e-ISSN 2795-3248
p-ISSN 2795-3222

www.gphjournal.org
SOCIAL SCIENCE AND HUMANITIES RESEARCH
Open Access
Global Publication House
International Journal

10.5281/zenodo.8195409 Vol. 06 Issue 07 July - 2023 Manuscript ID: #0955

THE ROLE OF FORENSIC ACCOUNTING IN MITIGATING AGAINST CYBER CRIMES DURING THE COVID-19 PANDEMIC ERA: ISSUES AND PERSPECTIVES

Dr Sunday Asukwo Okpo
Depart of Accounting, Faculty of Management Sciences Akwa Ibom State University, Obio Akpa Campus.
sundayokpo@aksu.edu.ng; saokpo@gmail.com. +234-0803-7864-947; 07017755777.
Dr Uwakmfonabasi Simeon
Depart of Accounting Faculty of Management Sciences, Akwa Ibom State University, Obio Akpa Campus.
uwakmfonsimeon@aksu.edu.ng 08035142357

Corresponding Author: sundayokpo@aksu.edu.ng

ABSTRACT

The advent of covid-19 pandemic not only create health challenges but also created difficulties in the conduct of economic activities across the world. Due to restrictions imposed as a result of the pandemic, the physical movements of individuals were restricted. Hence business transactions were conducted online through Internet services. Logistics services were adopted to move goods from the location where they were produced to where they were consumed. Payments or settlements for the products were conducted through the internet and this led to the astronomical increase in Internet fraud which culminated in the loss of valuable assets. This study was therefore conducted to examine how forensic accounting tools were adopted to investigate, track, and recover the lost assets and restore the victims to their original state prior to the loss, as well, as how the perpetrators were made to face appropriate sanctions. The study used a descriptive research design as the data for the study were obtained from secondary sources. The data were obtained through questionnaires that were administered to the personnel of agencies responsible for the management and control of cybercrimes in Nigeria and were analysed using percentages and correlation. The results of the analysis show that there was a significant effect of forensic accounting mechanisms in the management and control of cybercrimes. It also indicated that the application of forensic accounting tools was effective in obtaining admissible evidence in court. Furthermore, the result also showed a strong effect on the recovery of stolen assets. The study concluded that increased deployment of forensic accounting tools had an effect in reducing internet fraud, and provided enough evidence for prosecution of criminals and the recovery of stolen assets. The study recommends strict monitoring of Internet transactions as well as the adoption of forensic accounting tools as critical tools for tracking and recovery of stolen assets. The study apart from contributing to expanding knowledge on forensic accounting also addresses the fears of those who intend to carry on transactions through the Internet. Also, the recommendations will provide the roadmap towards addressing the problems of internet fraud.

KEYWORDS

Forensic accounting, cybercrime management and control, internet fraud, Covid-19.

Introduction

The advent of corona virus otherwise called covid-19 across the globe did not only create challenges in the health sector alone but also posed serious challenges across various sectors of the economyincluding particularly the business sector. The major effect of the crisis was the restriction in movement of human beings across the globe. Thus within the peak of the crisis activities were grounded and there was no movements of people as the virus was known to be transmitted as people move from one place to the other. However, transactions across the globe still went on and this created two very important economic crises. First was that goods and services have tobe transported from where they are produced to where they are consumed; and secondly, settlements have to be conducted through internet. The increased online transactions have opened up the cyberspace for more online crimes. Consequently, as noted bySuchi and Wika (2021) the convergence of transformation in information and communication technology (ICT) with increased access and dependence on internet for education, business, commerce and governance on a global scale, has opened up new opportunities for cyber-criminal and terrorist groups to carry out their nefarious activities without being detected or identified, let alone prosecuted.

The impetus for increased cybercrime is the fact that it is committed online with the perpetrators hidden or remotely located where they believed they cannot be identified or caught. As noted by Zegarra (2020) ‘online financial transactions give prospective lawbreakers a false sense of security because they believe that they easily conceal their tracks, nonetheless, sophisticated individuals can use the internet to obfuscate illegal transactions, and this is when the expertise of forensic accountants becomes inevitable’. The criminals are developing different strategies of perpetrating their nefarious activities. Thus the regulators and experts are expected to constantly develop techniques of fighting the crimes.

The concept of internet fraud otherwise known as cybercrime is not new and it is not restricted to covid-19 era only. It has always been in existence prior to now. As long as there are transactions through internet there will always be internet fraud. However, the advent of covid-19 made online transactions imperative across the globe and consequently, the perpetrators of online fraud now have opportunity of increasing their act of defrauding unsuspecting victims. Thus the roles of forensic accountants and fraud investigatorscome to bear. These roles come in three ways: first preventive, management and investigative. The preventive role arises when the activities of forensic accountants provide incentive to users of internet to understand how these frauds are committed and therefore provide the direction on how not to be a victim. The second role is how users of internet will continue to sustain operations without necessarily falling prey to the fraudsters. The third role is how to investigate and if necessary recover the stolen asset.

Internet fraud also refers to as cybercrime or ‘yahoo yahoo’ in Nigeria increased during the period of covid-19. The advent of covid-19 created an opportunity for cyber criminals to increase their trade. As documented by Kemp, Buil-Gil, Moneva, Miro-Linares and Castano (2021) cybercrime and total fraud increased beyond predicted levels and that changes in routine activities due to covid-19 have influenced cybercrime and fraud opportunities. Also Ma and Mckinnon (2020) asserted that as many services move online due to the covid-19 pandemic, cyber fraud also increased. In the same vein Stock (2020) documented thatcybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation caused by covid-19’. Ma and Mckinnon (2020) documented that cybercriminals target victim’s psychological vulnerabilities, taking advantage of covid-19 related anxiety by manipulating emotional instabilities to

enable cyber fraud. The major target of internet criminals is to deprive unsuspecting victims of their valuables thereby causing unnecessary pains which in some cases may lead to collapse of firms and untimely dead of individuals.

According to Federal Bureau of Investigation (FBI) internet fraud can be defined as the use of internet access to defraud victims or otherwise take advantage of them. During the covid-19 era, a lot of internet frauds have been committed and so much assets have been lost to fraudsters. Hence the application of forensic accounting and fraud examination skills in order to tackle the activities of the fraudsters cannot be overstated. Okpala (2019) identifies the importance of forensic accounting to include its ability to control and minimise financial fraud and other irregularities and at the long run may eradicate fraudulent schemes. This study therefore becomes imperativeconsidering the perceived benefits of deploying forensic accounting expertise at this critical times. The main objective of this study evaluates the impetus for forensic accounting in the covid-19 pandemic era and how the expertise can be used to ameliorate the effect of cybercrimes during the covid-19 pandemic era. Also Nabiebu and Akpanke (2021) described cybercrime as activities which are criminals in nature and effected through computer or internet.

Review of Related Literature

Concept of Forensic Accounting

The concept of forensic accounting is an evolving dimension of accounting which focuses on the extension of auditing beyond the presentation of true and fair view on the financial statements. It rather focuses on an in-depth investigation in order to obtain evidence that may be presented in a law court. Forensic accounting therefore is concerned with resolving criminal activities involving specific areas which require in-depth collection, analysis and evaluation of evidence relating to financial criminal activities. It draws from the knowledge of accounting, finance, law, auditing and analytical skills. Erasmus and Ibezim (2021) describes forensic accounting to involve the application of special skills in accounting, auditing, finance, quantitative methods, specific areas of laws and research, and investigative skills to collect, analyse and evaluate evidential matter, as well as the interpretation and communication of findings, and may involve either an attest or consulting engagement. Okpala (2019) identifies forensic accounting as a sub field of accounting profession that employs accounting practice, auditing and investigative skills to uncover fraud, embezzlement and other financial irregularities. This provides analytical evidence suitable for use in court during legal proceedings. KPMG (1999) as cited in by Imoniania, Antunes and Formigoni (2013) refers to forensic accounting as an assistance in disputes which are likely to involve litigation, arbitration, expert determination, mediation or an enquiry by an appropriate, and investigation of suspected frauds, irregularities or impropriety which could potentially lead to civil, criminal or disciplinary proceedings while focussing primarily on accounting issues.

Also Musa (2021) defines forensic accounting as a scientific accounting method of uncovering, analysing, resolving, and preventing fraud and white-collar crime matters in a manner that produces admissible evidence which is capable of proving or disproving facts in issue suitable in the court of law. In the same vein, Crumbley, Heitger and Smith (2015) define forensic accounting as the action of identifying, recording, settling, extracting, sorting, reporting and verifying post financial data or other accounting activities for settling current or prospective legal disputes or using such past financial data for projecting future financial matters or settle legal issues. Hopwood, Young and Leiner (2013) define forensic accounting as the application of investigative and analytical skills for the purpose of resolving financial issues in a manner that meets standards required by courts of law.

Ayas (2021) documents that forensic accounting is a discipline that refers to the stages of detection and investigation of crimes by judicial authorities in fraud evasion crimes, mostly on the basis of business. In the same vein Modugu and Anyaduba (2013) see forensic accounting as an integral part of the accounting profession which as the sole aim of unearthing fraudulent activities within and outside an organisation so far as the third party's action is in any way reflective on the activities of the organisation. Modumere and Onumah (2013) define forensic accounting as the practice of vigorous data collection and analysis in the area of litigation support consulting, expert witnessing and fraud examination.

Arising from the various definitions, it is evident that forensic accounting is concerned with the process of fact-finding in order to obtain admissible evidence in court with the main aim of recovering any lost asset or restoring the victims to their previous state. To achieve their objectives, forensic accountants apply special skills in accounting, auditing, quantitative methods, certain areas of law, research and investigative skills to collect, analyse, and evaluate evidential matter and to interpret and communicate findings. As pointed out by Rezaee and Wang (2019) as cited in Pearson (2008) the role of forensic accounting may include cybercrime risk assessment, cybercrime prevention, data preservation and analysis, information communication technology (ICT) policy compliance review, and using ICT to visualize, communicate and report results in the legal environment.

The importance of forensic accounting therefore cannot be over-emphasised. Apart from restoring the victims back to their original state, it helps in restoring the confidence of investors and consequently, promote economic activities across jurisdictions. According to Honisberg (2020) as cited by Pearson (2008) forensic accountants play a significant role in the process of detecting, preventing and prosecuting those individuals who are involved in criminal activities such as financial misstatements, money laundering and identity theft. Moreover, Ayas (2021) stated that forensic accountants examine whether private information and financial accounts are held with the legislation of the relevant country; and that forensic accounting is used in the determination of company value and transactions of insurance companies.

The scope of forensic accounting covers almost all human endeavours which involves financial transactions. In corroboration of the above, Zysman (2009) as cited in Imonania, Antunes and Formigoni (2013) document that the scope of forensic accounting covers a wide range of areas as:

- Criminal investigation carried out on behalf of the police with the aim of presenting evidence in a professional and accurate manner.
- Shareholders and partnership dispute which involves analysis of numerous year financial records for valuation and quantification of issues in dispute.
- Personal injury claim such as quantification of economic losses from motor accident or wrongful dismissal from employment.
- Business interruption and other types of insurance claim which involves detailed review of policy to investigate coverage issues and appropriate method of calculating losses.
- Business/employee fraud which involves fraud tracing, asset identification and recovery, forensic intelligence gathering and due diligence review.
- Matrimonial dispute involving the tracing, locating and evaluation of assets.
- Business economic losses which involves issues of disputed contract, construction claims, expropriation, product liability claims and trade mark.
- Professional negligence conducted in order to ascertain the breach and quantifies the loss involved, and mediation and arbitration, as a form of alternative dispute resolution.

Forensic Accounting and Auditing Compared

Naturally one would think that forensic accounting and auditing are the same. Though there is a thin line separating the two, there are still identifiable differences between the two. As observed by Smith and Crumbly (2009), auditing is a macro system, while forensic accounting is a microsystem. Forensic accounting draws heavily from the knowledge of auditing. Auditors are professionals who are appointed as an independent entity with the responsibility of analysing financial statement prepared by management in order to give an opinion on the financial statement. To achieve this, the auditor must examine the records and documents made available by management and then based on what they observe in the records and documents; they averred their opinion on whether the financial statement shows a true and fair view of the financial transactions of the organisation.

On the other hand, forensic accounting entailed thorough investigation in order to obtain evidence of fraud which will be tendered as a proof in the court. Thus forensic accountant must provide evidence to support litigation in court of law where cases of misstatement or fraud are involved. To achieve the aforesaid objective the forensic accountants must have inquisitive and analytical skills, must draw from the knowledge of law and must also be able to carry out research in details. Comparatively therefore the work of forensic accountant is more detailed and exhaustive than the work of auditors. This is because the auditors' work is mere attestation in which only an opinion is expressed. On the other hand the work of forensic accountant is definitive and precise in which case the forensic accountants must appear in court to substantiate his evidence.

Imoniana, Anyunes and Formigoni (2013) itemises the differences between forensic accounting and auditing in the following ways.

Items for analysis	Forensic accounting	Auditing
Why, when and where the services take place	Serves as a backing to prove fraud in the business in an apparent risk environment.	Continuous to certify the state of the art of business and comply with efficient market.
Scope of the job	Present analytical accounting and financial information to support legal and administrative decisions.	Opine on the accounting statements of business entities considering all criteria used in its preparations
Details of performed	Detailed planning aimed at documenting deterministic analysis.	Sampled and/or probabilistic procedures to serve as a base of concluding the financial statements
Periodicity	When necessary as particularly determined in the court.	Covering fiscal year to substantiate activities of financial period.
Reporting	Investigative or expert reports	Financial statements, management letters or auditors' report

Tools of Forensic Accounting

Various tools or techniques are adopted by forensic accountants in carrying out investigations of cybercrimes. The main objective of deploying the tools is to obtain sufficient evidence which is required to prosecute the perpetrators of cybercrimes in the court of law. The tool adopted by forensic accountants consist of gathering, verifying, processing, analysing and reportage on information so as

to get facts and proof in a predefined context. According to Mold (2018) digital forensic accounting techniques uses many of the traditional methods like interviews and interrogation, background research, confidential informants, undercover, laboratory analysis and analysis of transactions. Besides from the above tools, the forensic accountants also deploy electronic and physical surveillance in order to obtain the required evidence.

i. *Ratio Analysis* – This involves calculating both traditional and non-traditional financial ratios such as accruals to assets, assets quality, asset turnover, gross margin, increase in intangibles, as well as deferred charges to operating performance margin. Since ratios standardize firms for size and other factors, one would expect firms within an industry to follow similar trends. Generally, one would begin to raise suspicion when a particular firm's ratio is uniquely different from the industry normal.

ii. *Data Mining Techniques* – This is the set of assisted techniques designed to automatically mine large volumes of data for new hidden or unexpected information or pattern. These techniques are categorised into three ways: discovery, predictive and modelling and deviation and link analysis (Olatunji and Aruwaji, 2020). It discovers the usual knowledge or patterns in data without any predefined idea or hypothesis about what the pattern may be. It explains various affinities, association, trends and variations in the form of conditional logic.

iii. *Computer Assister Techniques (CAAT)* – This is the method of using computer programmes to assist the investigators in the performance of their investigations. It is a programme specially designed to enable tracking of transactions consummated through the computer networks.

iv. *Interrogation* – This involves subjecting any suspected person to series of enquiries in order to establish the involvement of the person in any suspected criminal activity.

v. *Interviews* – This involves conducting interviews from various parties for the purpose of gathering information that may indicate fraud risk factors. The main goal in interview is to obtain confessional statements from the suspect.

vi. *Background research* –This is when thorough background research is carried out about the perpetrators of the crime with the view to identifying their past trends with regard to crimes. Research can also be carried out on the nature of the similar crime committed by others in order to have an understanding of how such crimes were investigated.

vii. *Confidential informants* – This is where informants provide information to investigators about the activities of criminals within the environment. Anonymous informants can provide such information in a strict confidential cover. It is one of the most reliable means of tracking criminals.

viii. *Laboratory analysis* – This involves laboratory examination of evidences obtained in order to be very sure of the source. Finger prints of suspects could be analysed in the laboratory for proof of the crime.

ix. *Analysis of transactions* – This involves assessment of financial information with a view to identifying changes in amounts, ratios, trends or relationship. This will enable unusual transactions to be identified.

x. *Electronics and physical surveillance* -

Roles of forensic Accounting

The importance of forensic accounting cannot be overstated. As noted in the earlier discussions, forensic accounting is useful in many areas of human endeavours. However, the importance of forensic in the management and control of cybercrimes will be our focus. Firstly, the application of

forensic accounting will facilitate the collection of admissible evidence in court which will be used to prosecute the cybercriminals. This is importance in that the criminals have to be prosecuted in order to serve as deterrents and as well enable the prosecuting agencies to recover the stolen assets and restore the victims to their original state prior to their being attacked. It should be noted that forensic accounting facilitates the quantification of the economic losses or damage associated with cybercrimes activities. It identifies how cybercrime incidents have impacted the business' controls, calculating the potential losses and assisting with collection of evidence.

The second importance of forensic is to expose the trail of movement of ill acquired assets. The deployment of forensic accounting facilitates the tracking of movement of money and other assets acquired through dubious means. This is importance in that the criminals have different means of integrating ill-acquired wealth into the society. Forensic accounting provides the trail necessary to track the assets wherever they are located. The third is the reduction in the amount of cybercrime activities in the country.

Internet Fraud or Cybercrimes

The internet fraud has been described as cybercrime or as 'yahoo-yahoo' in Nigeria. It is an unauthorised access to the internet space of unsuspecting person or organisation with an attempt to carry out illegal transaction. The Federal Bureau of Investigation (FBI) defines internet fraud as the use of internet access to defraud victims or to otherwise take advantage of them. This often results in millions of dollars being stolen from victims from year to year. Mold (2018) documents that cybercrime consists of any criminal action or behaviour that is committed through the use of information technology like cyber hacking, identity theft, cracking, spamming, social engineering, data tampering, online fraud as well as programming attacks. He further describes cybercrime as an economic crime committed using computers and internet and it involves distributing viruses, illegally downloading files, phishing and pharming and stealing of personal information such as bank details. Also Olayiwola (2020) defines internet fraud as a type of fraud or deception which makes use of the internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.

According to FBI there are various forms of internet fraud that have been identified to be employed by cybercriminals during the covid-19 period.

i. Business e-mail compromise – this is the form of fraud which involves compromising legitimate account through computer intrusion to conduct unauthorised transfer of funds.
ii. Data breach – this involves the leakage or spill of data which is released from secure location to an untrusted environment.
iii. Denial of service – this involves interruption of an authorised user's access to any system or network with malicious intentions.
iv. E-mail account compromise (EAC) – this involves the use of compromised e-mails to request payments to fraudsters locations.
v. Malware/scareware – this involves introduction of malicious software with an intention to damage or disable computer systems and thereafter solicit funds from the victims.
vi. Phisting/spoofing – this involves forgery or faking of electronic documents. It involves the dissemination of e-mail which is forged to appear as though it was sent by someone other than the actual source. Phishing involves sending e-mail falsely claiming to be an established legitimate business in order to deceive the unsuspecting recipient into

divulging personal sensitive information such as passwords, credit card numbers and bank account details after directing users to visit a specified website.

vii. Ransomware – this involves delivery of e-mails to an end users resulting in encryption of sensitive files on a corporate network. And when the victim does not want to proceed further, they will demand payment before they are allowed access further.

The main target of internet fraud is to defraud unsuspecting users of internet space of their valuable assets including money, information and other important items. This usually creates untold economic hardship, pain and sometimes disruption of business activities. It also leads to erosion of financial assets of companies and individuals and consequently leads to extermination of such companies. In some cases the activities of internet fraudsters may lead to the early dead of victims.

The world of cybercrime is sophisticated and cuts across different nations and jurisdictions. According to Igwe (2021) Nigeria is currently ranked as the 16th worst affected country by cybercrimes and the rising number of scammers is phenomenal. The reason for the increase in Nigeria can be attributed to the erosion of societal values due to negative influence of politicians who acquire wealth suddenly through appropriation of state resources for their personal use. The advent of Covid-19 led to restrictions in movements which resulted in the loss of jobs and consequently, some of the criminals resorted to cybercrimes for the sake of job security. Cybercrime appears attractive to many partly because the probability of getting arrested is low. In Nigeria, end users of internet space were deceived to download Covid-19 related applications. This crime is perpetrated by individuals, hackers and connected interest.

Causes of cybercrimes or internet fraud

There are many factors which give rise to internet fraud. Generally, the availability of internet facilities and the migration of human activities to the internet would naturally make human beings to contemplate on how to subvert the system and benefit from it. The idle youth would consider this as an avenue to make quick money and prosper in fame and stature. According to Omodunbi, Odiase, Olaniyan and Esan (2016) the main causes of cybercrimes in Nigeria are as follows:

i. Unemployment –The numerous unemployed youths who are not gainfully employed has created the room for them to be exposed to cybercrimes in Nigeria.
ii. Lack of strong cybercrime laws in Nigeria has encouraged those committing the crime to believe that they will not be caught and therefore continue in the act.
iii. Quest for quick wealth – Youths of today are not willing to start small and growbut rather they want to get rich like other adults who have worked to get rich.
iv. Incompetent and unskilled security to handle computers and thereby exposing computers to cyber activities.
v. Lack of proper regulations guarding the operations of cyber activities in the country.
vi. Poor orientation of the youths on issues of crimes in Nigeria.
vii. The increase in internet access which makes more services to rely on them, and thus expending the cybercrime landscape to continue to expand.

Areas of cybercrimes

Every activity conducted through the internet is a potential target of cybercrimes. However, the major target areas of cybercrimes are as follows:

- Banking sector – the banks globally have taken advantage of internet services to introduce e-banking services. This creates room for internet fraudsters to execute fraudulent activities

with ultimate goal of illegally accessing user's account to carry out transactions without the authority of the rightful operator of the account. Different acts committedcomprises of BVN scams, phishing, cyber theft or banking fraud.

- E-commerce sector – This involves the use of technology particularly the internet to buy or sell commodities or services. Crimes in this area include software piracy, sales fraud and forgery, data airtime theft and manipulation.
- Cybercrimes in education sector – Included ere is plagiarism and theft of copyright of original owners.

Empirical Literature

Though literature on forensic accounting is relatively scanty, there are still some research work that have been carried out in this subject. Akinbowale (2018) conducted a study on the impact of information communication technology on forensic accounting practice. The data for the study were generated through questionnaires administered on randomly selected staff of Accountant General Office in Ogun State. The data were analysed using Kolmorov-Smirnov test and percentages. The result of the analysis reveal that IT based forensic accounting has significant agreement with the speed of detecting fraud with other financial crimes in the process of forensic investigation.

Okpara (2019) conducted a study to evaluate the impact of forensic accounting on financial fraud control in Nigeria public sector. The data for the study were obtained from questionnaires administered on selected respondents. The data were analysed using multivariate analysis. The result of the analysis showed that forensic accounting is an effective tool to control financial fraud in the public sector.Mold (2018) conducted exploratory study on the concept and relevance of forensic accounting and concluded that forensic accounting has come up with an effective tool for preventing the menace of cybercrimes.

Olatunji and Aruwaji (2020) conducted a study to investigate the effect of forensic accounting investigations on financial cybercrimes and terrorist financing using primary data obtained through questionnaires administered across a section of staff of agencies that use forensic accounting in their operations. Their findings reveal that forensic accounting can reduce financial cybercrime and terrorist financing. The study concludes that forensic accounting is suitable in investigating terrorist's financial transactions and procedures of cybercrime.

Olaoye and Akinleye (2021) investigated the impact of forensic accounting techniques for combating financial crimes in Nigerian public sector. The study adopted a survey research design with questionnaires administered on 86 accountants and auditors in selected ministries in Osun State. The data obtained were analysed using descriptive and inferential statistics tools. The result of the analysis shows that combating financial crimes in the public sector is possible through the application of forensic accounting tools.

Hamdan (2018) investigated the effect of forensic accounting on discovering and mitigating fraud. The study adopted survey research design and data were collected through questionnaires. The study used confirmatory factor analysis as a tool to figure out the contribution of different items to forensic accounting variables and contribution to discovering fraud. The findings of the study revealed that forensic accounting is an effective tool to find fraud. That is, forensic accounting is crucial and very important in helping to mitigate against fraud.

Theoretical framework

This study is anchored on the theory of fraud triangle. This theory was propounded by Crassey in 1953 to explain that there must be reason behind every criminal activities done by any human being. The theory identifies three basic factors responsible for commitment of an offence. These include: pressure, opportunity and rationalization. Relating this to cybercrime, the pressure for this crime comes from the influence from others such as peer group, societal decadence and weakness of the system. The advent of covid-19 which compelled everybody to stay at home and the need to do business online real time provided the opportunity for the criminals to increase the tempo of their cybercrime activities. Thus opportunity became more pronounced and this brought about the increase in the number of cybercrimes. The rationalization was the get rich syndrome and hustling mentality which anything that brings money to the table legal or illegal was justified in the eyes of the perpetrators of cybercrime in Nigeria. The cybercrime was considered as get-rich-quick syndrome by the perpetrators. AccordinglyAbdullahi andMansor (2021) re-echoed that the perpetrators of cybercrime usually formulate some morally acceptable reasons to engage in unethical behaviours.

Methodology

Hypothesis Development

In order to conduct the study three hypotheses were postulated which will be tested to see the effect of forensic accounting/fraud investigation on internet fraud.

H_1: The deployment offorensic accounting tools does not haveany effect on Cybercrimes management and control.

This hypothesis was formulated to test whether the deployment of forensic accounting mechanism has any effect oncybercrime activities. A positive response would really justify the importance of forensic accounting in the reduction of cybercrime activities.

H_2: The application of forensic accounting tools are effective in obtaining reliable and admissible evidence about internet fraud.

This hypothesis was aimed at examining whether forensic accounting tools are actually effective in obtaining reliable and sufficient evidence about internet fraud which are admissible in law court.

H_3: The deployment offorensic accounting tools are very effective in the tracking and recovery of stolen assets through cybercrimes

This hypothesis was postulated to examine whether thedeployment of forensic accounting tools could have any effect in the tracking and recovery of stolen assets. A positive response here will justify the needof deploying forensic accounting tools in the recovery of stolen assets.

Model Formulation

The dependent variable in this study is the management and control of cybercrimes. Based on the various hypotheses postulated, the functional relationship between forensic accounting tools and cybercrimes management and(CM&C), reliable and admissible evidence (R&AE) and tracking and recovery of stolen assets (T&RSA) are expressed in functional models. The first model establishes the relationship between the dependent and independent variables as follows:

The first model shows the relationship between forensic accounting tools and cybercrimes management and control as follows.

$$FAT = f(CM\&C)) \ldots\ldots\ldots\ldots\ldots \quad (i)$$

Where CM&C = Cybercrime management and control.

FAT = Forensic accounting tools.

The second model shows the relationship between forensic accounting tools and collection of reliable and admissible evidence as follows.

$$FAT = f(R\&AE) \ldots\ldots\ldots\ldots\ldots\ldots \quad (ii)$$

Where FAT = Forensic accounting tools.

R&AE = Reliable and admissible evidence

The third model shows the relationship between forensic accounting tools (FAT)and tracking and recovery of stolen assets is stated as

$$FAT = f(T\&RSA) \ldots\ldots\ldots \quad (iii)$$

Where FAT = Forensic accounting tools

T&RSA = Tracking and recovery of stolen assets.

The fourth model shows the relationships among the three models earlier stated as follows

$$FAT = ß_0 + ß_1CM\&C + ß_2R\&AE + ß_3T\&RSA + \mu \ldots.(iv)$$

Where $ß_0$, $ß_1$and $ß_2$are coefficients respectively which will be obtained from the analysis of the data; while μ is the stochastic error tem included in the model to measure other variables which affect internet fraud control but which are not captured in the model.

Data collection

This study uses descriptive design. The data for the study were obtained from primary sources through questionnaires administered on some personnel of agencies responsible for the management and control of cybercrimes in Nigeria. The questionnaires were designed to seek the opinion of respondents on whether the application of forensic accounting tools have really moderated the effect of internet fraud during the covid-19 period through reduction in internet fraud and recovery of stolen assets. The respondents included the practicing accountants and staff of investigating agencies.Eighty (80) questionnaires were administered and only sixty four (64)representing eighty percent (80%) were retrieved.

Analyses of Data

The responses were analysed with percentages, correlation and regression models. The questions used four scale Likert system as follows: strongly agreed (SA) with four points, agreed (A) with three points, disagreed (D) with two points and strongly disagreed (SDA) with one point. The questions were grouped into four categories to cover the three hypotheses and the dependent variable.

The various hypotheses earlier stated are tested. The data were analysed using the Statistical Packages for Social Science (SPSS 20.0 version). The decision rule is that the null hypotheses will be accepted if the calculated ‘F’ statisticand ‘t’- Statistic is lower than the critical or tabular value at 5%

significance level. The reverse will be the case if F and t-Statistic is greater than the critical or tabular value.The results of analyses are shown in the subsequent subsections.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.449	4.162		.829	.420
	C&MC	.327	.209	.265	2.564	.139
	R&AE	.943	.206	.892	4.579	.000
	T&RSA	.327	.237	.383	2.379	.188

a. Dependent Variable: FAT

Hypothesis One

The hypothesis is stated as follows:
The deployment of forensic accounting mechanisms does not have any effect oninternet fraud activities.
The results of the analysis as shown in the table above indicate that the beta factor of the application of forensic accounting toolson cybercrimes activities stood at 0.265. This indicates that the variation in cybercrime activities is accounted for by variations in the deployment of financial analysis tools. The t-value of 2.564 is greater than 1.960 at 5% level of significance indicating that the result is significant and that the null hypothesis should be rejected. This implies that the deployment of forensic accounting tool have significant effect on the activities of cybercrimes.

Hypothesis two

The second hypothesis states as follows:
The application of forensic accounting tools are effective in obtaining reliable and admissible evidence in court about internet fraud.

The results of the analysis in the table above shows the beta factor of the relationship between the application of forensic accounting tools and the collection of reliable and admissible evidence in court stood at 0.892. This shows that 89.2 percent of variations in the collection of reliable and admissible evidence in court is accounted for by the application of forensic accounting tools. Moreover, the t-value of the relationship stood at 4.579 and this is greater that the tabular value of 1.960 at 5% level of significance. This therefore provides sufficient evidence to reject the null hypothesis thus signifying that the deployment of forensic accounting tools is effective in obtaining reliable and admissible evidence in court.

Hypothesis Three

T*he deployment of forensic accounting and fraud investigation tools are very effective in the tracking and recovery of stolen asset through internet fraud.*

The beta factor of the results of analysis of the relationship between the application of forensic accounting tools and the tracking and recovery of stolen assets stood at 0.383. This indicates that 38.3

percent of variations in the tracking and recovery of stolen assets is accounted for by the application of forensic accounting tools. Furthermore, the t-values of the distribution of 2.379 was greater than the tabular value of 1.960 at 5% level of significance thereby providing sufficient evidence to reject the null hypothesis. Thus the alternate hypothesis is accepted indicating that the deployment of forensic accounting tools is effective in the tracking and recovery of stolen assets.

Discussions of findings

The model summary of the results of analysis is presented in the table below. The results shows that the adjusted coefficient of determination of the model stood at 0.933 indicating that 93.3 % variation in the dependent variable is accounted for by variation in the independent variable. Secondly, all the parameters that measure the outcomes of the deployment of forensic accounting were positive indicating that the deployment of forensic accounting tools had overall positive effect on the management and control of cybercrimes.

This is further interpreted to mean that the overall changes in the management and control of cybercrimes is accounted for by changes in the deployment of forensic accounting mechanisms.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.973[a]	.947	.933	12.73654

a. Predictors: (Constant), INTT, FAT, DMT, CAT

This finding is consistent with prior studies of Olaoye and Akinleye (2021), Olatunji and Aruwaji (2020) who have all concluded that the deployment of forensic accounting mechanisms contributed to the reduction of cybercrimes. The findings are also consistent with the findings of Hamdan (2018) who found that forensic accounting is an effective tool in finding fraud. Moreover, the findings of the study corroborates the apriori expectations that the deployment of forensic accounting mechanisms should bring about positive effect on the management and control of cybercrimes.

Conclusion and Recommendations

The findings of the study reveal that the application of forensic accounting tools have effect on cybercrime management and control. The application of forensic accounting has been found to facilitate the management and control of internet fraud. This is achieved through the collection of reliable and admissible evidence which are used to prosecute the perpetrators of the crime in court. Also the application of forensic accounting mechanisms have helped to trace, track and recover stolen assets through cybercrimes and restore the victims to their state before the the crime.

As a consequence of the above, the study concludes that the application of forensic accounting tools is effective in mitigating against cybercrime management and control.

The study recommends that investigators of cybercrimes activities should be properly trained on the application of forensic accounting tools as this will facilitate their functions. Secondly, there should be sufficient legislation regulating the activities of cybercrimes in Nigeria. The Nigerian youths should be properly counselled on the effect of cybercrimes activities. The study discovers that those who mainly engage in cybercrimes are youth. These youths are unemployed so they capitalise on their idleness to engage in cybercrime. Consequently, this study recommends that government should develop deliberate youth employment policy that keep the youth busy. Moreover, social welfare programmes targeted at the youth development should be initiated.

References

Asadu, U. (2021). Nigeria is ranked 16th in FBI global cybercrime victim's report, The Cable News, consulted on 6/3/2022.

Abdullahi, M. A. (2020). Forensic Accounting and Investigation, ANAN training Manual for 2021 MCPD Programme.

Akinbowale, O. E. (2018). Information Communication Technology and Forensic Accounting in Nigeria, International Journal of Business and Finance Management Research, 6 (2018) 1-7.

Ayas, O. (2021). The Intersection of Law and Business: Forensic in Turkey, Academia Letters, Article 2688. https://doi.org/10.20935/AL 2688.

Erasmus, E. G. &Ibezim, O. F. (2021). Forensic Accountants as Expert Witness in Nigeria: A Literature Reflection, International Journal of Economics and Financial Management, 6 (2).

Hamdan, M. W. (2018). The role of forensic accounting in discovering financial fraud, International Journal of Accounting Research, 6 (2).

Hopwood, W., Young, G. and Leiner, J. (2013). Forensic Accounting and Fraud Examination, McGraw-Hill Companies, USA.

Igwe, U. (2021). Nigeria's growing cybercrime threats needs urgent government actions. Downloaded on 6/3/2022 from: https://blogs.lse.ac.uk.africaatlse/2021/6/09.

Imoniania, J. O, Antunes, M. T. P and Formigoni, C. (2013). The Forensic Accounting and Corporate Fraud, Journal of Information System and Technology Management, 10 (1).

Kemp, S. Buil-Gil, D., Monera, A., Miro-Llinares&Castano, D. (2021). Empty Streets, Busy Internet: A time series analysis of cybercrime fraud trends during covid-19, Journal of Contemporary Justice.

Ma, K. W. and Mckinnon, T. (2020). Covid-19 and Cyber Fraud: Emerging threats during the pandemic. Downloaded 3/1/2022 – Doi: 10.13140/RG2.2.18540.39042.

Modugu, K. P and Anyaduba, J. O. (2013). Forensic Accounting and Financial Fraud in Nigeria: An Empirical Approach, International Journal of Business and Social Science, 4 (7).

Modumere, I. and Onumah, J. M. (2013). Forensic Accounting: a Relief to Corporate Fraud, Research Journal of Financial Accounting, 4 (14).

Mold, S. (2018). Fighting Cybercrimes using Forensic Accounting: A tool to enhance Operational Efficiency IJMBF 7 (3).

Nabiebu, M. &Akpanke, S. A. (2021). Covid-19 Pandemic and Anti-cybercrimes crusade in Nigeria: Changing the narratives for better enforcement regime, Journal of Legal, Ethical and Regulatory issues, 24 (36).

Okpala, K. E. (2019). Forensic Accounting and Financial Fraud control: Across sectional Analysis of Nigerian Public Sector, Journal of Forensic Accounting Fraud Investigation, 4 (1).

Olatunji, T. E. and Awuraji, A. M. (2020). Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing, Journal of Auditing Finance and Forensic Accounting, 8 (2).

Olayiwola, P. O. (2020). Computer Forensics and Cyber Security: A Compilation of Glossary and Definitions, Digital & Computer Forensics Associates, Abuja.

Omodunbi, B., Olaniyan, O., Odiase, P. O. & Esan, A. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention, https://www.researchgate, net/publication/320411102.

Omodunbi, B. A., Olaniyan, O. M., Adeyanju, I. A., Sobowale, A. A. Okonba, N. Esan, A., Adanigbo, O. O. and Oluseji, A. T. (2020). International Journal of Advanced Researchin Engineering and Technology, 11 (9).

Pearson, T. (2008). Fraud and Forensic Accounting in the digital environment, Issues in Accounting Education, 23 (4).

Suchi, P.M and Wika, P. N. (2021). Cybercrime and Terrorism Financing: Nigeria's Potential Vulnerabilities and Policy Options, International Journal of Research and Innovation in Social science V (VII)