International Journal of Social Sciences

Cyber Fraud in the Commercial Banks among the Public in Ibadan Metropolis, Oyo State Nigeria

by

Oluwafemi Amose Idowu
Deparment of Sociology
Nigeria Police Academy, Wudil, Kano State.
Email: idowuoluwafemiamos@yahoo.com
+234 8036759207 and +234 8144448159

Abstract

This study, cyber fraud in the Nigeria Banking System in Ibadan in Oyo State was surveyed in order to determine the perpetrators, causes, effects and means of control in Nigeria nowadays. Primary data was collected from 10 purposively selected banks in Ibadan, Oyo State and the general public who could testify to the issue of cyber fraud in Nigeria with the aid of survey (questionnaire) and In - Depth interview. Simple percentage comparison was used to analyze the data, with the aid of frequency tables. The findings of the study revealed that, educated youths (particularly males), bank staff, customers and non - bank customers are the major perpetrators of the menace of cyber fraud in Nigeria. Cyber fraud is caused in Nigeria by several social – cultural, economic and technological factors; and the national economy bears the effects at large (locally and internationally). It was concluded that, the menace calls for immediate attention before it soiled the nation. It was, therefore, recommended from the study that jobs be creation for the youths; adequate modern security technology in the banking sector; enhancement of the law enforcement agents; sensitization of the public on the implications of cyber fraud through education in order to curb cyber fraud in the Nigeria banking system

Keywords: Commercial Bank, Crime, Cyber Fraud, Hacking, Technology, Internet.

1. Intoduction

In the olden days, people found it cumbersome to carry huge amounts of money from one place to another for business transactions due to the potential security challenges

involved, and when the use of internet and computer came into the banking system, it was thought that the problems will be solved. In contrast, the advent of the advanced technology has come with its own seed of destruction in the Nigeria banking system, with cyber fraud and other varieties of fraudulent activities. As technology grows, so also, criminality advances on daily bases. Criminality in the banking sector nowadays has gone cyber. It is being committed boundless across national borders. Prior to the year 2001, the phenomenon of cyber fraud in the banks was not globally associated with Nigeria. It is also remarkable that the attempt to launch Nigeria into the digital age coincided with unprecedented rise in computer related financial crimes in the country. Post 2001, the country has been labeled a world - wide notoriety in criminal activities especially financial scams facilitated through the use of the internet.

Fraud is an activity which involves the use of deception to obtain on just advantages; intentional misstatement of accounting records in an omission or commission of amount from financial statement; theft whether accomplished by misstatement of accounting records or financial statement. A fraudulent practice is any form of deception intended to wrongfully obtain money from the reliance of another on the deceptive statement or acts, believing them to be true. As technology advances in Nigeria and in the globe, so also the means of carrying out fraud activities advances. Cyber fraud is any fraudulent activities with the use of internet and it has the possibility to move across boundaries, borders, continents and globally.

Banks are custodians of money, where cash and other valuables are kept, unlike the traditional ages. The banking industry is the pivot on which any economy rotates. Frauds have been identified as one of the most destructive factors that could easily lead to banking failure. The level of fraud is of great concern to all bank stakeholders, such as: shareholders, customers, staff regulators, government, auditors, and consultants and so on. Fraud incidence have been primarily attributed to weak internal control systems. In recent time, the dimensions and scope of fraud have become complex especially with the advancement in the information technology. The increasing number of attack on credit/financial institutions is a globally recognized phenomenon (Chucks, 2008). New technology has given rise to fundamental change in the security system in use.

Cyber fraud in the banking system is one of the principal challenges that relates to the establishment of security centers today. In the simplest terms, fraud occurs when someone intentionally lies to obtain benefits or advantage or to cause some benefits that is due to be denied. Fraud is a global phenomenon. It is unique to the banking industry or peculiar to Nigeria, because the banks deal in money and other financial asset. The ultimate ambition "*wants to get rich quickly*" is to acquire money and the bank has become persistent prime target for fraudsters. There is a general consensus amongst criminologists that fraud is caused by **"**WOE" - *Will, Opportunity* and *Exit*. In example, the will to commit fraud by the individual, the opportunity to execute the fraud; and the exit which is the escape route from sanctions against successful or attempted fraud and forgeries in banking (Godswill, 2002).

Nowadays, the patterns of cyber-crimes are also growing in different dimensions; we now deal more with issues of cloning of websites, false representation internet purchase and other e-commerce kind of frauds. The criminal notably uses false credit cards unlawfully acquired from websites that provide compromising credit card as well as from a Nigerian legally residing in western countries. Other typologies that have been noticed are through the manufacturer of false cheques, gift cards and other instruments of legal transaction. The truth is that, cyber - crime is depressing trade and locally, the harm is growing with the potential of crippling the whole domestic economy if not checked. Consequently, it is a serious threat to our national security and the prosperity of our citizens (Ribadu, 2007).

The issue of fraud in our banks is one of the most intractable and monumental problems to the Nigeria Banking system. The incessant fraudulent practices in commercial banks and the ultimate success of the fraudsters reveal the fact that most banks executives are not fully knowledgeable on the practical cause of bank cyber frauds. Some are aware of the cause, but do not know the effective preventive measures to be adopted. Cyber fraud is a problem and its implications for the banking industry and the society at large have inspired this research. When considering an act of cyber fraud in a society, the causes, means of perpetration and control mechanism must be put into consideration. It is on this background that the types, causes of cyber fraud in Nigeria banks, challenges of the law enforcement agents are examined in this study, so as to suggest the possible measures to control cyber fraud in Nigeria.

2. Literature Review

Fraud is a concept with diverse definitions, depending on the individual's perspective. Fraud is the number one enemy of the business world and no business establishment is immune to it. Fraud is a complex universal phenomenon (Chukwu, 2011).Fraud has gone beyond the Nigerian context; rather it is a global phenomenon. To understand what is meant by cyber fraud, we need to first understand each word separately. Therefore, "Cyber" is a prefix used to describe an idea as part of the computer and information age. The term "Fraud" is used to describe such act as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation and concealment of materials fact. Fraud is "the use of deception with the intention of obtaining undue advantages, avoiding an obligation or causing loss to another party fraud can be perpetuated by person outside as well as inside and by conclusion".

In the broadest sense, "fraudulent practice" is an act of intentional and successful of cunning, deception, collusion or artifice use to cheat or deceive another person whereby that person acts upon it to loss of his/her property and to his/her legal injury**.** It encompasses an array of irregularities and illegal acts characterized by intentional deception.Thus, it is any act or attempt of false or deceptive statement of fact intended to induce another person to rely upon and in reliance thereof, giving up a valuable thing he or she owns or a legal right he or she is entitle to. Zik (2002) defined fraudulent practice as "any form of deception intended to wrongfully obtain money from the reliance of

another on the deceptive statements or act, believing them to be true. Thus, fraudulent practice may be viewed as "any use of di*shonesty,* deception or false presentation in order to gain a material advantag*e".* Godswill (2002) was of the opinion that, fraudulent practice is an intentional misrepresentation, concealment of omission of materials fact done with the purpose of deceiving another which causes detriment to that person. Therefore, for any action to be fraudulent, "there must be an element of dishonest intention to benefit the perpetrator at the detriment of another person".

Computer fraud can remain undetected for a long time. It can take the form of corruption of the program or application packages and even breaking into the system via a remote censor. Storage devices can also be tampered with to gain access to unauthorized areas or even give credit to an account for which the fraud were not originally attended. This is a devastating bank fraud. This is caused by the use of computer and it involves very large sums of money. Such fraud occurs when wrong information is fed to the computer. Thus, it is resulting in the computer producing wrong and inaccurate information of the accounts.

Cyber fraud is any violation of criminal law that involves knowledge of computer technology for its perpetration. Ribadu (2007) revealed that, "indeed of all grand corruption perpetuated daily in our communities, most are of the nature of cyber - crime executed through the agencies of computer and internet fraud, mail, scam, credit card fraud, bankruptcy fraud, insurance fraud, government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, kickbacks, counterfeiting laundering, embezzlement as well as economic and copy right secret theft". Therefore, cyber - fraud refers to any crime that involves a computer and a network, where the computer may have played an instrumental part in the commission crime. With the increase of cyber - fraud in Nigeria, professionals in the information and communication technology (ICT) sector and the general public are emphasizing the need for government to do more to discourage the crime in order to solve the country's internet service and outright condemn the crime (Akano, 2012).

Classification of Fraud Perpetrators in Nigeria Banking System

The dimension that banking fraud has assumed is hydra - headed. The classification made by Ehinmen and Bola (2010) is fascinating and appropriating. They classified bank fraud into the namely: internal fraud, external fraud and mixed fraud. Thus, on the basis of perpetrators, there are three categories:

1. **Internal Fraud:** This is committed by members of the staff. These are fraud perpetrated by employees as well as agents of banks against the same banks. The fraud could assume the following character as reported in Central Bank of Nigeria (CBN) 2008:
   - **i.** Granting unauthorized credits.
   - **ii.** Foreign exchange related frauds such as: tripping, stealing of currencies misappropriation proceeds of traveler's cheque and so on.
   - **iii.** Discrepant transfer arising from falsified latter of authority.
   - **iv.** Suppression of clearing cheques.

v. Payments against unclear effects.
vi. Dry - posting of fictitious credits.
vii. Encashment of forged cheques by fraudsters.
viii. Debiting of head - office account through forged inter - branch credit advice.
ix. Manipulation of customers account.
x. Issuing of bank cheque and drafts without cover.
xi. Falsification of customer's cash lodgment.
xii. Fraudulent clearing of forged cheque and draft through other banks.

The aforementioned bank frauds are common in most commercial banks in Nigeria and they account largely for the sudden riches of some bankers in our outfit. In particular, some officers fund personal business outfits established elsewhere with their banks money without paying any interest on the clandestine loan (Ologun, 1994).

2. Externa Fraud: This is committed by those not connected with the banks. This form of fraud is a high class and sophisticated fraud which is usually executed and christened "419" meaning (Advanced Fee Fraud). It occurs when a customer of a bank or someone non – customer to the bank defraud either a customers of the bank or any other third party. This fraud manifests in the illegal activities of financial criminals that deal with illicit practice such as: looting, money laundering and such other practices. Most banks have fallen victims of these highly professional fraudsters.

3. Mixed Fraud: This is committed by outsiders in collision with bank staff. This is another highly complex form of fraud which falls within the same category of 419 details. This is more complex and difficult to detect.

Notably, other types of fraud that do not really fall under a clear category as above included: delayed payment of interest to customers, illegal charges of bank transactions, declaring bogey or paper profits to shareholders and illegal charges on bank transaction and financial widow aims not only to mislead shareholders, but also to mislead policy makers and the Nigeria public and the unholy alliance of banks and bank external auditors to deceive the Nigeria public and the financial authorities (Adewumi, 1990).

In addition, the analysis of returns from banks on fraud forgeries reveals a myriad of method used by fraudsters in perpetrating fraudulent activities (Wooldrlidgos, 1993). Besides cyber fraud, the most common means being used by fraudsters in the banks are: Declaration of Cash, Cheque Kitting, Inter - Branch Fraud, Computer Fraud, Counterfeit or Forged Cheque, Telex Transfer Fraud, Cheque Fraud, Cash Frauds, Foreign Exchange Frauds, Printing of Bank Stationary and Carving Bank Rubber Stamps, Intentional Wrong Total, Recording of Non - Existence Expenditure, Omission Receipt, I. O. U. (I OWE YOU) fraud, Lending to "Ghost" Borrowers, Balance Sheet Fraud, Over - Loading or Over – Invoicing, Advanced Fee Fraud (419), Clearing Fraud, Money Laundering Fraud, Cheque Kitting, Account Opening Fraud, Discounting or Factoring Fraud.

Types of Cyber Frauds

Cyber fraud in banks varies widely in nature, character and methods of perpetration in general. With the growing use of computers, cyber - frauds are becoming more predominant in today's world, various types of cyber - frauds encompass a broad range of potential illegal activities. Generally, it may be divided according to Omojunwa (1999), and Kuna and Wilson, (2011) into:

1. Spam or Cyber Stalking: Spam is the unsolicited sending out junk/bulk e - mails for commercial purposes. It is unlawful to varying degrees.
2. Alteration of computer inputs/outputs: This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false, or by entering unauthorized instruction by using unauthorized processes. It could also be through altering, destroying, suppressing or stealing output usually to conceal unauthorized transaction. This is usually difficult to detect.
3. Yahoo Boys: These are called 419ers (Advanced Free Fraud). They make use of e – mail addresses obtained or generated from the internet access points using e – mail address access applications (Saulawa and Abubakar, 2014). The Advanced Free Fraud is nicknamed "419", because the Section 419A in the Criminal Code Act, 1990 of the Federal Republic of Nigeria deals with obtaining credit by false pretences or other fraud.
4. Identity Theft: This involves the criminal acquiring the victim's identity and personal information, such as: name, address, place, security number (PIN or Password) and so on; and using the information to impersonate the victim for financial gain. The victim's identity is not stolen literally of cause, but rather used by another person for criminal end.
5. Identity Fraud: Identity fraud on the other hand simply means an unlawful change of one identity either by assuming of a real third person's identity or a completely fiction one altogether. Identity fraud does not necessary involve identity theft, as a person whose identity the fraudster assumes can sometimes be a willful accomplice in the fraud.
6. Phishing Scams: One of the most often used method of identity theft is known as phishing scam. Phishing scams refer to cloning product and e – commerce web pages in attempt to dupe the unassuming victims into given out their personal information and sensitive data, such as: e - mails, instant messaging or online banking users name and password. One common example of phishing scams attack involves the victims been contacted via e - mail by what appears to be a legitimate bank, asking him/her to confirm the user's personal information because potentially fraudulent activities observed in their names. The e - mail contains a link to a genuine looking website and the personal information that the victim submits gets into the hands of the fraudster(s).
7. Password Sniffing: Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they

especially want to penetrate, like telephone systems and network providers. Password sniffers are programs that simply collect the first 128 or more bytes of each network connection on the network that is being monitored. When a user types in a user name and a password - as required when using certain common Internet services like FTP (which is used to transfer files from one machine to another) or Telnet (which lets the user log in remotely to another machine) - the sniffer collects that information. Additional programs sift through the collected information, pull out the important pieces (e.g., the user names and passwords), and cover up the existence of the sniffers in an automated way. Best estimates are that in 1994, as many as 100,000 sites were affected by sniffer attacks (Hassan, Lass and Makinde, 2012).

8. Romantic Scam: This is the most devastating form of cyber fraud, not just because of potential material loss, but also because the victim tends to be among the most desperate and emotionally unstable people. A romantic scam is often harder to detect than a phishing e - mail that passes as a legitimate bank, for instance, because most people who sign up for internet dating site believe that everyone else on the site is as well - meaning as they are. This is especially the case with religion dating sites that involve emotional and psyche manipulation. These scammers also take advantage of presumed morally upright nature of members. They are disguised pretenders that ask the victim's personal information, such as their mailing address with excuses like wanting to send some present and so on.
9. Hacking: Hacking is the gaining of an illegal access or changing of information by an unauthorized person in a computer. A hacker is a specialist in illegal electronics access to the computer. Thus, these are specialists who can break the security code of your account without your presence or permission for e – commerce, funds point cards and e – marking product sites of computer system in order to steal or destroy vital data.
10. Credit Card or ATM Fraud*:* It is a wide ranging term for theft and fraud committed using a Credit Card, Debit Card, Point of Purchase (POS) or any similar mechanism as a fraudulent source of fund in a transaction. The purpose may be to obtain goods without paying or to obtain unauthorized fund from an account (Chucks, 2008). Credit Card fraud is also an adjunct to identity theft. This could be through the following:
    - Skimming: Skimming is the theft of credit card information used in an otherwise legitimate transaction. "It is typically an inside job" by a dishonest employee of a legitimate bank or others. The theft can produce a victim's credit card number using basic method, such as: photocopying receipt or more advanced method such as, using a small electronic device skimmer to swipe and store hundreds of victim's credit card numbers. Common scenario for skimming in restaurants or bars where the skimmers have possession of the victims' credit card out of their immediate view. The theft may also use a small keypad to cleverly transcribe the three or four magnetic strips.

- Carding: It is a term or process to verify the validity of stolen card data. The frauster presents the card information on a website that has real time transaction processing. If the card is processed successfully, the theft knows that the card is still good or valid. The specific item purchased is immaterial, and the theft does not need to purchase an actual product as a website subscription or charitable donation would be sufficient. The purchase is usually for a small monetary amount, both to avoid using the cards to avoid attracting the card issues attention. A website known to be susceptible to carding is known as a card - able website.

Causes of Fraudulent Practices in Nigeria Banks

The fact that banks deal with huge quantity of funds makes it vulnerable to corruption and fraud. According to Omojunwa (1999), Godswill (2002) and Chukwu (2011) the causes of fraud and forgeries in banking are very many. Causes of fraudulent practices in banks are quite numerous, but the under listed causes which are by no means exhaustive are very common:

i. Lack of Adequate Training and Experienced: Fraud will normally lead to loss to a bank if it goes undetected, and experience staff-member that knows it, can easily detect fraud unless he/she is involved. However, where staff members are not adequately trained or do not have enough explosive on the job, it is easier for fraudster to succeed. Lack of adequate training and retraining on both the technical and theoretical aspects of the jobs lead to poor performance which breeds fraud in the banking system. Failure by both management and staff to undergo on - the job - training and even relevant outside courses also leads to unsatisfactory performance which eventually creates more room for malpractice.

ii. Quest for Wealth: Another cause of cyber crime in Nigeria is quest for wealth; there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk. Most cyber criminals require less investment and a conducive environment. Nigeria is such an environment and many cyber criminals take advantage of that (Hassan, Lass and Makinde, 2012).

iii. Poor organization and Bad Management in the Banks: Bad management is in terms of incompetence, inadequate supervision, poor planning, lack of coordination, corruption and ineptitude general funds. Also, the organizational elements that facilitate the practice of the 419 practitioners in defrauding bank include the following: obsolete record keeping, naivety of banks staff regarding experience on the job which fraudsters take advantage of, general unattractive terms non - motivating terms and condition of employment, poor working condition, poor staff welfare, inadequate staffing, volume of work, Banking experience, staff infidelity, poor book - keeping and accounting, faulty personnel policies, frustration, staff negligence, absence of defined job schedule and so on.

iv. Faulty personnel policies: Poor personal policies resulting in poor selection, recruitment, poor job placement, promotion and staff welfare which in turn leads to demonization, lack of job satisfaction, low job enrichment, little job enlargement and absent of career development prospects causes frustration leading to fraud.

v. Poor Internal Control/Internal Check: Inadequate internal control and ineffective and/or inefficient application of internal control measures create loopholes for self inclined staff, customers and non - customers to commit fraud and also ineffective audit. Control is not only internal check and internal audit but the whole system of controls, financial and otherwise, established by the management in order to carry on the business of the bank in an orderly manner, safeguard its assets and secure as far as possible the accuracy and reliability of its records.

vi. Inadequate Infrastructure: Poor communication system, power failure, which result in a back log of unbalanced postings, congested office space, etcetera, are some other factors which encourage the perpetuation of frauds in financial institutions.

vii. Poor Security Arrangement for Documents: In financial institutions where security arrangement for valuable documents is weak, poor and vulnerable, it is easy for fraudsters to have their way without detections. The security arrangement in Nigeria commercial banks should involve advanced technologies. Lack of adequate cyber control and CCTV promote cyber fraud in Nigeria.

viii. Ineffectiveness of Law Enforcement Agents: A fraudster may not be afraid of the consequences o being caught if he knows that the law enforcement agents can easily be bought over. The unwillingness and inability of the police to investigate fraud cases or/and inability of the police to investigate fraud cases or prosecute the offenders help to encourage fraudulent practices.

ix. Weak Implementation of Cyber Crime Laws and Inadequate Equipped Law Agencies: The Nigerian legislation must implement strict laws regarding cyber criminals and when criminal offences occur, perpetrators must be punished for the crime they've committed because cyber crimes reduces the nation's competitive edge, failure to prosecute, cyber criminals, can take advantage of the weak gaps in the existing penal proceedings. Weak /fragile laws regarding cyber criminals exist in Nigeria, unlike in the real world were criminals such as armed robbers are treated with maximum penalties. Unfortunately, the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals. Laura (2012) stated that "African countries have been criticized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime" Nigeria is not an exception to this rule. Furthermore, It is therefore paramount that the nation's legislation should ensure proper implementation of their laws against cyber crime (Hassan, Lass and Makinde, 2012).

x. Socio - cultural environment: The socio – cultural environ in Nigeria is amenable to poor socialization, poverty, moral decay, corruption, lack of accountability,

questionable wealth acquisition (materialism), quick money syndrome, poor judicial system, unwarranted millionaire (without questioning the source of their wealth). Lack of appropriate deterrence for fraudsters and societal clamor for illegal and incriminating assistance from kinsmen in major or cooperate institutions/office, personality profile of fraudsters societal values, delays in the legal process, delay in the legal process, fear of negative publicity, availability of the WOE – (Will, Opportunity and Exit) and so on.

xi. Negative Role Models**:** Youths are mirrors of the society, but it is quite unfortunate how parents neglect their rightful duties. Meke (2012) remarked that, today many parents transmits crime values to their wards, via socialization as if it a socio cultural values which ought to be transmitted to the younger generation. Imagine a situation where the child supplies the father with vital information to wreck individual's banks account using the computer system, while the mother impersonates the account holder/owner at the bank. If this culture is imbibed among the younger generations, many of them will see no wrong in cyber crime practices (Hassan, Lass and Makinde, 2012).

Challenges of Combating Cyber Fraud in Nigeria

The challenges of the Nigeria law enforcement agents in combating cyber - fraud are not far – fetched. Notably among them are:

i. The Nigeria Criminal Code which can also presently be used to persecute those criminals, most of the activities of these criminal bother on first pretense, cheating which section 421 and 419 of Nigeria criminal code prohibited respectively. False pretense is the crime of knowingly obtaining title of another's personal property by misrepresenting a fact with the intention to defraud. This calls for review.

ii. Cyber Security and Information Protection Agency Bill (2008); a critical analysis of second draft bill highlight a number of gaps and identify the challenges the Nigeria faces when it comes to understanding and implementing adequate and sufficient computer crime and privacy legislation. There a number of sections with this bill that will need to be amended, removed and added to, before it can be deemed and appropriate and up to date legislation to deal with computer crime related activity applied in the 21st century.

iii. The Nigeria police lack internet policing capability: Nigeria law enforcement agencies are basically technology illiterate. They lack computer forensics training to deal with cyber - crime or combat cyber fraud. Without trained expert on the internet policy there is no way the perpetrator of cyber crimes can be brought to justice. The use of Global Positioning System (GPS) and Geographical Information Systems (GIS) will help a lot in the crime mapping and nabbing.

iv. Difficult to prove: Another challenge is that cyber – crime/fraud in Nigeria is difficult to prove as it lacks the traditional paper audit trail which requires the knowledge of specialists in computer technology and internet protocols where there

are no audited trials of the crime then combating the crime will be very much difficult to execute.

v. Weaken technology platform and digital illiterate environment: Another challenge is that Nigeria is currently operating on a weak technology platform and digital illiterate environment that is in urgent need of expert solution. The level of technological development in Nigeria is very weak compared to other developing countries, as such tracing and detecting cyber - crime is always difficult.

vi. Lack of central computer crime response wing: Nigeria lacks a Central Computer Crime Response wing to act as a guide and to coordinate computer crime investigation activities. The computerization project of Nigeria police formation should have served as a starting point of establishment of central computer crime response wing, but only stopped at computerizing of personal record, payroll and comparative, crime statistics and so on.

3. Methodology

This study made use of data obtained from a cross section of the staff members of 10 selected banks in Ibadan, Oyo State Nigeria and the general populace in Ibadan metropolis in Oyo State for information gathering. Purposive sampling method was used to administer the questionnaire among the respondents. The survey sampling involved the use of both simple random sampling technique and purposive sampling technique. A set of One Hundred and Eighty (180) copies of the questionnaire was administered as follows: 100 copies within the 10 selected banks (10 copies in each bank) and 80 copies for the general public. Altogether, 172 copies of the questionnaire were recovered. The information collected was analyzed into tables, percentages and pictographs. Frequency tables and percentages were used to analyze the data and the total numbers of items will be given. The purposively selected banks to be used in Ibadan are: Access Bank, Diamond Bank, First Bank Nigeria Plc., First City Monument Bank, Guaranty Trust Bank, Skye Bank, United Bank for Africa, Unity Bank, Wema Bank and Zenith Bank.

4. Results and Findings

The analysis of data collected from the field and its finding are presented in tables 1:

Table 1: Factors Influencing Cyber - Fraud in Nigeria Banks

S/N	QUESTION	YES	%	NO	%
i.	Contact with the Western World (developed Countries) intensifies cyber fraud rate in Nigeria.	**141**	82.0 %	**31**	18.0 %
ii.	Cyber fraud in Nigeria is caused by unemployment or poor recruitment system.	**145**	84.3 %	**27**	15.7 %
iii.	Improper internal control and monitoring promote cyber fraud in Nigeria	**163**	94.8 %	**9**	5.20 %
iv.	Technological advancement contributes to	**147**	85.5 %	**25**	14.5 %

	the increased rate of cyber fraud in Nigeria.				
v.	Poor security system encourages cyber fraud in Nigeria.	**155**	90.1%	**17**	9.90 %

Source: *Field study, 2016***.**

Table 1 revealed that Nigeria's contact with Western culture (developed countries) intensifies cyber fraud rate in Nigeria. This was affirmed as 141 (82.0 %) of the respondents agreed that Nigeria relationship with the Western World has great impact on the intensity of cyber fraud rate in Nigeria; while the remaining 31 (18.0 %) of the total respondents said that Nigeria's relationship had nothing to do with the increasing waves of cyber fraud in Nigeria. Also, it was further discovered that, high rate of unemployment or poor recruitment system in Nigeria has effect on cyber fraud in Nigeria. In the study, 145 (84.3 %) of the total respondents took the stands that the major cause of high rate of cyber fraud in Nigeria was the high rate of unemployment; 27 (15.7 %) respondents responded that cyber fraud was not caused by unemployment or poor recruitment system in Nigeria.

Also, it was discovered that improper internal control and monitoring of banking activities promote cyber fraud in Nigeria. Hence, 163 (94.8 %) of the respondents supported that improper internal control and monitoring promote cyber fraud in Nigeria banking system; and only 9 (5.20 %) respondents argued that the issue of improper internal control and monitoring do not contribute to the cause of cyber fraud in Nigeria. Furthermore, the study showed that the factor contributing to the high rate of cyber fraud in Nigeria is not far – fetching than technological advancement. This was affirmed as 147 (85.5 %) of the total respondents agreed that technological advancement contributes to the increasing rate of cyber fraud in Nigeria. And on the other hand, 25 (14.5 %) argued against the effect of technological advancement on the occurrence of cyber fraud in Nigeria.

It was revealed that, poor security system in Nigeria has encouraged cyber fraud in Nigeria: 155 (90.1 %) of the respondents agreed that poor security system encourages cyber fraud in Nigeria. In the other hand, only 17 (9.90 %) of the total respondents in the study disagreed that poor security system promotes cyber fraud in Nigeria.Therefore, it generally showed that Nigeria's contact with the Western World, high rate of unemployment in the country, improper internal control and monitoring in the banks technological advancement, poor security system in Nigeria and so on have one way or the other, contributed to the problem of cyber fraud in Nigeria banking system.

TABLE 2: Facilitators and Perpetrators of Cyber Fraud in Nigeria

S/N	QUESTION	YES	%	NO	%
i.	Bank staff contributes to the high rate of cyber - fraud in Nigeria.	**117**	68.0 %	**55**	32.0 %
ii.	Cyber fraud in Nigeria is majorly perpetrated by the youths.	**156**	90.7 %	**16**	9.3 %
iii.	Government also involves in cyber - fraud in Nigeria.	**76**	44.2 %	**96**	55.8 %
iv.	Cyber - fraud in Nigeria banks is perpetrated by the bank customers.	**84**	48.8 %	**88**	51.2 %
v.	Non – bank customers are majorly involve in cyber fraud in Nigeria.	**98**	57.0%	**74**	43.0 %

Source: *Field study, 2016*.

Table 2 shows the facilitators and perpetrators of cyber fraud in Nigeria. It was revealed that almost everybody perpetrates in fraud in the Nigeria banking system one way or the other. The table shows that, 117 (68.0 %) of the respondents in the study agreed that bank staff also contribute to the high rate of cyber fraud in Nigeria; while the remaining 55 (32.0 %) of the total respondents were of the opinion that bank staff were not contributing to the high rate of cyber in Nigeria banking system. It was further found out that the major perpetrators of cyber fraud in Nigeria were youths. This was affirmed by 156 (90.7 %) respondents in the study; and only 16 (9.3 %) of the total respondents disagreed. This simply indicated that people in their youthful ages are more prone to the activities of cyber fraud as a result of their education attainment and eagerness to get quick money syndrome.

It was evident from the study that, government officials did not directly involve in cyber fraud in Nigeria. Hence, 76 (44.2 %) respondents agreed and 96 (55.8 %) of the total respondents disagreed. The implication is that, government officials cannot be totally exempted from cyber fraud activities in Nigeria. One way or the other, they are contributory factors. Moreover, it was a bit difficult to strike out any serious margin to know if cyber fraud in Nigeria banks is perpetrated by bank customers only or not. The study showed that, 84 (48.8 %) of the total respondents believed that cyber fraud activities were perpetrated by bank customers only; and 88 (51.2 %) of the total respondents refute this belief. They were of the opinion that cyber fraud was perpetrated by the banks' customers and non – bank customers, since it involves cyber – link. In the same vein, 98 (57.0 %) of the total respondents agreed that non – bank customers are majorly involved in cyber fraud in Nigeria.

In general, it is very glaring that bank staff, youths, government officials, both bank customers and non – bank customers one way or the other act as facilitators or perpetrators of cyber fraud in the Nigeria banking system.

TABLE 3: Effects of Cyber Fraud in Nigeria Economy

S/N	QUESTION	YES	%	NO	%
i.	Cyber fraud has ruined many individual's businesses in Nigeria.	160	93.0 %	12	7.0 %
ii.	Cyber fraud has tainted the Nigeria image locally and internationally.	161	93.6 %	11	6.4 %
iii.	Cyber - fraud has adversely affected Nigeria economy.	127	73.8 %	45	26.2 %

Source: *Field study, 2016.*

It was revealed that, cyber fraud has ruined many individual's business in Nigeria. This was very obvious in the study as 160 (93.0 %) of the total respondents were in support of the opinion that cyber fraud has ruined many individual's business in Nigeria; and only 12 (7.0 %) of the total respondents went against the notion. Not that alone, 161 (93.6 %) of the respondents believed that cyber fraud has also tainted the Nigeria image locally and internationally; from which only 11 (6.4 %) of the total respondents disagreed that cyber fraud has tarnished the country's image at home and abroad. Furthermore, it was also observed from the study that cyber fraud has adversely affected Nigeria economy. From the total respondents in the study, 127 (73.8 %) of them confirmed that cyber fraud has adversely affected the Nigeria economy and so onwhile 45 (26.2 %) respondents disagreed. They were not of the opinion that the issue of cyber fraud did have any economic implication on Nigeria.

5. Conclusion and Recommendations

This research was primarily designed to get in - depth knowledge of the relationship between technology and fraudulent activities in the Nigeria banking system in Ibadan, Oyo State; its effects and possible solutions. The study was conducted to find out the factors that enhance cyber fraud in the Nigeria banking system and to make recommendation on how to control the menace of fraudulent activities in our banking system. The Nigeria police force and other law enforcement agents are saddled with the task of enforcing the law of cyber fraud and others in the banking sector, but their activities and abilities are hampered with inadequate equipment, politics, greedy, poverty, poor welfare and logistics, lack of required skills and other factors to combat the fraudulent activities in our banking system (cyber fraud precisely) in Nigeria.

The situation has created a very bad image for the country and its law enforcement agents. The law enforcement agents are perceived to be hostile, unfair and unjust to the public they are paid for to prevent from being vulnerable to cyber fraud in Nigeria banking system. Bank staff members are not exempt as they serve as aid and abating to the cyber fraud perpetrators in Nigeria. Cyber fraud is perpetrated by different people and it shows that illiterate does not perpetrate in cyber fraud as it requires knowledge and skills (technicalities). Inter – relationship between Nigeria and the Western world promotes cyber fraud in Nigeria.

It was revealed from the study that unemployment is a factor that majorly causes cyber fraud in Nigeria. And the corrupted recruitment procedure is a contributory factor as the notion is embezzlement (getting quick syndrome) by the non – intrinsically motivated job seekers. Thus, unemployment and poverty enhance the full involvement in cyber fraud in Nigeria. Lack of employment opportunities, low standard of living and abject poverty compel some people to indulge in fraudulent acts. This could also be adduced to poor socialization system and peer group influence contributes a lot to the increasing waves of cyber fraud in the Nigeria banking system among the youths.

Also, improper internal control and inadequate monitoring were discovered to promote cyber fraud in Nigeria banking system. It was unveiled that Nigerian banks lack internal control and adequate monitoring which make them to be vulnerable to cyber fraud perpetrators. Thus, if there was adequate internal control and monitoring in the banks, it would be difficult for the fraudsters to gain access to the people and individual's accounts. Ordinarily, the manifest function of technological advancement is for development, while the latent function is criminality. In the same vein, as technological advancement brought socio – economic development in the country, so also has it brought advancement in criminality. Therefore, technological advancement invariably contributes to the increasing rate of cyber fraud in Nigeria. It was also discovered that some bank staff members also perpetrate in the activities of cyber fraud in Nigeria. It was revealed that some of them serve as agent (informant) of criminality that gives vital information about customer's account to their allies.

With reference to the effect of cyber fraud in Nigeria, it was found out that cyber fraud has ruined many individual's business in Nigeria. Apart from the issue of the individuals, cyber fraud has also tainted the image of Nigeria in the World at large. Nigerians are now viewed as corrupt and dubious people within and abroad. Even at embassies, Nigerian visas are critically and thoroughly check with suspicions. This has also affected the country's economy adversely. Many countries are scare to do business with Nigerians in the other countries. The end result is that our economy is in jeopardy.

It was concluded from the study that cyber fraud has gone viral and the Nigeria law enforcement agents are handicapped in the area of cyber fraud control, cyber fraud has dented the image of the country both home and abroad, it affects the national economy adversely, Nigeria cyber crime laws are not well implemented and the security control systems in the commercial banks are too weak, ineffective and obsolete. It was suggested that that all hands must be on desk in order to control the hydra – headed monster (cyber fraud) in Nigeria.

Based on the findings of the study, the following recommendations were made to ameliorate the menace of cyber fraud in Nigeria banking system:

1. Job creation: The people with technical know – how (cyber - crime knowledge) should be employed in banking job and there should be adequate provision of job opportunity for the teeming youths and empowerment. Computer gurus and graduates should be employed in the field as cyber – fraud control agencies.

2. Security: There is the need for effective security system with latest equipment on bank information. In other words, there should be restriction of some valuable information to customers and robust passwords should be used to secure online links and there should be adequate internal control, supervision and monitoring in banking transactions that is computerized (inbuilt software and devices).
3. Law Enforcement: The law enforcement agents should be well – trained in cyber – crime control. There should be adequate and stiffer punishment implementation for any offender caught. There should be implementation and regulation of rules that bind the activities of cyber cafes, with adequate monitoring by the cyber - crime special task force. Thus, special cyber fraud investigation unit should be introduced and empowered in every bank in Nigeria.
4. Education: Sensitization of youths on the implication of cyber fraud and encourage literacy at all levels. Every individual should be educated and oriented on the safe – keeping of their bank account PIN. The general public should be enlightened on cyber – fraud. Business organizations and individuals should always protect their bank account and other related information strictly.
5. Technology: Also, there should be provision of digital national identification card for each Nigerian with centralized national database of the citizens and immigrants. There is the need for central processing of bio – data and thumb – printing of all citizens in a database to detect fraudsters. Advanced technological security system should be introduced in Nigeria banking system, such as: using Interactive Voice Response (IVR), terminals advanced tracking devices and the available ones should be upgraded when new technology is introduced.
6. Self - caution: Everybody should take good and extra care of their ATM or debit cards know where it is at all time, if you lose it, report as soon as possible. Never accept any form of help by strangers if you encounter a malfunctioning ATM. Choose a pin for your ATM or debit card that is different from your address, telephone number, or birth date, this will make it difficult for a thief to use your card through information already known to him. Make sure you know and trust merchant before you can share any bank account or card information or pre-authorized debit to your account. Make sure you do not open a code of transfer fund to someone that you know is not a staff of that bank that is operating your account.

7. References

Adewumi, W. 1990.Fraud in Banks.Nigeria Institute of Bankers. Lagos.

Akano, A. O. – DIG 2012. Objective of G - Department (ICT). Retrieved from: www.mpf.gov.ng

Central Bank of Nigeria (CBN) Research Department. 2008. *ND/CQuarterly*. Vol. 18.No. 4.December.

Chucks, N. O. 2008. Zenith Economic.*Quarterly*.Vol. 3. No 4. October.

Chukwu, P. O. 2011. *Fraud in the Nigerian Banking Systems, Problems and Prospects*(A Case Study of First Bank of Nigeria Plc, and Oceanic Bank Plc,Abakaliki Branch

Offices). A Post Graduate thesis submitted to the Department of Accountancy, Faculty of Business Administration, University of Nigeria, Enugu Campus.

Ehimen, O. R. and Bola, A. 2010. Cyber - crimes in Nigeria. *Business Intelligent Journal*.January.Vol. 3, No. 95.

Godswill, E. 2002.*Causes of Frauds and Forgeries in Banking*. Cash and Tellers Refresher Course: Abuja Nigeria.

Hassan, A. B., Lass, F. D. and Makinde, J. 2012. Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology***.**VOL. 2, NO. 7. ISSN 2225 – 7217.

Kuna, M. and Willson, P. 2011. *Computer Crime and Computer Fraud*.Department of Technology and Criminal Justice. Maryland, USA.

Laura, A. 2011. "Cyber Crime and National Security: The Role of the Penal and Procedural Law.

Meke Eze Stanley, N. 2012. An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".

Ologun, S. O. 1994. Bank failures in Nigeria: Genesis, Effects and Remedies. *CBN Economic and Financial Review*.Vol. 32.No. 2. 312 – 322.

Omojunwa, T. 1999. "Fraud in the banking industry".*Oceanic view*. Vol. No. 33. May/June.Pp. 1- 2.

Ribadu, N. 2007.*Cyber Crime and Commercial Fraud: A Nigeria perspective*. A paper presented at the Congress to celebrate the 4th Annual section of UNCITRAL Vienna, Austria 9 - 12th July.

Saulawa, M. A. and Abubakar, M. K. 2014. Cyber Crime in Nigeria: An Overview of Cyber Crime Act 2013. *Journal of Law, Policy and Globalization*.ISSN 2224 – 3240 (Paper).ISSN 2224 – 3259 (Online).Vol. 32.www.iiste.org

www.automation computer, Oct.2004.

www.fd/c.nd.com may 2010.

www.info.ethicspoint.comaug.2010

www.infomationmanagement.journal.oct.2016

www.mpf.gov.ng

Zik, O, 2002. Contemporary Lapses in Cash and Teller Operations: Paper Presentation of Teller Course in Abuja, Nigeria, May 16