International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org/current.php?title=IJRFM
Vol. 8 Issue 9, September - 2018
ISSN(o): 2231-5985 | Impact Factor: 6.397

IMPACT OF ELECTRONIC BANKING ON DETECTION OF FRAUD IN NIGERIAN BANKING

C. Emefiele[1],

E. N. Obim[2],

S. E. Nkamare[3]

[1,2,3]Dept of Banking and Finance, Faculty of Management Sciences
University of Calabar, P. M. B. 1115, Calabar, Cross River State, Nigeria

Abstract
The study empirically examined the impact of electronic banking on detection of fraud in Nigeria banking system. The specific objectives were; to examine the Impact of ATM ,Internet, mobile and POS on Fraud Detection in Nigeria. Primary sources of data was used and it is comprised of questionnaire, interview and observation. Desk survey method was adopted in this study to gather relevant information.. Chi square statistical analysis was adopted in this study. Based on the analysis the following findings revealed thus; there was a significant impact between Automated teller machine and fraud detection of selected banks in Nigeria, there was a significant impact between Internet banking and fraud detection of selected banks in Nigeria, there was a significant impact between mobile banking and fraud detection of selected banks in Nigeria and there was a significant impact between Point of sales and fraud detection of selected banks in Nigeria. The following recommendations were made for the study;:Banks should organize seminars/workshops on the awareness of electronic banking to people in the rural area and customers who find it difficult to make use of their ATMs for transaction and also let them know the benefit that accrues from using electronic banking. Also it is recommended that customers should be protected from the internet hackers, tight security should be put in place to ensure that customers information are not easily available to information hackers.
Keyword ; ATM ,Internet, mobile , POS ,Fraud Detection

1.0 Introduction

The rapid advancement of global information infrastructure during the last four decades, including information technology and computer networks (Internet and telecommunications systems) has enabled the development of electronic banking at a global level, allowing business to effectively interact more with their customers and other corporations inside and outside their industries. The banking industry, like many business sectors, utilizes information and communication technology (ICT) to offer its customers value added services and convenience. Akinlola,(2008).Electronic banking is the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. It includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet

. Electronics banking facilitates an effective payment and accounting system thereby enhancing the speed of delivery of banking services.With the rapid globalization of the Nigeria economy, financial institutions faced increased competition in an ever changing environment. These banking and financial institutions adopted strategies aimed at developing competitive advantage based on enhanced customer value in terms of product differentiation, quality, speed, service and costs. Through technology developments, banking services have become available 24

x 7 through automatic teller machines (ATMs) and at online banking.Electronic banking services are the class of banking services that can be offered by a bank to individuals and companies through electronic means via a fixed or mobile telephone, and internet. However, more attention towards e-banking security is required and needed against fraudulent behavior because the lack of control over security makes e-banking still un-trusted for many till today. This study presents security issues related to e-banking and how e-banking can be used to detect fraud. It also highlights the characteristics and challenges of e-banking fraud; different types of attacks, some fraud detection strategies, and some prevention methods used by electronic banks. The introduction of electronic banking has come with its challenges. These range from technology adoption, financial limitations and technology acceptance of new systems. Other factors experienced globally are the increased security fears, limited internet access and enabling legislative framework. Security is the major factor in the adoption of electronic banking and this is rated as the most important issue of online banking services.Security is a factor that is constantly highlighted for the success of electronic banking. The inadequacy of security potentially leads to financial loss, punitive measures by regulators. In electronic banking, fraud is a major contributory factor to security and needs to be managed closely.

The banking public expects accountability, fairness, transparency and effective intermediation from banks. The banks are expected to ensure that they carry out their responsibilities with sincerity of purpose, devoid of fraudulent practices. This is sacrosanct if the banking sector is to gain public trust and goodwill. Fraud in the banking industry before recapitalization effort was at an alarming rate. It has caused the collapse of many banks. Many investors and depositors funds were trapped in these banks and indeed, many banks are still suffering as a result of these fraudulent activities. In fact it has prevented many banks from achieving their goals and many businesses have gone into liquidation as a result. Fraud has become a cankerworm that has eaten deep into the financial sector of the Nigerian economy and millions of Nigerian naira has been lost to fraudsters through these activities

1.1 Objectives of the study

The specific objectives are

i. to examine the impact of ATM on fraud detection in Nigerian banking
ii. to examine the impact of internet on fraud detection in Nigerian banking
iii. to examine the impact of mobile on fraud detection in Nigerian banking
iv. to examine the impact of POS on fraud detection in Nigerian banking

2.0 Review of Related Literature

2.1 Theoretical framework

The following theories are postulated on electronic banking.

2.1.1 Theory of Information Production and Contemporary Banking Theory

Diamond (1984) suggested that economic agents may find it worthwhile to produce information about possible investment opportunities if this information is not free; for instance surplus units could incur substantial search costs if they were to seek out borrowers directly. There would be duplication of information production costs if there were no banks as surplus units would incur considerable expenses in seeking out the relevant information before they commit funds to a borrower. Banks enjoy economies of scale and have expertise in processing information related to deficit units (borrowers). They may obtain information upon first contact with borrowers but in real sense it's more likely to be learned over time through repeated dealings with the borrower. As they develop this information they develop a credit rating and become experts in processing information. As a result they have an information advantage and depositors are willing to place funds with a bank knowing that this will be directed to the appropriate borrowers without the former having to incur information costs.

Bhattacharya and Thakor (1993) contemporary banking theory suggests that banks, together with other financial intermediaries are essential in the allocation of capital in the economy. This theory is centered on information asymmetry, an assumption that "different economic agents possess different pieces of information on relevant economic variables, in that agents will use this information for their own profit" (Freixas and Rochet 1988). Asymmetric information leads to adverse selection and moral hazard problems. Asymmetric information problem that occurs before the transaction occurs and is related to the lack of information about the lenders characteristics, is known as adverse selection. Moral hazard takes place after the transaction occurs and is related with incentives by the lenders to behave opportunistically.

2.1.2 Innovation Diffusion Theory

Is an innovation as any idea, object or practice that is perceived as new by members of the social system and defined the diffusion of innovation as the process by which the innovation is communicated through certain channels over time among members of social systems. Diffusion of innovation theory attempts to explain and describe the mechanisms of how new inventions in this case internet and mobile banking is adopted and becomes successful.

Rogers (1995) identified five critical attributes that greatly influence the rate of adoption. These include relative advantage, compatibility, complexity, triability and observability. According to Rogers, the rate of adoption of new innovations will depend on how an organization perceives its relative advantage, compatibility, triability, observability and complexity. If an organization in Kenya observes the benefits of mobile and internet banking they will adopt these innovations given other factors such as the availability of the required tools. Adoption of such innovations will be faster in organizations that have internet access and information technology departments than in organizations without.

2.2 Conceptual framework

According to Aragba-Akpore (1998) on the application of information technology in Nigerian banks , pointed out that IT is becoming the backbone of banks' services in Nigeria. He cited the Diamond Integrated Banking Services (DIBS) of the Diamond Bank Limited and electronic smart card accounts (ESCA) of All States Bank Limited as efforts geared towards creating sophistication in the banking sector. Ovia (2000) discovered that banking in Nigeria has increasingly depended on the deployment of information technology and that the IT budget for banking is by far larger than that of any other industry in Nigeria. He contended that the on-line system has facilitated internet banking in Nigeria as evidenced in some of them launching websites. He found also that banks now offer customers the flexibility of operating an account in any branch irrespective of which branch the account is domiciled.

Woherem (1997) discovered that since 1980s Nigerian banks have performed better in their investment profile and use of ICT systems, then the rest of the industrial sector of the economy. An analysis of the study carried out by African Development Consulting Group Ltd. (ADCG) on IT diffusion in Nigeria shows that banks have invested more on IT, have more IT personnel, more installed base for PCs, LANs, and WANs and have a better linkage to the internet than other sectors of the Nigerian economy. The study, however pointed out that whilst most of the banks in the west and other parts of the world have at least one PC per staff, Nigerian banks are lagging seriously behind, with only a PC per capita 0.18 (Woherem, 1997).

Gwashi and Alkali (1996) observe that ICT covers all forms of computer and communications equipment and software used to create, store, transmit, interpret, and manipulate information in its various formats e.g., business data, voice conversations, still images, motion pictures and multimedia presentations. It also refers to the electronic devices used to collect, process, store and disseminate information. Similarly, the deployment of ICT is skyrocketing with many organizations using it in office automation, i.e. word processing, electronic mail, telecommunicating and teleconferencing. Other areas of ICT application are as follows:

In business management, computerized database management system (DBMS) and management information system (MIS) are now making commerce and Industry pleasurable and ensuring decision making.

Acharya, (2008) examined the impact of web design features of a community bank's performance using a sample of 55 community banks with online services in the five midwestern states of the USA. The author utilized both primary and secondary data by applying multiple regression models. The results show that banks with higher usability of ICT perform significantly better than those with low ICT usability.

Berger, (2003) examined technological progress and its effects in the banking industry using data collected from the banking industry in the United States over the period 1967 to 2001. The author employed multiple regression model, and the findings revealed that improvements in costs of lending capacity due to improvements in "back – office" technologies, as well as consumer benefits from improved "front office" technologies suggests significant overall productivity increases in terms of improved quality and variety of banking services.

2.2.1 Frauds in Nigeria's banking industry

There are significant fall on the value of financial frauds recorded in 2012, Nigerians still lost about ₦2.25 billion to activities of fraudster during the year. The Nigerian interbank settlement system (NIBSS) disclosed that in 2014, fraudsters made ₦1, 461attempts to steal ₦7.8 billion, but succeeded in stealing₦6.2 billion in the year. This is even as the Central Bank of Nigeria (CBN) has called for more vigilance from banks and the customers. About ₦2.25 billion was stolen from Nigerian by fraudster last year. Between 2014 and 2015, the financial sector recorded 63.7 percent reduction in actual fraud losses. In addition, Automated Teller Machine (ATM) was more vulnerable to frauds in 2015 and would even be the most targeted platform in 2016. Fraud valued through ATM in 2015 was 5,133, valued at ₦355, 892, 201, 30; point of sales (POS) had 1,853 volume valued at ₦63,555, 467,48, internet banking volume was 727 valued at ₦263,995,257,70; web volume was 1,463 valued ₦173,472, 360,60; cheque in terms of volume had 40 valued at ₦167, 413,696, among others in 2013 and 2014, the internet banking, web and ATM transactions happened to be the top three channels mostly reported. However, he disclosed that in 2015 another dimension to fraud scheme was reported and it became obvious that card relatedtransactions are becoming safe haven for the fraudsters.

Although there is no single accepted definition of fraud (the legal practitioner, 2013), it relates to wrongful or criminal deception that results in financial or personal gains. Bank fraud is the use of deliberate misrepresentation (which usually requires some technical expertise) in order to fraudulently obtain money or other assets from a bank. The types of fraud that are commonly experienced by financing institution include sales fraud, purchase fraud, cheque payment fraud and automatic teller machine fraud (ATM) (Benjamin, 2011). Other strategies employed include collaborating with security agents and bank officials as well as local and international networking (Aransiola, 2011). Worryingly, results show that internal personal personnel have direct access to banking systems and access to customer's personal information and records. According to Sidden (2005), the majority of fraud is committed by employees who exploit breakdowns in organizations.

2.2.2 Types of online banking frauds

This seminar presents the types of online fraud that have economic impact either directly or indirectly on the financial system of a nation or having cross border ripple effects. Longe & Chiemeke (2008) simplified the list of unintended consequences of ICT to include acts such as Phishing, Trojan horse, malware, electronic spam mails, cyber-stalking, and fake copy -cat websites. While some types of cyber-crimes are specific to Nigeria, other types, such as identity theft and false statements, cut across all countries, which include the following: -

1. Phishing Attacks

Phishing, the act of stealing customer's information via the internet for the purpose of committing online banking fraud, has become a significant criminal activity on the Electronic banking services. Phishing basically involves the use of fake email messages from the Bank or different

individual pretending to be a Bank representative. Mostly, the email seeks customer to make available sensitive information such as name, password, account number etc. and provides links to a counterfeit web site, in which the tricks are the ones a customer follow the link and provide the requested information, intruders can have access to his/her personal account information and finances. While, in some cases popup windows can appear in front of a copy of a genuine bank web site. The real web site address is displayed; however, any information a customer typed directly into the popup will go to unauthorized users. Conversely, as banks are consistently coming up with different strategies to defeat fraudsters, so also the fraudsters are in constant developing their means to defraud customers. Today, Hi-tech fraudsters have developed a new ways of tricking online banking customers, such as Trojan horse and Vishing. (Banking,2008; Singh, 2007; Anderson, 2007; Howard, 2008 and Randazzo 2004). The fraudulent practice of sending emails or pop-up web pages purporting to be from legitimate companies in order to induce individuals to provide personal or sensitive business/account information e.g. credit card numbers, account information, PINs or passwords

2. Trojan Horse

This is an application in which the program insinuates itself into a user's computer via an email, whereby the program will automatically direct the user of the system to a website which is exactly similar to a Bank website, which built a sophisticated command and-control (C&C) system that completely automates the attacks. Trojan horse attacks can defeat sophisticated authentication schemes that security experts previously thought rock solid

3 Malware

Malware is the term for maliciously crafted software code. Special computer programs now exist that enable intruders to fool customers into believing that traditional security is protecting customers during online banking transactions (Micro 2012 and Singh 2007). Essentially, Malware performs one of the following.

a. Account Information Theft

Malware capture the keystrokes of login information such as special images or “magic words” whenever a person is trying to log into the Bank website. (Gill, 2011; Anderson 2007)

b. Fake Web Site Substitution

Malware generate web pages that appear to be legitimate but are not. They replace bank’s legitimate web site with a page that can look identical, except that the web address will vary in some way. Such a “man in the middle attack” site enables an attacker to intercept customer user information. The attacker adds additional fields to the copy of the web page opened in a customer's browser. When customers submit their information, it is sent to both the bank and the malicious attacker without the knowledge of the customers. (Banking, 2008).

c. Account Hijacking

Malware hijack the customer’s browser and transfer funds without the knowledge of the customers. Ones a customer attempt to login at a bank website, the software launches a hidden browser window on the customer computer, ones a customer successfully logs in to his bank, the software reads the customer’s account balance, and creates a secret fund transfer to the intruder-owned accounts..

d. Pharming

This technique is used in hijacking the web address of service provider. This occurs when a user types in a Web address and it redirects to a fraudulent Web site without your knowledge or consent. The website will look similar to the legitimate site with the intention of capturing your confidential information. Essentially, pharming attacks involve the installation of malicious code into customers’ computer; however, pharming can also take place without any conscious action on the customer’s part. The common type of pharming attack is when customers open an email, or an email attachment, that installs malicious code on the customer’s computer. Later on, the malicious code will delude the customer to log into a fake website that closely resembles a customer bank website. Any information the customers provide during a visit to the fake site is made available to malicious users.

e. Account takeover

This takes place when a person takes over another person's account, first by gathering personal information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for a mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement card to be sent. They may then set up a new PIN. They are then free to use the card until the rightful cardholder discovers the deception when he or she tries to use their own card and most times the account would have been drained.

f. Card-not-present fraud

An unauthorized use of card details over the phone or on the internet

g. Skimming

It is a fraudulent collection of payment card details using typically a small electronic device called skimmer. The device most times is affixed to an ATM or Point-of-Sale terminals and allows criminals to capture customer's card information including PIN. The advent of wireless technology has made it easier for criminals to remotely download stolen data without physically visiting the terminals.

h. Sim Swap fraud

This occurs when the phone number of a customer is hijacked through fraudulent Sim replacement at a Telco outlet/agent. The perpetrator then uses the mobile line to access the account of the victim usually via mobile banking or receives account sensitive details like PIN through PIN reset request. Ways to fight and fight e-Fraud Transaction security is a complex challenge that requires concerted efforts from all stakeholders in the payment space to be effectively dealt with. The counter-fraud story isn't all about direct financial loss. Shrinkage or loss due to shoplifting has long been in the budgets of high street retailers and just as in online, there is a balance to be had between securing stock and allowing customers the freedom to purchase.

2.2.3 Methods of perpetrating online fraud

According to Idowu (2009), fraud can be seen as the deliberate falsification, camouflage, or exclusion of the truth for the purpose of dishonesty/stage management to the financial damage of an individual or an organization. It is dishonesty or an act of cheating aimed at causing a person or business to give up possessions or some lawful right. The Association of Certified Fraud Examiners (1999) further defines fraud as the use of one's' profession for personal enhancement through the conscious misuse, misapplication or employment of organizational possessions or property. Fraud is any action by which one person intends to gain a deceitful advantage over another. In other words, fraud is an act of commission which is planned to cause unlawful gain to one person and criminal loss to the other, either by way of concealment of information or otherwise. There are various methods by which fraud can be perpetrated in the banks and other organizations. The list of methods is usually not exhaustive as new methods are devised with time. The most important and common methods are:

i. Advance Fee Fraud

This may involve an agent approaching a bank, a company or individual with another to access large funds at below market interest rates often for long term. This purported source of funds is not specifically identified as the only way to have access to it through the agent who must receive a commission "in advance". As soon as the agent collects the fee, he disappears and the facility never comes through. Any bank desperate for fund especially distressed banks and banks needing large funds to bid for foreign exchange can easily fall victim of this type of fraud. When the deal fails and the fees paid in advance are lost, these victims are not likely to report the losses to the police or to the authorities.

ii. ForgedCheques

This is by far the commonest method by which customers and banks are defrauded. They occur mainly in company accounts and are invariably perpetrated by staffs within the company who have access to the company's cheque book. It also involves the deceptive copying and use of customer's signature to draw huge sums of money from the customer's account without

previous permission of the customer. Such forgeries may be targeted at savings accounts, deposit accounts, current accounts or transfer instruments such as drafts. Experience has shown that most of such forgeries are perpetrated by internal staff or by outsiders who act in conspiracy with employees of the bank who usually are the ones who release the sample signatures being forged.

iii. Fund Diversion

In this case, bank staff sometimes diverts customers' deposits and loan repayment for personal use. Another case of this is the tapping of funds from interest in suspense accounts in banks.

iv. Cheque Kitting

This happens when a depositor utilizes the time required for a cheque to clear to obtain an authorized loan without interest charge. The goal of the chequekitter may be to use these uncollected bank funds' interest fees for a short time to overcome a temporary cash shortage or to withdraw the funds permanently for personal use. Competition among banks in the era of deregulation encourages bank to make funds available before collection of customers' cheque in order to attract special business accounts.

v. Account Opening Fraud

This involves the deposit and subsequent cashing of fraudulent cheques. It usually starts when a person not known to the bank asks to open a transaction account such as current and savings account with false identification but unknown to the bank.

vi. Counterfeit Securities

Counterfeiting of commercial financial instruments is one of the oldest forms of crime. Modern photographic and printing equipment has greatly aided criminals in reproducing good quality forged instruments. The documents may be total counterfeit or may be genuine documents that are copied, forged or altered as to amount, payout date, pay or terms of payment. A common fraud is to present the counterfeit stocks or bonds as collateral for loan. The presenter would draw out the proceeds and disappear before the financial instruments are found to be counterfeit.

vii. Money Transfer Fraud

Money transfer services are means of moving to or from a bank to beneficiary account at any bank point worldwide in accordance with the instructions from the banks' customers. Some common means of money transfer are mail, telephone, over-the-counter, electronic process and telex. Fraudulent money transfer may result from a request created solely for the purpose of committing a fraud or altered by changing the beneficiary's name or account number or changing the amount of the transfer.

viii. Letter of Credit Fraud

This generally arises out of international trade and commerce. They stimulate trade across national borders providing a vehicle for ensuring prompt payment by financially sound institutions. Overseas suppliers continue to receive spurious letters of credit, which are usually accompanied by spurious bank drafts with fake endorsements which guarantee payments

ix. Computer Fraud

Computer Frauds involves the deceptive manipulation of the banks' computer, either at the data collection stage, the input processing stage or even the data dissemination stage. Computer frauds could also occur due to improper input system, virus, program manipulations, transaction manipulations and cyber thefts. It can also take the form of corruption of the program or application packages and even breaking into the system through remote sensors. A banks' data can also be tampered with at the data center to gain access to unauthorized areas or even give credit to accounts for which the funds were not originally intended. This kind of fraud can remain undetected for a long time. In this epoch of enormous deployment of automated teller machines (ATMs) and online real time e-banking and commerce; computer frauds arising from cyber thefts and crimes has assumed a very threatening dimension. No bank seems to be invulnerable to it, and a considerable percentage of the enormous amount of money spent annually in the banking sector to help reduce fraud usually are channeled towards fighting computer frauds and cyber-crimes and theft

x. Clearing Fraud

Most clearing frauds hinge on suppression of an instrument so that at the expiration of the clearing period application to the instrument, the collecting bank will give value as though the paying bank had confirmed the instrument good for payment. Clearing cheques can also be substituted to enable the fraudster divert the fund to a wrong beneficiary. Misrouting of clearing cheques can also assist fraudsters to complete a clearing fraud.

xi. Fraudulent loans

One way to remove money from a bank is to take out a loan, a practice bankers would be more than willing to encourage if they know that the money will be repaid in full with interest. A fraudulent loan, however, is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; the "borrower" then declares bankruptcy or vanishes and the money is gone. The borrower may even be a non-existent entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank. This can also be seen as a component within mortgage fraud

xii. Forged or fraudulent documents

Forged documents are often used to conceal other thefts; banks tend to count their money meticulously so every pesewa must be accounted for. A document claiming that a sum of money has been borrowed as a loan, withdrawn by an individual depositor or transferred or invested can therefore be valuable to a thief who wishes to conceal the minor detail that the bank's money has in fact been stolen and is now gone.

xiii. Unofficial Borrowing

This occurs when bank employees borrow from the vaults and teller tills off the record. Such unauthorized borrowings are done in exchange of the staff post-dated cheque or I.O.U or even nothing. These borrowings are more rampant on weekends and during the end of the month when salaries have not been paid. Some of the unauthorized borrowings from the vault, which could run into thousands of naira, are used for fast businesses lasting a few hours or days after which the resources are replaced without any substantiation in place that they were taken in the first place. Such a practice when done recurrently and with no official records, soon very easily becomes prone to manipulations, whereby they resort to other means of balancing the cash in the bank's vault without ever having to replace the sums of money collected.

xiv. Voucher Manipulation

Manipulation of Vouchers involves the replacement or alteration of entries of one account to another account being used to commit the fraud. This account would obviously be a fabricated account into which the funds of unsuspecting clients of the banks are transferred. The amounts taken are usually in small amounts so that it will not easily be noticed by top management or other unsuspicious staff of the bank. Manipulation of vouchers can thrive in a banking system saddled with inadequate checks and balances such as poor job segregation and lack of detailed daily examination of vouchers and all bank records.

2.2.4 Causes of bank fraud

There are two main sources of frauds in banks and these are the internal and the external. Though distinguishable in theory, these sources are very often inseparable in practice. That is to say, a successful fraud often takes place and succeeds as a result of the collaboration, intentional or unintentional (i.e. due to carelessness or error of judgment, of an insider, a bank employee or member of staff).Indeed it was recently affirmed that" the public believes and rightly too, that most frauds in banks are the active connivance of bank staff. Otherwise how does anybody explain for example, how a cheque drawn in favor of a named payee is paid into a different account and the funds withdrawn? Or how does one explain how a completely different institution or individual collects a draft prepared in the name of another institution or individual? This is not an exception of the rule, it is frequent occurrence" The causes of bank fraud can be classified into two namely institutional factors, lapses or inadequacies and environmental/societal factors or lapses,

Institutional Factors

According to Nwaze (2008), the institutional factors or causes are those that can be traced o the internal environment of an organization. They are to a great extent factors within the control of the management of the bank. Major institutional causes of fraud can be categorized as follows:

i. Poor Management

This comes in a form of inadequate supervision. A junior staff with fraudulent tendencies that is not adequately supervised would get the impression that the environment is safe for the perpetration of fraud. Poor management would also manifest in ineffective policies and procedures, which a fraudulent minded operator in the system will capitalize on. Even where there are effective policies and procedures in place, fraud could still occur with sometimes deliberate skipping of these tested policies and procedures.

ii. Inexperienced Personnel

Inexperienced personnel are susceptible to committing unintentional fraud by falling for numerous tricks of fraudsters. Inexperienced personnel are unlikely to notice any fraud attempts and take necessary precautionary measures to checkmate the fraudster or set the detection process in motion.

iii. Overstretching

Overstretching is another reflection of poor management. This can aid perpetration of fraud to a large extent. A staffwho is overstretched is not likely to perform at optimum level of efficiency.

iv. Job rotation

Ordinarily, the longer a man stays on a job, the more proficient he is likely to be. An operator who has spent so long on a particular job may be encouraged to think that no one else can uncover his fraud. The existence of this kind of situation in a bank is clear evidence of poor management and such situations encourage fraudulent practices.

v. Poor remuneration

Poor salaries and poor conditions of service can also cause and encourage fraud. Employees that are poorly paid are often tempted to fraudulently convert some of the employers' monies to their own use in order to meet their personal and social needs. This temptation is even stronger on bank employees who on daily basis have to deal with cash and near cash instruments. In our society, it is argued that greed rather than poor working conditions or poor salaries is what lures most people into fraudulent acts. This explains why fraud would still exist in the banking sector, which is reputed to be one of the highest paying sectors. Some people have an insatiable appetite to accumulate wealth and would therefore steal irrespective of how good their earnings are.

vi. Frustration

Frustration could also lead to fraud. Where a staff feels short-changed in terms of promotion and other financial rewards, they become frustrated and such frustration could lead to fraud as such employee would attempt to compensate himself in his own way.

vii. Inadequate Training and Re-Training

Lack of adequate training and retraining of human resources both on the practical and theoretical aspects of banking activities and operations more often than not leads to poor performance. Such inefficient performance creates a loophole which can very easily be exploited by fraudsters.

viii. Poor Book-keeping

Inability to maintain appropriate books of accounts together with failure to reconcile the various accounts of the bank on daily, weekly or monthly basis more often than not will attract fraud. This

loophole can very easily be exploited by bank staff that is fraudulent. The prevalence of fraud and forgeries are an indication of weakness in a bank's internal control systems. Aside the above-mentioned causes of fraud, the following factors greatly contribute to fraud:

1. Inadequate compensation, salaries and fringe benefits which are accruable to bank staff
2. Refusal to comply with laid-down procedures without any penalty or sanction;
3. Conspiracy between interacting agents charged with the responsibility of protecting the assets and other interest of the bank;
4. Poor working conditions;
5. Poverty and infidelity of employees.

2.2.5 Effects of online bank fraud

According to Reuter's media briefs from Cameroon, British prime minister, cyber-crime costs the British economy some 27 billion pounds a year. On the other hand, the Economic and Financial Crimes Commission Report ranks Nigeria as third among the top ten sources of cyber-fraud in the world. It is estimated that after the United States with 65 per cent of cyber-criminal activities and the United Kingdom with 9.9 per cent, Nigeria is the next hub of cyber criminals in the world with 8 per cent. The growth of online banking further presents enhanced opportunities for perpetrators of cyber-fraud. Funds can be embezzled using wire transfer or account takeover. Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online banking payment systems. Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions.
Therefore unless crime detection and prevention are confronted collectively, Nigeria like any other country will remain warm breeding grounds for cartels of such criminal activity. A global effort to combat this crime is of essence. Financial fraud is one of America's largest growth industries, creating annual losses of $189 billion. The cost of application fraud alone, they argued, is more than $35 billion a year.

This is by far more damaging than delinquent or bankrupt accounts, fraud losses which are generally three times higher than normal charge- off rates. This situation poses a real and constant threat to profitability and may raise the price of goods and services for consumers. They further argued that by far, the greatest threats is from e- commerce fraud, identity theft and international criminal organizations, all of which are becoming more widespread and sophisticated every day.

As e-commerce continues to grow, it will become an even bigger attraction for criminals. The report indicated that identity theft is escalating at 40% a year and is particularly problematic compared with more traditional forms of financial fraud. Greater access to credit, an abundance of information, faster electronic communications, and intense competition among financial institutions make it easier than ever for perpetrators to steal identities and falsify information. The existence of cyber-fraud and its effects require the formulation of appropriate policies to address them. The next section presents existing policies on cyber- related crime in Nigeria.

2.2.6 Loss of Public Confidence in Banks

Fraud is perhaps the most fatal of all the risks confronting banks. The enormity of bank frauds in Nigeria can be inferred from its value, volume and actual loss. A good number of banks' frauds never get reported to the appropriate authorities, rather they are suppressed partly because of the personalities involved or because of concern over the negative image effect that disclosure may cause if information is leaked to the banking public The banks' customers may lose confidence in the bank and this could cause asset back in the growth of the bank in particular.

Loss of Money

Fraud leads to loss of money, which belong to either the bank or customers. Such losses may be absorbed by the profits for the affected trading period and this consequently reduces the amount

of profit, which would have been available for distribution to shareholders. Losses from fraud which are absorbed to equity capital of the bank impairs the bank's financial health and constraints its ability to extend loans and advances for profitable operations. In extreme cases rampant and large incidents of fraud could lead to a bank's failure.

Increased Operating Cost

Fraud can increase the operating cost of a bank because of the added cost of installing the necessary machinery for its prevention, detection and protection of assets. Moreover, devoting valuable time to safeguarding its asset from fraudulent men distracts management. Overall, this unproductive diversion of resources always reduces outputs and low profits which in turn could retard the growth of the bank.

Low Asset Quality

It also leads to a diminishing effect on the asset quality of banks. The problem is more dangerous when compounded by insider loan abuses. Indeed, the first generation of liquidated banks (Co-operative Bank) was largely a consequence of frauds perpetrated through insider loan abuses. If this problem is not adequately handled, it could lead to distress and bank failures.

Control of online banking frauds

In view of the gravity of fraud in banks, the management of various banks has employed different measures, such as establishment of internal control unit, fraud alerts, security measures etc. Yet fraud has continued in an upward trend, and this has called the effectiveness of these measures into question.. Though details may differ from one bank to another, it all depends on size, location and general environment nationally and internationally.

Fraud Identification

Every bank is to be aware of and identify the types of frauds prevalent in the society, including the international society, the causes and modalities of the frauds and the potentials and prospects of some of them occurring in the bank. This will be a function of volume, types and concentration of the banks' operations and the management control systems. There are the internal and external management controls. Internal management controls are carried out on the inside of the company while external controls are carried out on the outside. Internal management control is classified into two major groups: Internal Checks and Internal Audit.

i. Internal Checks

Internal checks are the operational controls, which are built into the banking system to simplify the processing of entries in order to secure prompt services, to help in minimizing clerical errors and to act as insurance against collusion.

ii. Internal Audit

Internal Audit on the other hand involves the review of operations and records undertaken within a business by specifically assigned staff, which is usually the Internal Auditor. There are people called external auditors too who examine the books of the bank to determine its truth and fairness. This kind of audit is mostly statutory in nature, which is called for by the law.

2.2.7 Fraud Prevention and Detection

The process of identification of frauds will enable the bank to access its susceptibility and identify which types it has to address particularly. Having done so, the next stage would be to evolve measures to prevent the occurrence of such frauds. The existing control systems can be classified into two, those aimed at prevention and those aimed at detection.

The CBN as the supervisor and regulator of the banking systems is interested in ensuring that banks put in place comprehensive and effective internal control systems to minimize the incidence of frauds and whenever they occur to ensure that they are detected. From the point of view of supervisors, a good internal control system must have the following attributes:

1. Dual control

2. Segregation and rotation of duties,
3. An effective and independent inspection functions
4. Clearly defined levels of authority and responsibility
5. Existence of an efficient Audit Committee
6. Adequate fidelity insurance cover

It is also the responsibility of the supervisor to determine banks' compliance with rules And bureaus to monitor fraudulent customers and accomplices The supervisors are also to cooperate with the external auditors of banks to ensure that the internal audit program of banks is comprehensive, adequate and effectively executed. The supervisors should also conduct an in-depth investigation into activities of a bank when put on enquiry. In order to enhance the ability of supervisors to carry out their responsibility effectively, they must be adequately trained and equipped with modern tools for supervision.

2.2.8 Cyber-fraud policy in Nigeria

There is presently no law that is specific to cyber-fraud in Nigeria. However, this is not to say that cyber criminals are free to operate in the country. There are general laws that are not specifically related to cyber-fraud but are being enforced to deal with the crime. Some of these laws are: the Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006.
The Nigeria Criminal Code Act 1990 The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber-fraud is not mentioned in the Act, it is a type of stealing punishable under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with "obtaining Property by false pretenses- Cheating." The specific provisions relating to cyber-fraud is section 419, while section 418 gave a definition of what constitutes an offence under the Act.

3.0 Research methods

This study is a survey research. A survey research can be defined as the investigation of the behaviour, opinion or other manifestation of a group of people by questioning them. Here, individuals are the unit of analysis as they constitute the respondents in questions. In this case, the questionnaire carries close ended questions; this is not to limit the respondents from expressing themselves as much as they would want to in their choice of words but this is calculated to give the respondents a structured pattern, to answer the questions while providing answers that are easier to interpret and tabulated. The study area is Calabar metropolis. This area comprises Calabar municipality and Calabar South; this has to do with the following banks such as First Bank of Nigeria Plc, Ecobank of Nigeria of Plcand First City Monument Bank.

Population refers to the total number of customers in the listed banks. The population of this study comprises four thousand five hundred customers (4500) in the three(3) selected banks residing in Calabar, Nigeria .This constitutes the target population. This study used random sampling where customers were chosen from each of the bank, a total of two hundred Primary sources and secondary are used in this study. Primary sources of data comprises of questionnaire, interview and observation while secondary comprises of textbooks, journals etc. Desk survey method is adopted in this study to gather relevant information .The instrument that will be used for the study is questionnaire. This will be prepared by the researcher. Part A of the instrument will be meant to collecting of personal and demographic information of the respondents while section B of the questionnaire contains items that are derived from the hypotheses of the study. The requirement is for the respondents to read and tick using Likert scale. The instrument will involve pre test and test of the instrument. Data analysis is carried out through statistical process: Chi square statistical tool was adopted in this study

4.0 Findings

The major findings of the study include; there is a significant relationship between Automated Teller machine and fraud detection of selected banks in Nigeria, there is a significant relationship between Internet banking and fraud detection of selected banks in Nigeria, there is a significant relationship between mobile banking and fraud detection of selected banks in Nigeria, there is a significant relationship between Point of sales and fraud detection of selected banks in Nigeria.

5.0 Conclusion/Recommendations

The study empirically examined the impact of electronic banking on detection of fraud in Nigerian banks. Electronic banking is the conduct of banking business electronically which involved the use of information communication technology to drive banking business for immediate and future goals. The success of e-banking is contingent upon reliable and adequate data communication infrastructure. It is concluded that ATM, Internet, Mobile and POS have a significant relationship on the performance of deposit money banks in Nigeria.

The following recommendations were made for the study:

1) Bank should organize seminars/workshops on the awareness of electronic banking to people in the rural area and customers who find it difficult to make use of their ATMs for transaction and also let them know the benefit that accrues from using electronic banking.
2) Customers are the main reasons why banks are going concern, therefore, this customer should be protected from the internet hackers, tight security should be put in place to ensure that customers information are not easily available to information hackers.
3) Mobile banking services should be made accessible and easier to use to improve it popularity
4) The regulatory authorities should enforce new standings and policy on the charges of electronic transaction and should be able to provide adequate security both physically and electronically to check the incidence of hacking fraudsters

REFERENCES

Akinlola, S. (2008) "The adoption of e-banking: The Case of Omani Banks" *International Review of Business Research* 4(5), 120-128

Diamond, M. J. (1984), "Do European Primarily Internet Banks Show Scale and Experience Efficiencies?" European Financial Management (forthcoming).

Bhattacharya, J., Thakor, I., (1993). Do European primarily internet banks show scale and experience efficiencies? European Financial Management, 13(4), 643-671.

Freixas, I. and Rochert, M.J. (1985) "Is the internet delivery Channel Changing Banks' Performance? The Case of Spanish Banks" Banco de Espana Working Paper Series, Madrid 1(2), 624- 630.

Aragba-Akpore, Y. K. (1998). The Quality of internet banking services encounter in Jordan. *Journal of Internet Banking and Commerce,* 13(3), 1-8.

Woherem, F.O. (1997), "Valedictory Lecture" B & F Publications, Enugu September, 2005.

Gwashi, C., Alkali, E.. (1996) *The impact of Internet Banking on bank profitability*- the case Turkey" Oxford & Economics Conference programme June 22-24

Ovia J. (2001) Internet Banking: practice and Potentials in Nigeria. Paper Delivered at a Workshop organized by ICAN at Lagos,

Acharya, E.M. (2008), *Diffusion of Innovation* (4th Ed).New York,;The Free Press

Berger, P. S. (2003). *Commercial Bank Management*; (5th Edi) London; McGraw-Hill Irwin

Benjamin, M. (2011). The impact of internet banking on performance and risk profile: Evidence from Australian credit unions. *Journal of Banking Regulation,* 6(2), 163-174.

Aransiola, A.Z. (2006) "Role of the Banking Services on the Profits of Jordanian Banks" *American Journal of Applied Science* 3(9), 60-67.

Sidden, J. (2005) "The Impact of the Internet in Banking: Observations and Evidence from Developed and Emerging Markets" Telematics and Informatics, 19, pp315-330

Longe, R. J., Chieneke, K (2008) "How Has the Adoption of Internet banking Affected Performance and Risk of Banks? A look at Internet Banking in the 10th Federal Reserve District"FRB Financial Industry Perspectives 1-16

Banking J., W. (2008) "E-banking in the RuralArea- Recent Trend and Development" communication of the HMA

Singh, S. (2007) "The adoption of e-banking: The Case of Omani Banks" *International Review of Business Research* 4(5), 120-128

Anderson S.A. (2007)"The Impact of Electronic Banking on the Performance of Jordanian Bank "*Journal of Internet Banking and Commerce* 2(1),16- 20.

Howad, U. M. (2008). Domestic electronic payment in Nigeria: The Challenges. *Central Bank of Nigeria Bulleti*n, 29(1), 80-90.

Randazzo, J. (2004), "Don't Open an Account, If It isn't an E-Bank" (httpwww.jida.com) retrieved 9th September, 2008.

Nwaze, M. J. (2008), "Do European Primarily Internet Banks Show Scale and Experience Efficiencies?" Working Paper No. 0412, Banco de Espana, Madrid.

Idowa M.J. (2009) "Is the internet delivery Channel Changing Banks' Performance? The Case of Spanish Banks" Banco de Espana Working Paper Series, Madrid 1(2), 624- 630.

Micro, Y. K. (2012. The Quality of internet banking services encounter in Jordan. *Journal of Internet Banking and Commerce,* 13(3), 1-8.

Gill, J.D (2011). Intermediate Accounting,South-Western College Publishing, Ohio.