e-ISSN : 2347 - 9671, p- ISSN : 2349 - 0187
EPRA International Journal of Economic and Business Review | Vol - 3, Issue- 12, December 2015
Inno Space (SJIF) Impact Factor : 4.618(Morocco) ISI Impact Factor : 1.259 (Dubai, UAE)

FINANCIAL INNOVATION AND FRAUD RISKS IN DEPOSIT MONEY BANKS OF NIGERIA

✍

Akinyele Akinwumi Idowu[1]
[1]Department of Economics, Accounting and Finance. Jomo Kenyatta University of Agriculture and Technology, Juja Main Campus, Kenya

Dr. Willy Muturi[2]
[2]Department of Economics, Accounting and Finance. Jomo Kenyatta University of Agriculture and Technology, Juja Main Campus, Kenya

Dr. Patrick Ngumi[3]
[3]Institute of Certified Public Accountants Kenya

ABSTRACT

The Nigerian banking landscape continues to face significant headwinds on its bottomline, topline and costs. The greatest opportunity to grow revenue will not come from just new markets or products but rather from the ability to deliver a high quality and differentiated customer experience. Convenience and consistency in service quality were the resounding themes across the segments. Corporate and personal customers are increasingly looking for a clear demonstration of value in product features. They expect a commensurate reflection on pricing, devoid of fraud risk and that does not compromise security. Information technology is considered as the key driver for the changes taking place around the world. Electronic banking is the latest and most innovative service offered by the banks. The transformation from the traditional banking to e-banking has been a 'leap' change. The evolution of e-banking started from the use of Automatic Teller Machines (ATMs) and telephone banking (tele-banking), direct bill payment, electronic fund transfer and the revolutionary online banking. Technological development, revolutionize the banking industry. Financial innovation is a vital strategy for banks and financial institutions to keep customers engaged and remain competitive. The imperative of Nigeria becoming cashless with the goal of minimizing cash transaction and economic dangers associated with it and the necessity of poverty eradication through financial empowerment have sparked off innovations from the Central Bank of Nigeria (CBN), the telecommunications companies (telcos), the Nigeria Deposit Insurance Corporation (NDIC) and other stakeholders, ranging from Mobile Money System to online banking and e-wallets. However, challenges propping up with the various innovations, operators and regulators admit, are overwhelming. As technology explodes, so also does the sophistication of frauds, for as banks rely more on technologies, they increasingly have to make huge amounts of sensitive personal data readily available to customers, clients, vendors and employees through various platforms with risks of compromise via mobile apps and cloud servers. Tackling the challenges and achieving the financial inclusion were the main issues for financial innovation adoption and growth. This study examines the consumer's perspective on financial innovation adoption, how fraud impact on customer's decisions to adopt financial innovation, the rate of cybercrime (fraud) and its sophistication. It will add to the existing literature in a changing bank marketing environment.

INDEX TERMS—*Financial innovation, cybercrime, fraud, information and communication technology (ICT),*

INTRODUCTION

Globally fraud is on the rise as well as its sophistication. In Nigeria, over the years most of these incidents have gone unreported. However, in 2013 under the directive of the CBN (Central Bank of Nigeria), NIBSS (Nigeria Interbank Settlement System Plc) developed the Anti-Fraud Portal with a view of getting the Banks to report their e-payment frauds as it occurs, in which, the InfoSec (Information System Security) department of NIBSS shows the analysis of the reported frauds to detect and show the trends of e-payment frauds in Nigeria. The report is focused on informing and helping the public understand payment fraud issues. The aggregated data also inform consumers and businesses on how fraud occurs using various channels, as well as aid financial institutions with more effective fraud trend monitoring and preventive measures to combat the fraud.

The term 'Fraud' has been defined in different ways by different scholars and authors. According to the Collins English Dictionary, fraud can be defined as: "deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage". Also, the Association of Certified Fraud Examiners defines fraud as "any illegal acts characterized by deceit, concealment or violation of trust. These acts are not dependent on the application of threat of violence or of physical force". Frauds are perpetrated by individuals and organizations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage. Awe (2005) defines fraud as the intentional alteration of records accompanied by the defalcation of asset in order to deceive certain group of people for the benefit of the perpetrator. Although not all frauds are accompanied by the defalcation of asset but majority of frauds perpetrated by low and middle officers normally involve the defalcation of asset.

According to the American Heritage Dictionary, (Second College Edition), fraud is defined as "a deception deliberately practiced in order to secure unfair or unlawful gain". In a nutshell, "Fraud always involves one or more persons who, with intent, act secretly to deprive another of something of value, for their own enrichment" (Davia et al., 2000). Wells, (2005) also stresses deception as the linchpin to fraud.

Defrauding people of money is presumably the most common type of fraud. Bank fraud on the other hand, is the use of fraudulent means to obtain money, assets, or other property owned or held by a financial institution (Glaessner and Mass, 1995). Bank fraud is a crime that has been around for as long as banks have been in operation. Anytime there is a large amount of money floating around, there will be people trying to figure out ways of getting it.

Apoorva and Juhi , (2007) defined bank fraud as a deliberate act of omission or commission by any person carried out in the course of banking transactions or in the books of accounts, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank. They concluded that bank frauds are the failure of the banker and mentioned the major elements responsible for the commission of frauds in banks; active involvement of the staff-both supervisor and clerical either independent of external elements or in connivance with outsiders, failure on the part of the bank staff to follow meticulously laid down instructions and guidelines and external elements perpetuating frauds on banks by forgeries or manipulations of cheques, drafts and other instruments. There has been a growing collusion between business, top banks executives, civil servants and politicians in power to defraud the banks, by getting the rules bent, regulations flouted and banking norms thrown to the winds.

Fraud can be committed through many methods, including mail, wire, phone, and the internet (computer crime and internet fraud). The difficulty of checking identity and legitimacy online, the ease with which hackers can divert browsers to dishonest sites and steal credit card details, the international dimensions of the web and the ease with which users can hide their location, all contribute to making internet fraud the fastest growing area of fraud. Estimates are that just twenty percent of frauds are exposed and made public. The remaining frauds are either undetected or discovered and not made public because of reputation risk (Bartlett and Ballantine, 2002).

Oseni (2006) opined that the incessant frauds in the banking industry are getting to a level at which many stakeholders in the industry are losing their trust and confidence in the industry. Corroborating the views, Oseni and Idolo (2010), stressed that the spate of fraud in Nigerian banking sector has lately become a source of embarrassment to the nation as apparent in the seeming attempts of the law enforcement agencies to successfully track down culprits. Fraud is the number one enemy of the business world (Nwankwo, 1991). The fear is now widespread that the increasing wave of fraud in the recent years, if not prevented might pose certain threats to economy and political stability and the survival of financial institution and the performance of the industry as a whole.

Nweze (2008) grouped the major causes of bank fraud into two: Institutional factors and Environmental factors:

Institutional factors or causes are those that can be traced to internal environment of the financial institution. They are as follows;

1)Inadequate Infrastructure: Poor communication systems and power failure result to ATM bank fraud which encourages the perpetration of fraud in banks.

2) Nature of Service: Fraud may be caused where documents of value and liquid assets are exposed to an undisciplined staff or unauthorized person(s) like customer(s) in the bank.

3) Poor Management: This comes in 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 especially ATM.

4) Poor Security Arrangement: Banks security arrangement for valuable documents are weak, poor and vulnerable, it is easy for fraudsters to have their ways undirected in the bank.

5) Poor Salaries: Employees that are poorly paid are often tempted to fraudulently convent some of the customer's monies to their own use in order to meet their personal and social needs. This temptation is stronger on bank employees who are on daily basis have to deal with cash and near cash instruments.

6) Frustration: This is a place where a staff feels short-changes in terms of promotion and other financial reward, they became frustrated and such frustration could lead to fraud as much as such employee would attempt to compensate himself in his own way and it is an indication of weakness in bank internal control system.

Environmental Factors: These are those factors that can be traced to the banks immediate and remote environment (Nweze, 2008).

1) Unemployment and High level of Poverty in Nigeria: Nigeria is one of the richest economics in sub-Sharan African and indeed the world both in human and natural resources (Oil), but 80% of the Nigeria youths especially university graduates are unemployed. Most of the politicians squirt away the looted funds in foreign banks without been punished by the EFCC. This causes unemployment and lack of infrastructure which is not good for a developing country like ours. Because of over stayed after graduation, directly or indirectly, some Nigeria youths especially those that find themselves in the banking industry with criminal intent engage in one bank fraud or the other with the aim of eradicating poverty.

2) Fear of Negative Publicity: Many financial institutions fail to report fraud cases to the appropriate authorities. They believed that doing so will give unnecessary negative publicity about the bank and it is a chance for fraudsters to thrive because it is a great challenge to a researcher as regards to data collection.

3) Societal Value: When the possession of wealth determines the reputation ascribed to a person, that society is bound to witness unnecessary competition for acquisition of wealth. The desire to be with the high and mighty calibre of the society, extreme want that is often characterized by need and cultivation of a life too expensive for the legitimate income of the individual which to a large extent encourages bank fraud.

Fraud in the Nigerian payments system and also on a global scale has been on the increase over the past few years as technological advances impact on the way we pay. Internet banking, the ever increasing use of the ATMs and other electronic platforms has one way or the other accelerated the growth of fraudulent activities. Cheques and over-the-counter fraud has given more room to a sophisticated and more concise electronic type of fraud. In Nigeria, Internet banking and ATM scored as the lead channels for perpetuating e-fraud in 2014. Internet banking and ATM scored as the lead channels for perpetuating fraud in 2014 as it recorded the highest value lost to fraudulent activities (NIBSS, 2014).

TECHNOLOGY ADVANCEMENT AND BANKING FRAUD

The banking industry has witnessed tremendous changes linked with the developments in ICT over the years. The ICT infrastructure used in banks includes internet access, internal networks, which facilitate automated payment systems otherwise known as financial (technology innovation) e.g. Automated Teller Machine (ATM), Real Time Gross Settlement (RTGS), Electronic Funds Transfer and cheque truncation. Internet access is a precondition for e-Business as it is the main channel for e-banking. The general availability of Internet allows for the analysis of overall ICT-readiness in the Banking Industry. Products that rely on the internet include both internet and mobile banking.

The application of networks is also vital part of an effective ICT-enabled system, which is especially true in the case of banks with a branch network, to enable banks to conduct ebanking at a substantial level. Wire-based and Wire-less technology (Internet facilities) are new technology in the Banking Industry, used to permit banks and their customers to access network resources from nearly any convenient location for financial transactions. Instant notification of transactions made is another innovation brought by ICT through the use of smart phone in conjunction with the internet facility in the Banking Industry. There has also been the digitalization of formerly paper-based processes. All these facilitate financial innovations through; ATMs, Debit and Credit cards, EFT, POS, RTGS, MB and IB (Ngumi, 2013; Idowu, 2006; 2012).

The security issue which is the basis of ICT related fraud is of special concern in the Banking Industry, as banking is highly based on trust from its customers. The risk of hackers, denial of service attacks, technological failures, breach of privacy of customer information, and opportunities for fraud created by the anonymity of the parties to electronic transactions can be managed by enhancing security of information. Depending upon its nature and scope, a breach in security can seriously damage public confidence in the stability of a financial institution or of a nation's entire banking system. (Agboola, 2001).

Scholars have different opinions on technological innovation and fraud. Kariuki, (2005) agreed that technological advancement has positive impacts on the banking performance in commercial banks in Kenya. However, Apoorva and Juhi, (2007) were of the opinion that the losses sustained by banks as a result of frauds exceed the losses due to robbery, burglary and theft-all put together. Such fraud is perpetrated by employees within the bank, outsiders or even both employees and outsiders in collusion (Olaoye and Dada, 2014).

STATEMENT OF THE PROBLEM

Bank fraud has being since the advent of the banking industry. But recently its growth and has been facilitated by the technological innovations and the widespread use of the Internet. The main driver of financial innovations in banks is adoption of ICT. It enables banks to develop sophisticated products, implement reliable techniques for control of risks and to reach geographically distant and diversified markets. On the other hand, a pre-condition for ICT adoption is proper risk management including fraud risk. The risk management framework cannot fully address the risk of fraud because it involves collusion between several parties. As technology advances fraudsters have also become technologically savvy. Banks are rapidly adopting the Real Time Gross Settlement (RTGS) which processes very large amounts on a real time and gross basis. This may be a challenge because fraud on such transactions is noticed after it has occurred.

OBJECTIVE OF THE STUDY

The objective of the research was to examine the relationship between financial innovation and fraud risks in Deposit Money Banks in Nigeria, with a view to determining the degree of association between fraud and financial innovation adoption. This will help to uncover the significance or impact of fraud risk on financial technology adoption. It is a recognized fact that average transaction in Nigeria is cash based. This is no longer acceptable in this information age of growing commerce. Whatever it is that is making customers keep money at home or with the informal financial sector must be uncovered, determined and rectified such that banks can boost the embracement and adoption of financial innovation and grow their deposit base in the interest of the general economy

SIGNIFICANCE OF THE STUDY

The study will open up and increase the knowledge in the area of bank fraud. It is an important topic because it will help the banking sector to realize that the technological advancement in the country calls for advancement in fraud control and detection skills especially in banks. As technology innovation has increased fraud level in banks, hence the need to invest more in detecting and deterring it instead of trying to suppress the number of fraud and theft-related cases.

REVIEW OF THEORETICAL FRAMEWORK

Three theories have been reviewed to help understand both financial innovation and fraud .These theories are the theory of the fraud triangle, diamond fraud theory and the theory of reasoned actions.

The theories of Diamond and the Fraud triangle:-

Fraud is one of inherent risks in banking often perpetuated by customers, staff, external people even management staff. Fraud in bank could be internal or externally carried out or by collaboration of both forces. Event has proved that some factors aid perpetuation of fraud, especially in this information age. The facelessness, boundarilessness, knowledge driven and no wavelength policing characteristics of technology made it subsceptible to fraudulent practices. An American criminologist named Cressey Donald in 1950s developed the Fraud Triangle Theory Model where he explained that in most incidences of fraud some common three factors are always present: perceived financial need (greed- motivation), perceived opportunity and rationalization/justification. There is also the Diamond theory proposed by David Wollfe and Dana Hermanson that added fourth dimension to fraud, this is capability factor (Wolfe and Hermanson, 2004). See figure 1

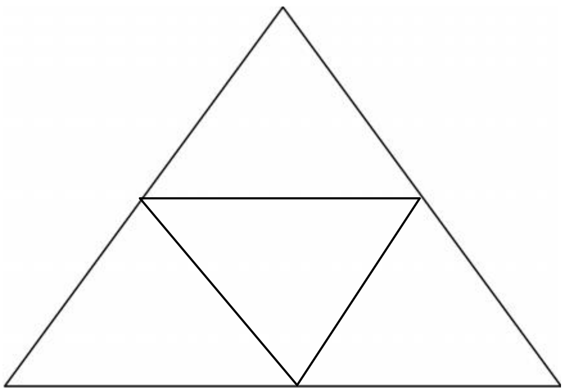

Figure 1. Fraud Triangle Model

The most essential fraud ingredients common to both models are greed, opportunity and exploitation According to a survey (Hayward, 2007), it was found out that greed constitute the main cause of fraud, responsible for about 65% of the cases. In term of opportunity, it was found out that fraud thrives where internal control is weak, poor security system and little chance of detection or immediate apprehension. To some people fraud is seen as being smart and this is their justification. These are quite evident in some of the character trait of fraudsters where trait such as ego, illusion, positioning and intelligence abound.

Donald Cressey developed the theory of the fraud triangle. He concluded that individuals commit fraud when three factors are present: (1) a financial need that cannot be shared, (2) a perceived opportunity for illicit gains, and (3) a personal rationalization of the act. Perceived pressure relates to the motivation that leads to unethical behaviors. Every fraud perpetrator faces some type of pressure to commit unethical behavior. Albrecht, Howe, and Romney, (2006) pointed out that the word perceived is important due to the fact that pressure does not have to be real; if the perpetrators believe they are being pressured, this belief can lead to fraud. Perceived pressure can result from various circumstances, but it often involves a non-sharable financial need. Financial pressure has a major impact on an employee's motivation and is considered the most common type of pressure. Specifically, about 95% of all cases of fraud have been influenced by financial pressure (Albrecht et al., 2006). Motivations are so natural to human beings that no special forces are necessary to explain law-breaking (Jensen, 2003).

Opportunity is created by weaknesses in the systems that allow an individual to commit fraud; in the accounting field, this is called weak internal control. The concept of perceived opportunity suggests that people will take advantage of circumstances available to them (Kelly & Hartley,

2010). In most cases, the lower the risk of getting caught, the more likely it is that fraud will take place. Other factors related to perceived opportunity can also contribute to fraud, such as the assumption that the employer is unaware, the assumption that employees are not checked regularly for violating company policies (Sauser, 2007).

Rationalization refers to the justification that the unethical behavior is something other than criminal activity. If an individual cannot justify unethical actions, it is unlikely that he or she will engage in fraud. Some examples of rationalizations of fraudulent behavior include "I am only borrowing," "the organization can afford it," and "it is not really a serious matter." It is important to note that rationalization is difficult to observe, as it is impossible to read the perpetrator's mind. Bank employees have knowledge of the systems as well as classified and confidential information which together with technological advancement can give them the opportunity to commit frauds. All they need is some pressure and the rationalization and that way they become part of fraud cartels that are fleecing millions of shillings from the banks (Jensen, 2003).

Theory of Reasoned Actions (TRA):-

This theory originates from social psychology and was developed by Ajzen and Fishbein in 1975. They developed TRA to define the links between the beliefs, attitudes, norms, intentions, and behaviors of individuals in their intention to use ICT. The theory assumes that a person's behavior is determined by the person's behavioral intention to perform it, and the intention itself is determined by the person's attitudes and his or her subjective norms towards the behavior. The subjective norm refers to "the person's perception that most people who are important to him think he should or should not perform the behavior in question" Fishbein and Ajzen, (1980). In

TRA rational considerations determine the choices and behaviors of individuals, and individual intentions determine behavior. Intentions refer to individuals' plans and motivations to commit a specific act. Intentions also reflect individual attitudes and the extent to which individuals perceive a specific act as desirable or favorable. The theory suggests that human behavior is governed by personal attitudes, but also by social pressures and a sense of control.

Experts agree that frauds and other unethical behaviors often occur due to an individual's lack of personal integrity or other moral reasoning (Dorminey et al., 2010; Rae & Subramaniam, 2008), as moral and ethical norms play essential roles in an individual's decisions and judgment. But environmental circumstances that provides opportunities for exploitation is also a contributory factor.

Empirical Review:-

There have been an extensive studies conducted in many countries on fraud and financial innovation. The customer's intention to use an innovation can be influenced by security risks as this can create opportunities for fraudsters. In a study ABF (1997) found that security concerns are keeping both consumers and bankers away from financial innovation. Booz et al. (1997), reveals that security concern among customers was the top ranking obstacle for non-adoption of financial innovation in Latin America. Perceptions of risk are a powerful explanatory factor in consumer behavior as individuals appear to be more motivated to avoid mistakes than to maximize benefits.

In the banking system especially as regards the proliferation of innovative products, fraud had been on the increase because of security compromise and unethical behavior of some unscrupulous individuals who exploit operational and process loopholes to defraud banks and unsuspecting customers. These are risks in the banking innovative system (Soludo, 2008). Financial innovation adoption should be enhanced by reducing the level of risk (Ovia, 2005). Owing to the open Internet technology infrastructure and lack of sufficient local and international laws concerning e-finance activities, the trust and trust related-concepts (that is risk, credibility, image and reputation) have to be integrated with the financial innovation control models. According to the Bassel Accord (2001), operational, legal, reputational and transaction risks add to the total risk profile of the bank.

According to Kondabagil (2007) security is a major problem facing customers whenever they make online transaction. In a study conducted on internet users by Zhou, Lu and Wang (2005), it was found that 81% of users are concerned about privacy when they are online. In a research conducted by Besavros (2000) it was found that, consumers are always reluctant to share their information online due to fear that their financial file will be opened to the internet universe. Gaining the confidence of customers is of paramount important to service providers and if not well managed could discourage users and could encourage negative spread of information which could pull back intending customer. Customers' security is one of the very important factors in determining the decision of consumer to use financial innovation. Cooper (1997) identifies "the level of risk" as an important characteristic from a consumer's perspective in the adoption of innovation. Consumers believe that security risk is related to the threat of losing money. Surveys have shown that security risk is one of the important factors that can have influence on adoption of online banking services. The gap between the perceived security of a technology and its real security level can affect behavior of people (Huang *et al.*, 2011). The success of financial innovation service adoption is threatened by lack of awareness and incorrect perceived knowledge about information and money security.

Key fraud enablers in financial innovation services are: Weak regulation, Maturity of the financial system, Processes Compliance monitoring, Consumer awareness and poor communication within the system, High cost of transactions, Pricing policies, Cultural issues and Seasonality. Occurrence of fraud depends on the stage of the deployment of financial services.

In India according to Assocham PWC Report (2015), technology has become the biggest driver of change in the financial services sector. Most financial institutions are therefore insisting on cashless and paperless transactions. The new technologies adopted by financial institutions are making them increasingly vulnerable to various risks such as phishing, identity theft, card skimming, social engineering, website cloning and cyber stalking. According to RBI records, 22 million of the 589 million bank account holders use banking innovation applications and the volume of mobile banking transactions has risen from around 18,190 million INR in 2011–12 to approximately 1,018,510 million INR in 2014–15. The value of financial innovation fraud rose from 350000 billion INR in 2012 to 800000billion INR in 2015. Around 65% of the total fraud cases reported by banks were technology-related frauds (covering frauds committed through/ at an internet banking channel, ATMs and other payment channels like credit/debit/prepaid cards).

In Nigeria according to Olaoye and Dada (2014), level of fraud in the banking industry rose from N13000million in 2002 to N222000million in 2012. 75-80% of these frauds are financial technology innovation based. Apparently, financial innovation may not be totally adopted in Nigeria unless it is considered safe and secured by the customers. Nobody rational will want to invest in an environment latent with risks and frauds

In a study conducted by Wole and Couisa (2009) using automated teller machines (ATMs) as the target innovation. The study found that attitudinal dispositions significantly influence the use of ATM in any bank. Adewunmi (2007) in his explanation of bank fraud identify socio-economic lapse in society such as misplacement of societal values, the unquestioning attitude of society towards the sources of wealth, the rising societal expectations from bank staff and the subsequent desire of the staff to live up to such explanations as contributory factors of fraud.

Nwude (2006) carried out a bank frauds using methodology of an interaction with bank staff of various cadres with structured questionnaire to identify the fraud forms and characteristics in the banking industry. The study reveals that some staff involve in fraud due to greediness and arrogance. In a different study, Otusanya (2008) carried out a study on the role of Bank CEO in the perpetration of corporate executive frauds in the Nigerian Banking sector. The study reveals that recent banking crises in Nigeria have exposed the activities of bank executives in corruption and fraudulent practices.

Adepoju and Alhassan (2010) opined that bank customers have come to depend on and trust the Automatic teller machine (ATM) to conveniently meet their banking needs, but that in recent times; there have been a proliferation of ATM frauds in the country. Akindele (2010) conducted a research on the "challenges of automated teller machine (ATM) usage and fraud occurrence in Nigeria banking industry". The study posits that lack of adequate training, communication gap, and poor leadership skills were the greatest causes of fraud in banks. He advised that adequate internal control mechanism be put in place and that workers satisfaction and comfort be taking care of.

RESEARCH DESIGN/ METHODOLOGY

Desk survey and exploratory designs were used in this study. Secondary data on frauds and forgeries, deposit liabilities and financial innovation contribution in all the 21 Deposit money banks were sourced from CBN, NDIC, NIBSS and KPMG. Panel interview was also used to corroborate secondary data. The data obtained was analysed by trend analysis, in order to determine the relationship between fraud risks (fraud cases and loss) and financial (technology) innovation (adoption) proxied by deposit liabilities of all banks. Descriptive statistics such as frequency table and percentages were used to present the data.

ANALYSIS AND INTERPRETATION OF RESULTS

a) The panel discussion is summary explained that the imperative of Nigeria becoming cashless with the goal of minimising cash transaction and economic dangers associated with it have sparked off innovations from the Central Bank of Nigeria (CBN), the telecommunications companies (telcos), the Nigeria Deposit Insurance Corporation (NDIC) and other stakeholders, e g Banks ranging from Mobile Money System to online banking and e-wallets. However, challenges propping up with the various innovations, operators and regulators admit, are overwhelming. As technology explodes, so also does the sophistication of frauds, for as banks rely more on technologies, they increasingly have to make huge amounts of sensitive personal data readily available to customers, clients, vendors and employees through various platforms with risks of compromise via mobile apps and cloud servers

The NDIC boss identified e-fraud and web-based sharp practices as some the hurdles, saying, "It is worrisome to note that the banking system has continued to record very high incidences of fraud and forgeries in recent years.... The amount involved in 2013 was N21.80 billion as against N25.61 billion in 2014, which was a 17.5% increase with expected/actual loss increase from N5.76 billion in 2013 to N6.19 billion in 2014. "The types and nature of frauds and forgeries were largely web-based and ATM related, fraudulent transfer/withdrawal of deposit frauds and suppression of customer deposits, among others" attributing some of the causes to weak IT infrastructure. Commenting on risk-mitigation strategies against e-fraud and associated risks, Director of Research Department of NDIC said "The growing number of Mobile Money Operators (MMOs) and subscribers in the country present new challenges, which include the safety and security of the depositors' funds in the digital and virtual environment.

Between 2013 and 2014, actual loss to fraud through the PoS increased from N5.8 million to N157.6 million. ATM loss also increased from N55 million to N2.7 billion, while Mobile Banking increased from N6.8 million to N13.3 million. While expatiating on investigations into e-banking frauds and forgery cases in the country, Deputy Superintendent, Bank Fraud Section of the Economic and Financial Crimes Commission (EFCC), said though the percentage increase in fraud cases had been alarming, efforts were being made by the security operatives, CBN, NDIC, Nigeria Inter-Bank Settlement System (NIBSS) Plc and telecoms operators to demystify, resolve and prevent frauds. The EFCC investigator said the Bank Verification Number (BVN) initiative of the CBN and Bankers' Committee, the use of E-FASS software and Know Your Customer strategies would go a long way in minimising the risk exposure and actual loss to e-banking in particular, while harping on imperative of effective use of KYC strategy by DMBs to checkmate loss to forgeries and bank frauds.

Speaking from the operator's perspective, Managing Director of GTbank, said emplacement of a number of policies and control mechanisms by DMBs and other operators to check-mate e-fraud and forgeries would go a long way. Some of the measures, he said, are filling of appropriate register for ATM Card/PIN release; proper stocktaking of ATM cards Chip and PIN technology encoded in ATM cards; 24-hour contact centre hotline to escalate card-related issues and internal fraud management technology to monitor irregular transaction patterns.

Managing Director of NIBSS, speaking on 'Managing the risks of e-banking in Nigeria', said NIBSS manages cheque clearing and settlement, Nigeria Electronic Fund Transfer (NEFT), e-dividend, Nigeria Instant Pay (NIP), Point of Sales (PoS), ATM Switching, e-Bills Pay platforms on behalf of participating banks for easy tracking, identification and resolution of transaction hurdles. He added that e-reference, Anti-Fraud, e-identification verification and BVN had been put in place to checkmate frauds, protect depositors and e-channels users' wealth. He argued that most e-banking frauds were associated with users' disclosure of personal and security details, knowingly or otherwise, to third parties, while adding that insider collaboration in the banking system also accounted for rising cases of e-frauds.

b) Fraud data and implication for financial innovation adoption:-

The increase in the number of fraud cases and the amount involved could be said to be as a result of rising fraud cases through ATM, internet banking and suppression of customers' deposits (NDIC Annual Report 2012). This assertion could not be better said than by the man in charge of NDIC. His view was aptly supported with facts and figures from reliable sources and relevant authorities. Ten banks with the highest number of reported frauds and forgeries cases, as presented in Table 1 above, were responsible for 90.10%(2009), 88.38%(2005), 87.1(2011), 86.16(2012), 64131%(2008), 51.77%(2006), 51.08(2010) and 25.64%(2007), of the total frauds and forgeries that were reported in the banking industry in the 8 eight years (i.e. 2005-2012) respectively. Year 2011 and 2012 have higher proportion of % share which are 87.1% and 86.16% respectively while the amount involved in 2012(15,478.31) was lower to that of 2011(24,730.044).

Table 1: Ten Banks with Highest Fraud Cases

	All Banks Amount involved in fraud (N'm)	10 Banks Amount involved in fraud (N'm)	% of 10 Banks to Total Amount involved in fraud
2005	10,606.18	9,373.74	88.38
2006	4,832.17	2,512.73	51.77
2007	10,005.81	2,565.01	25.64
2008	53,522.86	34 311.72	64.11
2009	41,265.50	37,179.90	90.10
2010	21,291,417.00	10,874,680.00	51.08
2011	28,400,855.00	24,730,044.00	87.10
2012	17,965.00	15,478.31	86.16

Source: Adapted from NDIC Annual Reports (2005 – 2012)

From CBN 2015 Report, since 2001 till date, the incidence of fraud in banks has been on the increase, with correspondent increase in actual total loss. The loss was astronomical within 2009 and 2010, but as at 2011 it is still above N5.8 billion mark. It is unfortunate that as the volume of banks' deposit liabilities are increasing, so also the number of fraud cases, the value of fraud and actual losses due to fraud, mainly supported by financial technology innovation which is suppose to encourage financial deepening and inclusion. These facts are as disclosed in table 2 below. The heartache of management and financial regulatory authorities on the issue is that; while they are busy strategizing on widening financial inclusion and financial deepening thereby stimulating and encouraging financial innovation adoption by customers to achieve the goal, it is the same instrument or channel of financial innovation (technology) that is being used to enhance fraud perpetuation and growth, what an irony? From CBN report the cybercrime fraud totaled N10.0 billions in 2012, N18.5 billions in 2013 and N20.0 billions is 2014

Table 2: Number of reported fraud cases, Actual fraud losses and Total bank deposit liabilities

Year.	Number of Reported Cases of Fraud.	Actual Loss to Fraud (N' Billion)	Banks' Total Deposit Liabilities.(N' Billion)
2001	908	0.931	947.18
2002	981	1.4	1,157.11
2003	1036	1.5	3,013.37
2004	1175	2.6	1,661.48
2005	1229	1.38	2,036.09
2006	1193	2.6	3,245.16
2007	1553	2.87	5,001.47
2008	1974	3.67	7,960.17
2009	3852	7.0	9,150.04
2010	5960	11.4	9,784.54
2011	2527	5.8	12,330.00

Source: CBN Statistical Bulletin 2012

According to a Customer satisfaction survey carried out in Nigeria by KPMG in 2014 and NIBSS report of 2015, the number of fraud cases in 2013 and 2014 were 822 and 1462 respectively. The value of fraud for the period were N19,148,787,069.00 andN7,750,152,748.00 respectively, while the actual loss were N485,194,350.00 in 2013 and N6,215,987,323.00 in 2014. From the data obtained from survey and these two institutions more people are patronizing and adopting financial innovation, though traditional banking (branches) still has a stronghold, but this is gradually given way to financial innovation from data collected. See tables 3. 4 and 5

Table 3: Respondents / Customers preferred (used) channel of transaction

Service or Product required		Preferred channel of Disbursement %tage	
		Branch Service %	**Innovation Product %**
1	Cash Withdrawal	20	80
2	Buying Financial product	96	4
3	Making complaint	95	5
4	Financial Advice	92	8
5	Bill payment	79	21
6	Balance enquiry	31	69

Source: Respondent survey.

KPMG (2014) concurred that 30% of the customers are satisfied with financial innovation saying that even with the apparently preferred ATM operations on cash dispensation, transaction error and downtimes are too frequent and this is laden with fraud risk. No doubt, in the last two years (2013, 2014) financial innovation products are becoming more relevant and popular, while the volume and value of cash and cheque transactions are diminishing, despite increase in level of cyber fraud as displayed in table 4. Bank customers are making more use of e-banking financial innovation products in 2014 than in the previous years. In 2014, more people are going cashless. Financial innovation account for 86% of total banking transactions in volume and 82% in value, these were 80% and 76% respectively in 2013 i e 6% across board improvement

Table 4: Financial Products Transaction Volume and Value in 2013 and 2014

	Volume /Number		Value	
	2013	**2014**	**2013**	**2014**
POS	11,258,846	24,607,497	229,903,237,909	447,459,739,698
EFT	30,134,545	30,203,908	14,218,018,800,813	14,536,388,062,398
ATM	17,967,646	42,540,034	11,674,496,434,771	21,148,614,937,311
CHEQ	14,698,538	16,070,494	8,069,550,477,646	7,725,215,739,533

Source: NIBSS Report 2015

According to the NIBSS report as the financial innovation products are growing in relevance, so also are the numbers, value and losses associated to it. Table 5 below gives a general breakdown of financial transaction, fraud attempts, fraud loss, and the contribution attributed to financial innovation products in volume and value in 2013-2014.

Table 5: Summary of fraud incidence per Channel

	2013			2014		
Product	**No of fraud**	**Value of fraud (N'm)**	**Actual loss (N'm)**	**No of fraud**	**Value of fraud (N'm)**	**Actual loss (N'm)**
CHEQUES	15	15	8693770	11	60	4448600
COUNTER	73	160	13851780	153	940	140813927
INTERNET	287	100	54999829	287	350	2688669292
e-COMMER	78	90	5851443	114	220	157610831
POS	2	90	271762696	166	30	2120881512
WEB	212	2	13948390	218	110	58994920
ATM	147	10	6787544	491	210	13328957
MOBILE	8	2	109298898	21	20	1031239284

Source: NIBSS and KPMG Reports 2015

SUMMARY, CONCLUSION AND RECOMMENDATIONS.

Undoubtedly, fraud leads to loss of money which belongs to either the bank or customers. This loss results in a decline of productive resources available to the bank Adewunmi (1986). Prominent factor in discouraging adoption of financial innovation, other side effects of bank frauds and forgeries are:

a) It destroys the bank's reputation
b) It discourages banking habit among the banking public.
c) The trust and understanding among bank, staff and customers is reduced
d) Fraud reduces bank's profitability
e) It places emotional and psychological burdens on the fraud victims.

Summarily: Increased operating expenses, reduced operational efficiency, damage to credibility, public criticisms, endanger ank's plans and strategies, bank's liquidation, depletion of shareholders' funds and banks' capital base, and bad national image. Consequently, it can be said that:

Cost of Fraud in Banks = Instantaneous loss due to fraud + Cost of fraud preclusion and

exposure + Cost of lost business + Opportunity cost of fraud avoidance and uncovering +

deterrent effect on spread of e-commerce (Olaoye and Dada, 2014)

As a part of measure to combat and prevent fraud in the banks, Central Bank of Nigeria as designed "whistle blowing policy". Whistle blowing process is a mechanism by which suspected breaches of the bank's internal policies, processes, procedures and unethical (like fraud) activities by any stakeholder (staff, customers, suppliers and applicants) are reported for necessary actions. It ensures a sound, clean and high degree of integrity and transparencies in order to achieve efficiency and effectiveness in our banks. The responsibility to protect the bank from any persons or act that might jeopardize its reputation is rest on both staffs and customers.

Concerns of fraud should not be just how to detect fraudulent activities but how to prevent them from taking place (Jesper, 2008). This aspect is more directed towards the internal control systems which banks set up in order to detect and prevent fraudulent behavior from occurring.

Fraud can be detected through internal audits, external audits and anonymous fraud hot lines.

Internal and external audits would indicate control weaknesses e.g. a lack of segregation of duties and lack of oversight through continuous, automated monitoring of journal entries.

Leuchtner, (2011) suggests that bank fraud can be deterred and detected through having sufficient technology and security to safeguard the customers' information. Such technology can record internal user activity across the bank and replay it for later investigation. Others include restricting access to customer data to prevent identity theft and continuous monitoring of employee behavior and transactional activity to help uncover warning signs of internal fraud.

The study concluded that there is need to create more awareness on the benefits of technology in minimizing fraud losses in the industry as the fraudsters are now targeting countries with slightest opportunity. Do all the needful to deter fraudulent and unethical practices on financial innovation otherwise customers will ignore it for traditional branch banking, all investment on it will be a drain and the dream of financial inclusion and deepening will be a mirage in Nigeria.

REFERENCES

1. Agbemabiese, C.G., Patrick, A.A. and Joseph, G.N. T.N. (2015) Determinants of Mobile Banking Adoption in the Ghanian Banking Industry. A Case Study of Access Bank Ltd. Journal of Computer and Communication, 3, 1-19.
2. Agboola, A. A. (2006). Electronic payment systems and tele-banking services in Nigeria, Journal of Internet Banking and Commerce. 11, (3)
3. Agwu, M. E., & Carter, A. L. (2014). Mobile phone banking in Nigeria: benefits, problems And prospects. International Journal of Business and Commerce, 3(6), 50-70.
4. Ajzen, I. and Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behaviour. Prentice-Hall, Englewood Cliffs.
5. Akintoye, R. I. (2004): Investment Division Concept, Analysis and Management Glorious Hope Publishers, Lagos.
6. Anyasi, F. I. and Otubu, P.A. (2009). Mobile Phone Technology in Banking System. Its Economic effect. Research Journal of Information Technology, **1**, 1-5.
7. Assocham/ PWC Report (2015). Current fraud trends in financial sector. Price Waterhouse Copper Pvt Ltd .India.
8. Auta, E. M. (2010). e-Banking in developing economy: Empirical Evidence from Nigeria.Journal of Applied Quantitative Methods. Vol 5/2.
9. Iddris, F. (2013). Barriers to Adoption of Mobile banking: Evidence from Ghana. International Journal of Academic Research in Business and Social Sciences, 3(7).
10. Idowu, A. A. (2005). Automated Banking and the Nigerian Economy. Ede Christatosh-Consult Nigeria.
11. Idowu, A. A. (2013). e-Banking - Banking On the Super Highways. Ede. Aseda Publishing ISBN 978-37765-7-8
12. Iftekhar, H., Schmiedel, H. & Song, L. (2009). Return to retail banking and payments. Working Paper Series 1135, European Central Bank.
13. Kemppainen, K. (2008). Integrating European Retail Payment Systems. Some Economics of SEPA. Bank of Finland Discussion Papers.
14. Khalfan, A., Alrefaei, S. & Al-Hajery, M. (2006). Factors influencing the adoption of internet banking in Oman. A descriptive case study analysis. International Journal of Financial Services Management. 1(2/3),155-172.
15. Klonner, S. & Nolen, P. (2008). Does ICT benefit the poor? Evidence from South Africa.http:// privatewww.essex.ac.uk/~pjnolen/ KlonnerNolenCellPhonesSouthAfrica. pdf. accessed on 12th April 2012.
16. Kombo, D. K. & Tromp, D.L.A. (2009). Proposal and Thesis Writing. An Introduction. Paulines Publications Africa, Don Bosco Printing Press, Nairobi, Kenya.
17. Kombe, S. K. and Wafula, M. K. (2015). Effects of Internet Banking on the Financial
18. Performance of Commercial Banks in Kenya a Case of Kenya Commercial Bank.
19. International Journal of Scientific and Research Publications, Volume 5, Issue 5,
20. Kondabagil, J. (2007). Risk Management in Electronic Banking. Concept and Best Practices. Journal of Business Administration and Management. 6(1)
21. KPMG International (2014).Nigeria Banking Industry Customer Satisfaction Survey. Issue number: 8. Published and Printed in Nigeria.
22. Mugenda, O.M. & Mugenda, A.G. (2003). Research Methods. Quantitative and Qualitative Approaches. Nairobi. Acts Press
23. Muiruri, J. K .and Ngari, J. M. (2014). Effects of Financial Innovations on the Financial
24. Performance of Commercial Banks in Kenya International Journal of Humanities and
25. Social Science Vol. 4, No. 7; May 2014
26. Muthén, L.K. and Muthén, B.O. (2007). Mplus User's Guide. Sixth Edition.Los Angeles,
27. CA: Muthén & Muthén Myoung, P. H. (2008). Univariate Analysis and Normality Test Using SAS,Stata, and SPSS* The Trustees of Indiana University Univariate Analysis and Normality Test:1 http://www.indiana.edu/~statmath. 2008 Revision with new versions of software packages.
28. Nadia, M., Anthony, S. & Scholnick, B. (2003). Is there a customer relationship effect from bank ATM surcharges? NYU Stern School of Business Department of Finance Working Paper No. 03-020
29. Nasri,W.(2011). Factors Influencing the Adaption of Internet Banking in Tunisia, Internationa Journal of Business and Management Science. 6(8), 143-160.
30. NIBSS, (2015). 2014 E-Payment Fraud Landscape in Nigeria. www.nibss-plc.com.ng
31. Ndlovu, I. and Siyavora, A.(2014). Impact of internet banking on the Zimbabwean Banking sector: An application of the multinomial logit modeling. International Journal of Economics, Commerce and Management United Kingdom Vol. II, Issue 8.
32. Newing, H. (2011). Conducting research in Conservation: Social Science Methods and Practice.New York: NY Routeledge.
33. Ngumi, M. P.(2013) Effect of Bank Innovations on Financial Performance of Commercial Banks in Kenya. A PhD thesis in Business Administration at the Jomo Kenyatta University of Agriculture and Technology
34. Odumeru, J. A. (2013) .Going cashless. Adoption of Mobile Banking in Nigeria. Arabian Journalof business and Management Review (Nigerian Chapter).1 (2),9-17.
35. Ojo, J. A. & Lawal T. T. (2014). Practice of Banking. Ibadan . Aseda Publishing, ISBN-978-006-290-4
36. Olatokun, W. & Bankole, N. (2011).Factors Influencing Electronic Business TechnologiesAdoption and Use by SMES in a Nigerian Municipality. Journal of Internet Banking andCommerce. 16(3), 1-29.
37. Olaoye, C. O. Dada, R. A. (2014). Analysis of Frauds In Banks: Nigeria's Experience. European Journal of Business and Management www.iiste.org ISSN 2222-1905 Vol.6, No.31.