforms, is upending existing socio-economic models, and new rules are needed to generate trust, protect data and Intellectual Property Rights (IPRs), and ensure security across the entire value chain in the increasingly digital and data-driven economy, however fraud has spread throughout the globe and is now a major cause for concern. irrespective sector, it exists everywhere and affects all different kinds of organizations.

Keywords: Digital economy, Data driven.

Introduction

Global digitization has been a defining feature of socio-economic growth in the twenty-first century. Although the digital economy has been a policy reference point since the turn of the millennium in relation to the emergence of e-commerce and e-government services, business to consumer (B2C), business to government (B2G), and business to business (B2B), it now encompasses the entire contemporary economy (Aguera *et al.*, 2020). Digitalization has both benefits and drawbacks. Technology is a double-edged sword that may be used both adversely and favorably. The same might be stated in cases involving financial crimes. While technology aids investigators and prosecutors in their fight against crime, it also provides crooks with a simple means of committing fraud.

Home to the youngest population in the world, Africa is progressing rapidly in digital adoption. Over the past ten years, the continent has recorded the highest growth globally in Internet access, moving from 2.1% in 2005 to 24.4% in 2018. The progress is not only visible in Internet connectivity but also in mobile-cellular telephone subscriptions and in households with a computer, and the trend is affecting the economy as a whole.

Cybercrime is on the rise around the world, and it is getting more sophisticated every year. Companies, consumers, and governments have lost billions of dollars globally as a result of a wide range of frauds, ransomware, phishing assaults, and viruses/infections. Personal and business information are particularly vulnerable.

Cybercrime wreaks havoc on the digital economy by stealing and distorting digital products, and it erodes customer trust in the online world. The adoption of the digital

economy is being hampered by security threats (actual or perceived) in payment channels and a lack of understanding about fraud detection.

Cybercrime, commonly known as online fraud, encompasses all offenses that online crimes are committed with the aid of computers or online technology. The terms "fraud" and "fraudulent activity" have numerous definitions. According to the Association of Certified Fraud Examiners (ACFE), "fraud" is the intentional misuse or misapplication of an employing organization's resources or assets for personal gain (ACFE, 2002).

(Maras, 2015; Maras, 2016) defines cybercrime as traditional, real-world (offline) crimes (e.g., fraud, forgery, organized crime, money-laundering, and theft) are 'hybrid' or 'cyber-enabled' crimes committed in cyberspace, as well as 'new' or 'cyber-dependent' crimes made feasible by the Internet and Internet-enabled digital technology.

Cybercrime is on the rise around the world, and it is getting more sophisticated every year. Companies, consumers, and governments have lost billions of dollars globally as a result of a wide range of frauds, ransomware, phishing assaults, and viruses/infections. Personal and business information are particularly vulnerable.

Warren *et al.* (2016) states that annually, cybercrime costs the world economy over $450 billion; this amount exceeds the market capitalization of Microsoft Inc. and Exxon Mobil Corp. and is rapidly catching up to Apple Inc. In other words, cybercrime would be the 23rd largest economy in the world, surpassing nations like Iran and Austria while (Graham,2017) confirmed same amount of $450 billion was lost in 2017.

Cybercrime is prevalent and impossible to eradicate fully. Governments, on the other hand, can mitigate its effects by building a resilient general economy and strong institutions, as well as investing in deterrent capacity. In this process, legislative frameworks play a crucial role.

Literature Review

The digital economy, according to (Bukht & Heeks, 2018), is comprised of "social and economic activities that demonstrate the following characteristics: are enabled by internet/mobile technology platforms and ubiquitous sensors, offer an information-rich environment, are built on global, instantaneous/real-time information flows, provide access 24 hours a day, anywhere, and support multiple, virtual, connected networks."

The "fraud triangle," which includes the pressure or motivation to commit fraud, the opportunity to commit fraud, and the justification offered by the perpetrators, is the traditional paradigm or classical framework for researching fraud (Lederman, 2021).

Trompeter *et al.* (2013) add three additional components to the triangle in their synthesis to embrace an extended view of (accountancy) fraud: the act of fraud, its concealment, and the ensuing "conversion" (the benefit to the fraudsters).

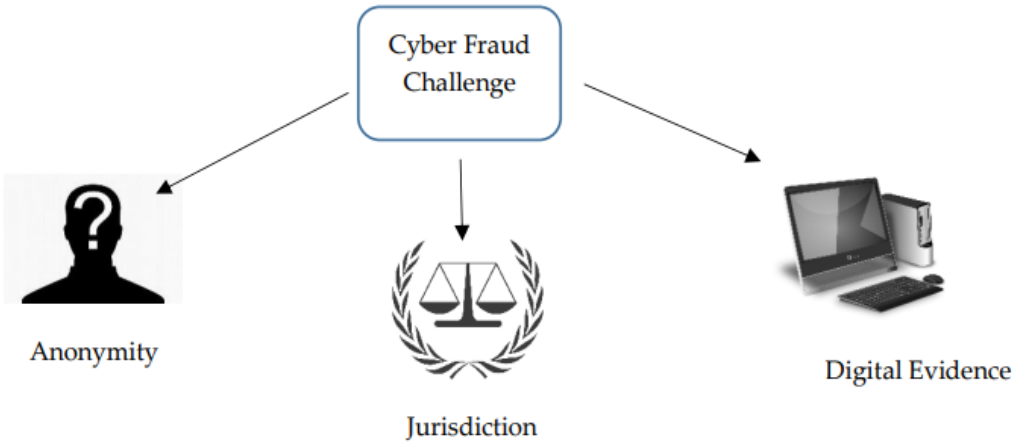

Fig 1: Fraud Triangle

As shown in Fig 1 above, there are three factors that contribute to the rise in cyber fraud cases. The first is the anonymity factor, which allows criminals to operate without detection until it is too late for the authorities to find out who is responsible for the fraud. The next explanation for the rise in cyber fraud offences is jurisdiction. This is due to the fact that cybercrimes would make it challenging for legal authorities to determine the location where the legal procedure will be handled. The absence of jurisdictional cooperation between nations, such as those in Southeast Asia, South America, and Africa, is one of the factors that makes law enforcement subject to limits and gives this character the additional name "borderless." (Hayes *et al.,* 2015). The final factor is how challenging it is for law enforcement to locate the evidence they need (Hidayati *et al.,* 2021).

Types of Frauds

1) Credit Card Fraud: The credit is termed as the process of purchasing and selling products without having cash on hand. A credit card is a little plastic card used to provide customers credit (Raj & Portia, 2011). Today, ATMs, swiping devices, store readers, banks, and internet transactions all read card information.

Each card has a special card number, which is very essential. The physical security of the card and the confidentiality of the credit card number are what determine how secure it is(Sandhya *et al.,* 2023).

Credit card frauds are easy and friendly targets. Financial fraud is an issue that has emerged as a threat with broad ramifications for the financial sector. The widespread use of credit cards has been facilitated by the development of technology. The rate of fraud has also increased as a consequence of this. Credit card fraud may result from the use of a card by an unauthorized user who presents a false name to a bank representative or it may result from the use of stolen credit cards.

In a just concluded research by (Dornadula & Geetha, 2019) to create and implement a novel fraud detection technique for streaming transaction data with the goal of analyzing past customer transaction information and identifying behavioral patterns, the team reported

that according to statistics provided by the FTC, there were 1,579 data breaches in 2017 that affected almost 179 million records, with credit card fraud being the most reported type (133,015 reports), followed by employment or tax-related fraud (82,051 reports), phone fraud (55,045 reports), and bank fraud (50,517 reports).

2) Electronic Fraud: Fraud is described as any illegal deception that is committed with the intention of making money.

The rising tendency of electronic fraud in important areas of the Nigerian economy is causing growing concern. The danger that results from the widespread adoption of new technologies like mobile money and computerized banking and payment systems has been estimated to cost the nation a staggering N197.9 billion a year

According to Vanguard news report, banks are targets both internally and internationally, hacking has turned into a serious threat, with billions of naira in losses. In recent times, the North Korean hacker Lazarus has attacked banks in Nigeria. The largest risk, according to the Central Bank of Nigeria (CBN), in the industry that has extensively adopted electronic payment solutions like Automated Teller Machines (ATMs), NIBBS Instant Payment (NIP), and mobile banking, is e-fraud (Ariana, 2016) .

3) Phishing: Experts, researchers, and cybersecurity organizations have put forth and discussed various definitions for the word "phishing." Despite the fact that the word "phishing" lacks a set definition due to its ongoing evolution, it has been interpreted in a variety of ways depending on its usage and context. (Alkhalil *et al.,* 2021) in their just concluded research defined Phishing as a fraudulent activity that includes the creation of a replica of an existing web website to trick a user into submitting personal, financial, or password data. Phishing is an attempt to trick a user into disclosing private information, like bank account and credit card numbers, by sending the user malicious links that take them to a phony website. Some claim that emails are the sole assault avenue. People are sharing more of their personal information online due to the substantial increase in internet usage. Cybercriminals can now access a vast amount of personal data and financial transactions as a consequence. Phishing is one instance of a very efficient type of cybercrime that allows offenders to trick users and take crucial data.

4) Smishing/Vishing: One of the most popular communication channels is the short message service (SMS). Because SMS messages are quick and easy to send and receive without an Internet link, some users prefer them to emails. Additionally, the cost of SMS services has been reduced by telecom companies, which has increased SMS usage and drawn assailants to SMS attacks. In order to make it difficult to track down the attacker, attackers can buy any mobile number with any area code and send spam messages from it (Jain & Gupta, 2019).

Smishing is a cyber-security threat that uses Short Message Service (SMS) to steal mobile users' personal credentials. Because users place a high degree of trust in their smart devices, attackers have been drawn to perform Smishing and other mobile security attacks.
This occurs when an e-fraud perpetrator sends text texts to victimize e-fraud victims. Frequently, the text message will include a phone number for the recipient to call. When the recipient does, the e-fraud perpetrator will have an opportunity to ask the victim for private information. Vishing also refers to when e-fraudsters contact their victims using a secret phone number in order to obtain sensitive information (Ololade *et al.,* 2020).

5) Telecommunication Fraud: Although the popularity of the Internet has increased work productivity, it has also opened up new spaces and possibilities for criminal activity. The recently emerging Internet and telecommunication fraud, which includes telephone, SMS, WeChat, QQ, and other telecommunications network platforms, uses the Internet or telecommunication as a medium to conduct fraud. Large populations can easily and rapidly become targets of this new non-contact crime type, which poses new risks to society and leaves victims with significant financial losses (Ni & Wang, 2022).

6) Spyware: Computers are now at risk from unidentified malware activities when they are linked to a network. Without the users' awareness, malicious software is downloaded and installed in the system. Malicious software has the intention of causing harm to the system, such as slowing down the network performance, raising the electricity bill, or obtaining private data, such as bank account numbers and login passwords, in order to be misused. It may also have the intention of having control over users through screen monitoring and key loggers that record the keys or content they type. All of this information is sent to the hacker using this program after being obtained or processed.(hpa & thiya, 2018).

7) Impersonation: Imitating someone with the intention of dishonestly perpetrating fraud is known as impersonation. Another common form of bank fraud is impersonation, which involves third parties obtaining new checkbooks through fraud and then using them to conduct other crimes.
When impersonation is carried out with the help of shrewd bank employees, who are able to easily procure the sample passport photos and signatures of the unsuspicious customers, it has been observed that such cases of impersonation are particularly successful (Akinyomi, 2012).

Types of Fraud/Cybercrime Prevention and Detection Techniques

1) Statistical Data Analysis Methods: By conducting in-depth investigations, statistical data analysis for fraud detection carries out a number of statistical processes, including fraud data collection, fraud detection, and fraud validation. The following categories have been added to these techniques: statistical parameter calculation, Probability distributions and models, Regression analysis and Data matching.

2) AI-Based Methods: Businesses have improved their internal security and streamlined business processes by implementing AI for fraud prevention and detection. AI has become a key technology for preventing fraud at financial institutions due to its increased efficiency. AI methods comprise the following ways:

- **Data Mining -** Data is classified, clustered, and segmented for fraud detection and prevention purposes, and associations and rules are automatically found in the data that may indicate intriguing patterns, including fraud-related trends. Data mining takes information and knowledge from large databases and extracts it for use (decision support systems and intelligent systems). Examples of data mining classification methods include the usage of neural networks and support vector machines. The K-means algorithm is used as a clustering approach in data mining. Additionally, a variety of techniques from other fields, including statistics, machine learning, pattern recognition, database and data warehouse systems, information retrieval, visualization, algorithms, high-performance computing, and numerous application domains, have been incorporated into data mining (Han *et al.,* 2022).
- **Neural Networks -** In the context of fraud detection, neural networks classify, cluster, generalize, and forecast fraud-related data that can be compared against findings from internal audits or official financial documents. Neural networks (NN) are a proven innovation with established hypotheses and anticipated application domains. In these organizations, several kinds of neurons are created. The weight, which is associated with each association, is a numerical value
- **Machine Learning -** Due to ML algorithms' capacity to recognize past fraud patterns in future transactions and learn from them, fraud detection is made possible.
- **Pattern Recognition -** Pattern recognition algorithms detect approximate classes, clusters, or patterns of suspicious behavior, either automatically (unsupervised) or manually (supervised).

For the objective of preventing and detecting fraud, other methods are also employed, including link analysis, Bayesian networks, decision theory, and sequence matching.

Comparison of the Different Kinds of Frauds

Farahbod *et al*. (2020) notes that the most common cybercrimes listed in the 2017 Norton Cyber Security Insights Report are hacking a device (53%), debit/credit card fraud (38%), compromised account passwords (34%), hacking email or social media accounts (34%), fraudulent online purchases (33%), and phishing scams (32%). The victims share certain attributes. They are usually early adopters of newer security techniques, such as security software, personal Virtual Private Network (VPN) technology and two-factor authentication, and are overconfident in their abilities to avoid becoming a cybercrime victim.

A total of twenty-seven thousand three hundred and fifty-six (27,356) incidents of fraud and forgery were reported for the second quarter of 2022 under review, compared to forty

thousand, five hundred and twenty-two (40,522) reported cases2 for the first quarter of 2022, representing a decrease of 32.49 percent between the periods. According to the report, Card fraud, computer/web fraud, and mobile fraud which encompasses fraud activities through USSD transactions were the three types of fraud that occurred most frequently(FITC, 2022)

In the second of 2022, the instruments most frequently used to commit frauds are cards and cash, making card fraud the highest fraud in Nigeria as of now.

Conclusion

The growth of the digital economy is hampered by fraudsters' escalating attempts, which severely damage consumers' wallets, trust, and sense of security as well as the nation-state. In contrast to more developed economies like the United States, where reported instances of fraud against customers cost consumers more than $5.8 billion in 2021, there is no national data on how much money Nigerians in the digital age lose each year to frauds due to a culture of disregarding cases.

This review, which is concerned with strategies for dealing with online frauds, will undoubtedly be fascinating to experts in the economic and financial fields who deal with similar issues on a daily basis. In addition, our work educates the general public about the dangers they face and the necessity of taking precautions against economic and financial crime.

Acknowledgement

I would like to acknowledge the Nigerian Communication Commission (NCC) for funding this work.

References

ACFE. (2002). *Report to the Nations on Occupational Fraud and Abuse*. https://www.acfe.com/-/media/files/acfe/pdfs/2002rttn.ashx

Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & Van Der Spuy, A. (2020). SADC Parliamentary Forum Discussion Paper: The Dgital Economy and Society. https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/

Akinyomi, J. . (2012). Examination of fraud in the Nigerian banking sector and its prevention. *Asian Journal of Management Research*, *3*(1), 217–229.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). *Phishing Attacks : A Recent Comprehensive Study and a New Anatomy*. *3*(March), 1–23. https://doi.org/10.3389/fcomp.2021.563060

Ariana, R. (2016). 済無 No Title No Title No Title. *RISING WAVE OF E-FRAUDS PUTS ECONOMY AT RISK*, 1–23.

Bukht, R., & Heeks, R. (2018). Defining, conceptualising and measuring the digital economy. *International Organisations Research Journal*, *13*(2), 143–172. https://doi.org/10.17323/1996-7845-2018-02-07

Dornadula, V. N., & Geetha, S. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. *Procedia Computer Science*, *165*, 631–641. https://doi.org/10.1016/j.procs.2020.01.057

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *32*(1), 63-71.

FITC. (2022). *Report on Frauds and Forgeries in Banks*.

Graham, L. (February). *Cybercrime costs the global economy $450 billion: Ceo,* https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

Han, J., Pei, J., & Tong, H. (2022). *Data mining: concepts and techniques*. Morgan kaufmann.

Hayes, B., Jeandesboz, J., Simon, S., Mitsilegas, V., & Scherrer, A. (2015). The law enforcement challenges of cybercrime: are we really playing catch-up?

hpa, P., & thiya, S. S. (2018). Review On Spyware - A Malware Detection Using Datamining. *International Journal of Computer Trends and Technology*, *60*(3), 157–160. https://doi.org/10.14445/22312803/ijctt-v60p124

Hidayati, A. N., Riadi, I., Ramadhani, E., & Al Amany, S. U. (2021). Development of conceptual framework for cyber fraud investigation. *7*(2), 125-135.

Jain, A. K., & Gupta, B. B. (2019). Feature based approach for detection of smishing messages in the mobile environment. *Journal of Information Technology Research*, *12*(2), 17–35. https://doi.org/10.4018/JITR.2019040102

Lederman, L. (2021). The fraud triangle and tax evasion. *Iowa Law Review*, *106*(3), 1153–1207. https://doi.org/10.2139/ssrn.3339558

Maras, M.-H. (2015). *Computer forensics*. Jones and Bartlett Learning.

Maras, M.-H. (2016). *Cybercriminology*. Oxford University Press.

Ni, P., & Wang, Q. (2022). Internet and Telecommunication Fraud Prevention Analysis based on Deep Learning. *Applied Artificial Intelligence*, *36*(1). https://doi.org/10.1080/08839514.2022.2137630

Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020). E-Fraud in Nigerian Banks: Why and How? *Journal of Financial Risk Management*, *09*(03), 211–228. https://doi.org/10.4236/jfrm.2020.93012

Raj, S. B. E., & Portia, A. A. (2011). Analysis on credit card fraud detection methods. 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET).

Sandhya, G., Abishek, M., Gunal Kumar, S., & Jisenthira Kumar, R. S. (2023). Credit Card Fraud Detection using Machine Learning Algorithms. *Lecture Notes in Networks and Systems*, *516*(07), 313–320. https://doi.org/10.1007/978-981-19-5221-0_30

Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Riley Jr, R. A. (2013). A synthesis of fraud-related research. *32*(Supplement 1), 287-321.

Warren, T., Favole, J., Haber, S., & Hamilton, E. (2016). Cybercrime costs more than you think.