POLAC MANAGEMENT REVIEW (PMR)
DEPARTMENT OF ECONOMICS AND MANAGEMENT SCIENCE
NIGERIA POLICE ACADEMY, KANO

FRAUD IN A DIGITAL ENVIRONMENT: CHALLENGES AND PROSPECTS OF DETECTION IN NIGERIA.

Sani Alfred Ilemona Department of Accounting. Federal University, Gombe State.

Isaac, M. Ikpor Department of Business Administration Alex Ekwueme Federal University, Ndufe-Alike, Abakaliki-Ebonyi State.

Abstract

The paper examined fraud in digital environment, the challenges and prospects of its detection in Nigeria. The aim was to explore ways the fraud is usually perpetuated and the forensic accounting techniques that can be deployed in detecting the fraud. Being an exploratory research relevant literature on the subject matter were used. Findings suggested that lack of knowledge regarding the nature of the fraud and funds to procure the equipment/tools are largely responsible for low deployment of the detective tools. The study concluded recommendation that in addition to creating awareness on the digital crime, individuals and organisations should be encouraged to employ the detective tools. Also, since it is a public security issue, government should establish and equip all her security outfits with tools that can effectively detect cybercrimes.

Keywords: Digital, Environment, Fraud, Forensic, Accounting.

JED Classification: B22, B26, D31, F65

Introduction

Fraud has always been in existence with human development all across the globe. It is one of the social and economic ill confronting economies around the world with consequences on both the perpetuators and the victims.

Though the consequence of the illicit act can be very huge to the perpetrators ranging from life imprisonment to death penalty, the 'evil' occupation of fraudster is thriving and many have taken it up as means of livelihood. With the way, the evil act is planned and the boldness of its execution by the perpetrators, one cannot but admit that fraud is an upcoming sector of the invisible yet forceful industry called crime (Adefila, 2006).

The most disturbing dimension of the illicit act (fraud) in recent time (21st Century) is the one taking place in a digital environment prone to so many risks of internet transactions. The rate of the crime escalated during coronavirus pandemic (Covid-19) the period of isolation when movement across and association were highly restricted (Barnewi& Douglas, 2020). The period paved for incidence of fraud scheme, committed mostly through email, websites, chatrooms with individuals and corporate entities that suffered huge financial losses (Wagner & Julian, 2010). For instances in Brazil, Canada, Columbia, Hong Kong, USA, and UK it was reported that financial loss suffered by individuals and corporate organisations in these countries was higher than losses suffered in the last 10years, prior to the year of the pandemic (Elien & Allein, 2020). In Nigeria, the case was not different as the estimated loss suffered by organisations attributable to cybercrime during the pandemic was put at N30bn (Dayo & Martin, 2020). The pandemic period gave fraudsters the opportunity to exponential use of internet to commit fraud in the cyberspace. The fraud can be swift because several relationships can be established through network including purchase, sales and transfer of funds within few minutes.

Generally, fraud risks will continue as long as companies, firms and individuals would continue to exist and as long as fraudsters continue to benefit from the proceeds of the crime. The disturbing aspect is the negative impact of the act on the victims and sophisticated dimension of the illicit act in the digital age (Bamio, 2020). Since frauds are becoming sophisticated, with devasting effects on economies, at international, national, macro and micro level, more advanced and modern techniques are needed to detect and fight schemes of fraudsters.

Statement of the Problem

For fraud detection in a digital environment, a lot of data must be analysed to detect the risks and fraud that might likely occur (Othman, 2018). Given the sophistication of the crimes and devastating effects on organisations especially those in advanced nations like USA, UK and China are now investing more in technology to detect and prevent fraud (Smith & Morien, 2017). Unfortunately, however, many organisations in developing nations especially Nigeria are not investing much in these frauds detecting and preventing technologies (Boyo & Dele, 2020).

The issue of inadequate technology is more for Micro, Small and Medium Scale Enterprises (MSMEs) due to lack of the knowledge of the technology funds to procure the analytic tools (Dagudu & Norman, 2019). The technology is expensive to buy and adopt across organisations in Nigeria is an uphill task (Dagudu & Norman, 2019).

Quite apart from issues of the tools and funds for procurement, the problem of intelligence gathering by security agencies also has contributed to the thriving of fraudulent activities in cyberspace in Nigeria as many of Nigerian security outfits don't have the needed equipment and training to investigate cybercrime cases (Festus &Surkin, 2018).

Objectives of the Study

The paper presents as its main objective, the nature of fraud in a digital environment/age, the techniques/tools for the detection and prevention of the fraud. This is with the view to enlightening the Nigerian Public (individuals and corporate entities) where necessities for detecting and checking the menace of the fraud are lacking.

Significance of the Study

Frauds and particularly those taking place in cyberspace (cybercrime/internet fraud) are largely responsible for impairment of capital formation and growth of economies mostly the developing ones like Nigeria (Omosurumi & Rumlia, 2018). In fact, the many dimensions of fraudulent activities occurring in digital environment are partly responsible for crumbling financial sector of Nigerian economy (Okoye & Hawe, 2019).

Therefore, an expository study on techniques for detection and prevention of the seemingly little foxes (fraud) destroying the fragile economy of Nigeria is considered significant.

Literature Review

Conceptual Review

Fraud: It is an illicit act and irregularity involving the use of criminal deception to obtain an unjust or illegal advantage (Morris, 2013). The illicit and irregularity are illegal and entails conversion or diversion of a person's or organization's money or material for selfish satisfaction of the perpetrator. It is an activity that amounts to unfair dealing with a person or organisation by the perpetrator for the purpose of depriving them of their belongings (Adefila, 2006). The English Advanced Learners' Dictionary defined fraud as deceitfulness, criminal deception and using false representation to obtain unjust advantage. It is an unlawful and intentional making of misrepresentation which causes actual or capable of causing prejudice to another. Fraud is an act characterized by deceit, concealment of truth and violation of trust of the victim (Zebbis, 2011).

Campbell Black Law Dictionary cited in Adefila (2006) defined fraud in generic term to embrace all multifarious means which human ingenuity can device and which are resorted to by one individual to over-ride

the other by false suggestions or by suppression of truth and any unfair way by which the other is cheated.

Gleaning from the definitions of fraud, Adefila (2006) coined the intents of fraudsters as follows:

1. Intent to permanently deprive the owner of a thing of it.
2. Intent to use the thing as a pledge or security.
3. Intent to part with it on a condition as to its return which the person taking or converting it may be unable performs.
4. Intent to deal with it in such a manner that it cannot be returned in the condition in which it was at the time of the taking or conversion.

From all the narrations, fraud can simply be described as any crime for game that uses deception as its principal modus operandi by the perpetrator(s) to deprive an individual, group of individuals, organisations and society as a whole their rightful belongings.

Digital environment: It is an integrated communication environment where digital devices communicate and manage the content and activities within it (Kenedy & Bolly, 2009). The integrated systems are implemented for global community. The components of a digital environment generally include websites, cloud servers, search engines, social media outlets, mobile apps, audio and video and other web-based resource (Lyon & Danny, 2007).

A digital environment in a business setting includes all resources that are either computer, mobile devices or electronically based resource in the organisation in an integrated system (Talmot& Wagner, 2010). Therefore, it suffice to say that if an organisation conduct its business activities through the internet or any other electronic-based communication system including websites, e-mail, search engine optimization strategy, social media and Voice Over IP Phone Service (VOIP), the organisation is said to be conducting its business transactions in a digital environment.

As businesses and individuals conduct their activities within their digital environment, they interact with people globally (Polyner & Morr, 2008). As the interaction get stronger and faster, usage of gadgets such as computers, servers, mobile devices, personal digital based devices, accounting software, web-based application become a necessity (Reela & Akler, 2005).

Types of Fraud in a Digital Environment

The most common type of fraud scheme of fraudsters in a digital environment according to Madlan (2018) are as follows:

i. **Spam:** It is a generic term used to describe electronic junk mail or unwanted messages sent by fraudsters to email account or mobile phone of the intended victim (Madlan, 2018). The messages are usually commercial in nature persuading people to buy a product or service or visit a fraudulent website for purchases. They (fraudsters) through the fraudulent messages trick their victims into divulging their bank account or credit card details for their fraudulent activities (Brown & Matthew, 2016). In 2020, during the pandemic about N200m was reported to have been lost by individuals and corporate organisation in Nigeria attributable to spam scheme (Nayo& Charles, 2021).

ii. Spyware: It is software that is installed on a computer and takes things from it without permission or knowledge of the user (Schwart& Winn, 2011). Spyware may take personal information, business information or processing capacity of an organisation and give it to someone else for competitive edge of the organisation sponsoring the fraudulent activity.

iii. **Phishing:** It is a fraud scheme/technique used to gain personal information for the purpose of identity theft (Sparkler, 2010). The scheme involves using a form of spam to fraudulent gain access to people's identity and online banking details.

The term phishing is a semantic game means that the cybercriminal will "fish" their victim on the internet (Sparkler, 2010). The Ph comes from "Phreaking" or phreaks which refers to enthusiasts who experimented with telecommunication networks to find out how they work (Rotney & Veny, 2012).

Phishing attack has three components; (i) the attack is carried through electronic communication such as email or over the phone (ii) the scammer pretends to be a trusted individual or organisation and (iii) that the scammer intended to obtain sensitive personal information such as login credentials or credit card numbers.

There are three types of phishing, namely:

- **Smiley:** These are messages that prompt the victim to make immediate decisions. For instance, a message could be sent to a victim that he or she has won an unexpected lottery of a large sum of money or selected for a specific benefit programmes. Many have fall victims of this Smiley Scam in Nigeria either as a result of poverty or out of desire to get rich quick (Eddy &Leornad, 2018).
- **Scam:** Phishing scams are meant to get information from potential victims via contaminated links or files (Ornell & Kale, 2016). Contact can be via phone, email, text messages or social media communications.
- **Phishing clone and spear phishing:** Clone phishing involves cloning another website to attract users and induce them to behave as if they were in a safe and known environment. Spear phishing on the other hand, occurs when the scammer targets a specific person or group of persons/victims with the aim of accessing a particular database to obtain confidential files for sensitive information which in most cases are financial in nature.
- **Whaling**: The aim of whaling is to target specific high-profile individuals of repute in the society. The scheme is intended to gain access to confidential data on finances of the victims (Witneys & Neolen, 2012).
- **Vishing**: The technique uses voice mechanism to apply scams on the internet. Voice calls and messages transmitted are meant to fraudulently address urgent issues requiring the victim to take urgent action to provide money. "Urgency" of the matter is usually the emphasis in the message (Witney&Neoten, 2012).

  Pharming:Through pharming**,** traffic from a legitimate website can be manipulated to direct users to fake websites that install malicious software. The malicious software is capable of collecting personal data on victim's computer that can be used for various fraudulent purposes.
- **Internet Banking Fraud:** Internet banking fraud is common only especially in black nations where technology for cyber fraud detection is low (Barvman, 2015). The scheme is a type of fraud committed using online technology to illegally remove money from a bank account and/or transfer the money to an account in a different bank. Among all the forms of fraud taking place in a digital environment, internet banking is the most common in Nigeria with phishing as the most common technique used for the fraudulent activity (Olowati&Tigma, 2018).

Forensic Accounting Tools for Fraud Detection in a Digital Environment

In recent time, some forensic accountant in developed nations in UK, USA, Canada, France, China, and Japan have engaged in development and procurement of electronic data to reconstruct and detect financial fraud taking place in digital environment. The forensic analytical tool mostly used by these specialist (forensic accountants) according to Betty (2018) are as follow;

1. **Encase:** is a court proven solution for finding, decrypting, collecting and preserving forensic data from a wide variety of devices (Betty, 2018). It is a traditionally used in forensic detection to recover evidence from sized hard drives. Encase allows the investigator to conduct in depth analysis of user files to service evidence such as documents, pictures, internet history and windows registry information. It is a shared technology within a suite of digital investigation. The software is widely used in cyber security, security analytics and e-discovery use (Shruri & Esslyn, 2016).
2. **Forensic Tool Kit (FTK):** The tool allows the investigator to view the content of images, conduct searches and potentially retrieve hidden and deleted data (Huwan, 2014). FTK is helpful in fraud detection and communication as communication between culprits via instant messaging or chat on websites can easily be tracked (Huwan, 2014).
3. **Sleuth (autopsy) forensic software:** Used to investigate what happened on a computer. The

software allows the investigator to efficiently analyse hard drives and smart phones to discover communication or transactions that have occurred (Daron &Iflan, 2013). Investigator working with multiple machines enabled by the software can build a central flag phone numbers, email addresses, files and other data that might be found in multiple places.

4. **Computer Aided Investigative Environment (CAINE):** It is an operation environment designed to provide all the forensic investigative processes for presentations, collection, examination and analysis of transaction to confirm their genuine-ness. The tool (CAINE Linux) support disk imaging in raw data and expert witness in advanced file format (Corln & Booklyn, 2015).

5. **Network Analysis (NA):** It isa set of integrated techniques that depicts relations among actors for analysis of the social structures that emerge from the reoccurrence of the relations (Evenshen, 2016). Two techniques for NA developed in 1980 according to Eveshen (2016) were PERT (Programme Evaluation and Review Technique) and CPM (Critical Path Management). The interactive representation of data analysis the techniques are used to generate useful insight and provide an overview of all data connections. The connections are useful for analysing control, and monitoring business processes and work flows necessary for detecting unusual processes and transactions (Chikson & Edler, 2010).

6. **Memory Forensic Volatility:** It is the analysis of volatile data in a computer's memory dump (Kedley & Rodglin, 2013). Forensic accountants conduct memory forensics to investigate and identify attacks or malicious behaviour that do not leave easily and are capable of facilitating malicious/fraudulent entries into a system.

7. **Mobile Forensic Cellebrite:** The software is able to automate physically, extracting and indexing data from mobile devices (Onrinn, 2014).

The software was developed in 2007 and useful in providing digital forensic and intelligence tools for use by forensic accountants in fraud detection and investigation (Chavrya, 2014).

The Role of Government in Cyber Fraud Detection

Government at all levels have the duty to protect the society by preserving, peace, develop and run programmes in crime prevention, aid in emergencies and manage emergency incidence (Tolley & Franklin, 2015). In modern society, law enforcement agencies especially police perform essentially role in achieving cyber security by investigating a wide range of cybercrimes and apprehending those responsible for security infractions. These cyber security functions are premised on the availability of necessary tools and requisite training which unfortunately are inadequate in Nigeria (Ivy & Murphy, 2016). The equipment and training are necessary for proper investigation and prosecution of cases especially those involving cyber financial crimes (Ivy & Murphy, 2016).

Theoretical Framework

The study is anchored on fraud triangle theory. The theory was propounded by American criminologist, Donald Cressey in year 1978 (Nayo& Charles, 2021). The theory explains the factors that lead individual or group of individuals to commit fraud and other unethical behaviour. These factors broadly categorized into three(3) are (i) pressure from financial force pushing towards fraud (ii) rationalization as personal justification of dishonest actions and (iii) opportunity which means ability to execute fraudulent plan without being caught.

This theory assumes that when businesses, individuals and organisations understand the fraud triangle, they can effectively combat criminal behaviour that negatively impact their operations (Nayo& Charles, 2018). The assumption underscores the relevance of the theory to the study.

Methodology

The study being a theoretical exposition of nature and fraud schemes in a digital environment, made use of relevant literature on the subject matter.

Findings and Discussion

Forensic analytical tools have been developed and deployed by individuals and corporate organisations in many advanced nations to tackle the issue of fraud in digital environment (Betty, 2018). Unfortunately, in Nigeria, individuals and enterprises are not much aware of these tools (Dagudu& Norman, 2019). Lack of awareness and other factors such as high cost of procuring the need tools/technology and inability of individuals and businesses especially the SMEs to lure the services of experts (forensic accountants) who have what it takes (knowledge) to detect the high wire fraud occurring almost every day in Nigeria. The problem of detection of this high wire fraud (fraud in a digital environment) is further compounding in the country due to ill-equipped government agencies who may not be unable to effectively investigate cyber scams taking place in Nigerian society (Festus & Surkin, 2018; Dagudu & Norman, 2019).

Indeed, fraud in a digital environment is a global socio-economic problem more pronounced in developing of Nigeria where a myriad factors are militating against the procurement and development of the needed technology to nip the occurrence of the menace at the bud (Festus & Surkin, 2018; Dagudu & Norman, 2019 & Boyo & Dele, 2020).

Conclusion and Recommendations

The processes of detecting and preventing digital fraud (internet fraud) are quite costly and time consuming. But then, it is necessary to fight the schemes of the fraudsters for growth and development of the society. It is with this growth objective that individuals and corporate organisations all across the globe are investing heavily in modern technology to detect and curtail the menace of the rising trend of fraud happening in digital environment.

Though, the burden of investment and development of technology for fraud detection usually fall more on individuals and corporate organisations, government has a lot to do especially in developing nations like Nigeria. Government has a duty to maintain public order and manage public security including curtailing fraudulent transactions occurring in cyberspace. It is in view of this collective responsibility of internet fraud detection in Nigerian society that the study recommended the following:

1. Creation awareness in the general public, the nature of modern fraudulent activities of fraudster that can take place in a digital environment.
2. Government through advocacy emphasize on need for individuals and corporate organisation to must in modern technology for cybercrime detection.
3. Government should assist business enterprises especially the SMEs with funds to procure technology for internet fraud detection. Utilization of the fund should be monitored by appropriate body of Government. Find utilization should include hiring of the service of forensic accountants when necessary.
4. Law enforcement agencies in Nigeria should be well-trained and equipped with modern gadgets for investigating cybercrimes and special unit created for that.

References

Adefila, J. J. (2006). Fraud: Its nature, detection, prevention and control. *Journal of Arid-Zone Economy* 2(1), 49-63.

Barmo, A. L. (2020). Internet fraud in the pandemic era. *Journal of Management Research* 4(2), 102-116.

Barvman, P. C. (2015). An examination of strategies for curbing fraud in the society. Journal of Business Strategy and Finance 4(1), 105-120.

Batnewi, T. U. & Douglas, M. R. (2020). The challenges of curbing white crime in the society. *Journal of Scientific Management Studies.* 1(2), 42-52.

Betty, L.O. (2018). Fraud control: The waste and Abuse in organisations. *Journal of Administration and Economics* 1(3), 23-35.

Boyo, O. U. & Dele, M. B. (2020). Imperatives of technology acquisition for fraud detection in the computer age. *Journal of Modern Research in Social Science*. 2(4), 93-105.

Brown, W.S. & Matthew, O. (2016). Impact of fraud on organizational performance. *Journal of Accounting and Management Studies.* 4(2), 141-153.

Charrya, O. (2014). An analysis effects of fraud on Micro and macro-economic growth of a nation. *Journal of Finance Economics and Entrepreneurship Studies* 2(3), 13-28.

Chikson, B. &Edker, K. (2010). Effect of fraud on sustainable development. *Journal of Auditing, Management and Social sciences* 2(1), 88-97.

Corln E. &Booklyn, P. (2015). The role forensic accountants in fraud detection. *Journal of Finance and Business Management*. 4(3), 138-152.

Dagudu, N. & Normal, P. (2019). The role of government in internet fraud detection in Nigerian society. *Journal of Business Research and Political Studies*, 4(1), 121-133.

Daron, I. C. &Iflan, A. U. (2013). An analysis of the destructive role of fraud in society. *Journal of Accounting Policy and Economics*, 3(1), 48-61.

Dayo, G. A. & Martin, C. (2020). Effects of digital fraud on Nigerian economy. *Journal of Social Sciences and Financial Studies* 2(3), 38-42.

Eddy, K. S. &Leornad, N. (2018). Matching the events digital time, with digital fraud: An analysis of the evils of times. *Journal of Political Psychology and Economy* 1(3), 98-110.

Elien, T.S. &Allein, O. O. (2020). The dimensions of internet fraud. *Journal of Finance, Management and Business.* 3(1), 29-41.

English Advance Learners Dictionary. 7th Edition.

Eveshen, V.O. (2016). Internet Fraud: Control and Preventive measure. *Journal of Public Policy and Accounting.* 2(4), 107-121.

Festus, U. O. &Surkin, S. (2018). Emerging problems of the digital age. *Journal of Accounting and Entrepreneurial Research*, 3(1), 47-59.

Hywan, A. (2014). *Reading and cases in auditing and assurance service*. Lagos: PLT Publishers.

Ivy, W.N. & Murphy, K.L. (2016). An analysis of fraud motivating factors and effects of the act on economic growth. *Journals of Finance and Entrepreneurship* 4(2), 47-59.

Kedley, A. &Rodglin, T. (2013). Fraud Control: Management responsibility for fair reporting on corporate performance. *Journal of Management and Financial Reporting,* 5(2), 143-156.

Kenedy, T. C. &Bolly, B. F. (2009). Activating models for fraud investigating tools in the digital world. *Journal of Research in Accounting and Economics*, 7(2), 39-52.

Lyon, M. & Danny, T. (2007). The multiplier effect financial fraud on an economy. *Journal of Entrepreneurial Studies and Management* 2(1), 14-26.

Morris, I. Z. (2013). X-raying the effects of fraud on public and private institutions. Yola, a sensitization seminar for CEO of enterprises.

Nayo, P. & Charles, M. (2021). Causes of rising trend of cybercrime in the pandemic era. *Journal of Management and Business Studies*, 1(2), 24-36.

Okoye, O. &Hawe, G. H. (2019). Tackling the rising trend of internet fraud in Nigerian society. *Journal of Accounting and Management Studies.* 1(3), 19-31.

Olowati, A. O. &Tigma, R. (2018). Fraud detective and prevention: Whose responsibility? *Journal of Finance and Strategic Management.* 1(2), 12-25.

Omosurumi, N. &Rumlia, A. (2018). Effects of modernization on societal behaviour. *Journal of Psychology and Behavioural Studies.* 5(3), 81-94.

Onrinn, H. (2014). Internet Fraud: An examination of the techniques and tools for control and prevention. *Journalof Entrepreneurship Studies and Management.* 3(1), 28-42.

Ornell, I & Kate, F. T. (2016). Fraud detection and prevention in public and private organisations. *Journal of Corporate Governance and Ethics* 4(3), 39-54.

Othman, D. I. (2018). Hindrances to internet fraud assessment. *Journal of Entrepreneurship Research and Economy* 5(2), 59-71.

Polymer, O.A. &Morr, S. (2008). Phishing: A framework for understanding digital fraud. *Journal of Research in Economics and Business Finance* 2(2), 69-82.

Reela, B. &Akler, E. (2005). The social psychology of fraud. *Journal of Business and psychology* 3(3), 43-54.

Rotney, F. &Veny, G. C. (2012). Fraud prevention and control in organisations: The role of management vs employees. *Journal of Behavioural Sciences and Humanities,* 2(3), 134-147.

Schwart, V.T. & Winn, A. (2011). Towards effective forensic investigation: An examination of techniques. *Journal of Business and Economy* 2(3), 133-146.

Shruri, W. &Esslyn, O. M. (2016). Fraud detection and deterrence measures. *Journal of Accounting and Public Policy,* 2(2), 62-74.

Smith, T. &Morien, A. (2017). Issues with fraud detection in the digital age. *Journalof Contemporary Research in Business and Economy. 2(3), 131-144.*

Sparkler, D. (2010). Is cybercrime tedious to investigate? An analysis of the dimensions of the emerging fraud schemes. *Journal of Accounting and Entrepreneurship Research,* 2(4), 52-66.

Talmot, O. & Wagner, V. (2010). An examination of the nexus between social problems and fraud in the digital age. *Journal of Psychology, Economics and Entrepreneurial Research* 2(3), 106-122.

Tolley, U.K. & Franklin, G. (2015). The changing effect of frauds on economies. *Journal of Finance, Accounting and Management* 2(1), 90-103.

Wadlan, N.B. (2018). Fraud prevention and related benefit to business. *Journal of Contemporary Management and Social Sciences*, 3(1), 9-24.

Witney, W. &Neolen, O. (2012). The role of code of ethics in fraud prevention in organisations. *Journal of Behavioural Sciences and Humanities*, 2(3), 95-108.

Zebbis, R. N. (2011). Micro and macro effects of fraudulent practices on an economy: A global perspective, Dekina-Nigeria: A Workshop paper held for government entities.