Evaluation of Insider Threat on Banks Performance: Evidence from Nigeria

Eze Charles U. and Ikpor Isaac M.

1Department of Accountancy and Banking/Finance Ebonyi State University Abakaliki, 2Department of Accountancy and Business Administration Faculty of Management and Social Sciences Federal University Ndufu -Alike Ikwo

Corresponding Author: Uzomaeze.y2k7@yahoo.com

ABSTRACT

Insider threats in the banking sector has dominated accounting and finance literature in recent years as the major issues affecting performance of banks in Nigeria. This paper evaluates the impact of insider threats on the performance of banks in Nigeria. The study covers all Deposit Money Banks existing in Nigeria for the period 2003 to 2015. Data were extracted from the financial statements and accounts of Financial Institution Training Centre (FITC) and Central Bank Statistical Bulletin for various years. Multiple linear regression analysis was used to analyze the data using Statistical Package of Social Sciences (SPSS) version 20.0. Findings reveal that Employee fraud has negative effect on Return on Asset (ROA) while Outsider Related fraud has positive effect on ROA. Based on these findings, the study recommends that banks should ensure that the banking environment create equal opportunity for employee growth and aspiration and to undertake secrecy compliance agreement before engagement, formulating policy on the use of personal devices for official assignment by employees.

Keywords: Insider, Insider Threats, Insider Fraud and Bank Performance.

1.0 Introduction

Insider threat is a universal occurrence and has continued in upward trend over the years. Research has shown that insider fraud constituted above sixty five percent of all the insider threat globally (Randazzo, Keeny, Kowalski, Cappelli, and Moore, 2005). In Nigeria for instance, a total of 43,118 outsider fraud cases, 5,423 employees' fraud cases, 249 cases of insider/outside fraud collusion cases and 2,265 not specified fraud cases were recorded from 2004 through 2015, involving an approximated sum of 202 billion naira and actual or expected loss of 41.8 billion naira (Financial Institution Training Centres (FITC)). In these reports, insiders were regarded as current employees of the banks thus, overlooking the impact of actions of former employees, contractors, vendors and other related insiders that have or had privileged access to information or information system (Yang and Wang, 2011), whose violation of trust could result to a threat or financial loss to banks. Zaini, Sherliza, and Abu-Bakar, (2012) referred to this group of insiders as “Professionals in Crime” termed white collar criminals. This situation is very complex because insiders can use their unique access privileges and technical knowledge of bank operations to commit fraud, theft of intellectual property, breach confidentiality as well as altering or disabling security controls which make it more difficult to detect abuse (Perez, 2014), thus resulting to severe impact on the banks and endangers survivability. Recently, insiders’ fraud had led to distress of some Deposit Money Banks in Nigeria. Fraud losses affect the credibility of the banks and had been noted to have negative influence on banks performance and the economy at large (Inaya and Isito, 2016). The concern presently is that the increasing rate of insider involvement in bank fraud, if not controlled might become a norm capable of creating instability in the industry and generate tension in the larger economy. Previous studies on fraud in Nigerian banks identified insider fraud and abuse of privilege as a threat to banks performance and suggested implementing adequate security measures, sanctions and punishments (Owolabi,
adequate remuneration of staff, reward for excellence and encouragement of good code of conduct (AdduRaheem, Isiaka and Mohammed, 2012; and Olaoye and Dada, 2014).

Former and current employees, as well as directors of companies with cruel intents stand for threats to businesses and organizations. This is especially so given the tendency of some groups of individuals to commit illegal acts deliberately for a variety of reasons such as quest to get rich quick, job dissatisfaction, job insecurity, fear of disengagement, hostile working environment and conditions, and/or manipulation by others seeking to exploit access to confidential business information (Omar, 2015). Insider threats can be in form of fraud, system sabotage, theft of valuable data or information and/or information system assets/network (Cummings, Lewellen, McIntire, Moore, and Trzeciak, 2012). Insider threat in banks has remained an unending problem threatening banks in Nigeria for decades. The situation is very worrisome because in severe cases, the impact of insiders’ fraud could lead to collapse of banks. Notably, most of the liquidated banks by NDIC were largely a resultant effect of insider fraud and loan abuses (Uchenna and Agbo, 2013). Furthermore, as banks continues to embrace Information Technology (IT) innovations to guarantee efficient service delivery, attentions of these malicious insiders has gradually shifted from loan abuses to electronic payment channel with peculiar interest on abuse of users privilege and theft of Personal Identification Information (user access). These fraudulent activities over the years have resulted to huge financial losses to banks. According to FITC annual reports, Nigerian banks lost approximately N42.9 billion naira from 2003 to 2014. Other consequences of this menace include: increased investment on control measures, increased audit and investigation costs, reputational damages, loss of share values and loss of customers confidence and so on.

Unfortunately, Nigerian banks have taken several actions with the view to save cost but consequently increased the opportunities and possibilities for white collar crimes by related insiders especially among professionals with Information Technology (IT) expertise. For instance, the regularity of disengagement of staff, downsizing and/or engagement of temporary/contract staff in Nigerian banks suggests a traumatic situation because these actions have been identified as key factors contributing to the increasing number of fraud cases in Nigeria banks (Olaoye and Dada, 2014). Thus, the need to evaluate “insider threat” in Nigerian banks and its effect on banks “performance” with the view to suggest possible remedial actions using insider fraud involvement as a proxy for insider threat.

The objective of this study therefore is to evaluate the impact of insider threats on the performance of banking sector in Nigeria. The findings from the study will help to advance the frontier of knowledge in banking fraud in Nigeria. This study will particularly be of benefit to supervisory authorities, forensic accountant, internal and external auditors and bank management as it highlights critical issues connected to insider threats and its effects in Nigerian banking industry. It will also serve as resource material for further researcher.

2.1 Literature Review

2.2 Conceptual Review

An insider is an individual that has been legally, rightfully and officially empowered with the access privilege/s to act, represent and take critical decisions about one or more assets of the organization’s (Bishop, Gollmann, Hunker, and Probst, 2008). Trusted insiders (employees, clients, vendors, contractors, partners, customers etc.) who have authorized credentials (username, password and token) have access to the information system and the network; thus enabling the malicious ones to compromise the confidentiality, integrity, and availability of the information system (Yang and Wang, 2011). The threat of insiders ranges from fraud, system sabotage, theft of valuable data or information and/or information system assets/network (Cummings et al, 2012). Malicious insider threat is regarded the most destructive source of threat to an organization and the most difficult to deal with because insiders are usually granted opportunity to privileged, confidential and valuable information/data and information system which they can choose to exploit and their ability to circumvent vulnerable areas (Carol, 2006 and Bishop et al, 2008). Unfortunately, most organizations are looking elsewhere to safeguard against security threats while the most time, attentions is devoted to catching the criminals.
outside but the most costly and least caught is the criminals inside (Warkentin and Willinson, 2009 and Gupta and Hammond, 2007 in Babatunde and Salamat, 2011).

Globally, scholars have identified fraud as the most frequent and critical of all the insider threats confronting banks and finance industry (Randazzo, Keeny, Kowalski, Cappelli, and Moore, 2005; Cummings, et al, 2012; Inaya and Isiko, 2016; and Taiwo, Agwu, Babajide, Okafor and Isibor, 2016). Fraud is an intentional and dishonest actions practiced to acquire unjustifiable benefits (Aub- Chapman, 2000). Fraud was also defined as a deliberate action practiced of an individual or groups among corporate executives, staff or related parties resulting to misrepresentation of financial statements (Adeniji, 2014) and ICAN, 2006 in Inaya and Isito, 2016). Insider fraud is a universal occurrence that has existed for long and its persistent increases trend especially with the advancement in information technology has attracted a number of studies particularly in the finance and banking sector.

For instance, Randazzo et al (2005) conducted a case study on 23 incidents of threats involving 26 employees and related insiders of banks and other financial institutions in United States of America (USA) from 1996 to 2002 and noted the following:

a. Insider threats: 15 out of the 23 of incident studied involved fraud, 4 involve theft of data and information assets, and 4 involved sabotage of information system/network;

b. Vulnerable opportunity: most of the cases examined did not involve sophisticated technical means. Thus, the perpetrators simply exploited vulnerability in policy, regulations, guidelines and standards (but not weaknesses in the information system network) and culprits did not have sufficient technological capability;

c. Planning of Incident: perpetrators planned their actions in advance. In 74 percent of the cases, only the individuals involved were aware of the plan, in 22 percent of the cases, some co-workers knew about the incident before it occurred; friends knew about the incident in 13 percent of the cases while families were aware in 9 percent of the incident;

d. Motivation: the most notable motivation of illicit insider activities is financial gain. Other motivations noted include: sabotage of business operations, data or the organizations’ information system/network;

e. Profile of perpetrators: Different categories of people were involved in all the cases. A good number of them were insiders and were not holding technical position in the institutions, were not envisaged as possible threats, did not have criminal record of previous circumvention of control or misuse of information system or attacks on the network;

f. Detection of Incident: the crimes were spotted by different technique and individuals mostly by non technical methods. These include non security personnel's, customers, supervisors and other non security personal, security staff, IT security staff, and system administrator;

g. Victims and Organizations suffered huge financial losses and;

h. Most of the incidents were executed at work places and during business working hours.

Again, Cummings, et al (2012) studied 67 insider fraud cases, as well as 13 outsiders fraud cases in the banking and finance industry between 2005 to 2012 in the US and noted the following critical issues: criminal that carried out illicit activities with miniature method and slowly were more successful, most dangerous and took longer detection time. In several incidence, there were evidence of abuse of privilege, either by present authorized insiders or related insiders who have had authorized access but later withdrawn for various rationale; cases involving individuals in executive positions are more damaging, very significant in value and lasted for longer period, because the damage done by managers’ fraud is more devastating and lasted for longer time before detection; most of the cases did not involve collusion; most of the fraud were detected through an audit, customers complaint or co-workers suspicion; and personal identification information (user access) are the most common or prominent target of those committing fraud.

In the Nigerian context, the National Insurance Deposit Corporation (NDIC) annual reports, the Financial Institution Training Centres (FITC) annual reports and accounts and the Nigerian Inter-Bank Settlement System (NIBSS) fraud landscape provide evidences of annual insider fraud by different categories of employees of Nigerian banks. The NDIC went further to categorize insider frauds and forgeries in Nigerian banks as follows:
Supervisors and managers; Officers, accountant, and executive assistants; Clerks and cashiers; Typists, technicians, and stenographers; Messengers, drivers, cleaners, security guards and stewards; Temporary staff; and others not specified. Table 1 in appendix 1 presents the details of insiders' abuses and their categories of insiders involved in fraud and forgeries from 2003 to 2014 as used in this study.

The dreadfulness of fraud in Nigerian banks can be evidenced from its total amount involved, and/or number of reported fraud cases and/or actual/expected loss (Uchenna, and Agbo, 2013). It was also noted that most of the bank frauds in Nigeria were not reported by banks partly because of the individuals' involved or its reputational and societal impact on banks (NDIC, 2013). Adewunmi (1986) in Olaoye and Dada (2012) noted the effects of bank fraud and forgeries to include: destruction of bank's reputation, discouraging banking habit among the banking public, financial liquidity problems, reduces the trust and understanding among staff, creates unfavourably competitive environment among banks, reduces profitability and performance, and creates emotional and psychological problems on fraud victims. Finally, in a severe scenario, fraud can lead to bank distress. However, these fraud losses are absorbed by the earnings which would have been available for distribution to shareholders, thus reduces the equity capital of the bank, weaken the bank's financial health and limit banks ability to engage in profitable businesses (Uchenna, and Agbo, 2013). Contrarily, banks depend on its earning for payment of dividend, capital adequacy stability, creation of investment opportunity, diversification and maintaining the competitive outlook among others. Therefore, in measuring performance of financial institutions globally, earning quality is the component of CAMEL that seeks to measure the profitability and productivity of the banks, and explain the growth and sustainability of future earnings (Mohhamed, 2016). Using this approach, two major ratios are prominent: return on asset and return on equity.

2.3 Empirical Review

Researchers had recorded tremendous contribution on studies connected to fraud in Nigerian banking industry. For example, Kanu and Okoroafor (2013) studied the Nature, Extent and Economic impact of Fraud on Deposits Banks in Nigeria. The aim was to investigate several incidences of frauds in the banking sector in order to ascertain the nature and its effect on deposits, to ascertain the relationship between total amount involve in fraud cases, amount lost to fraud and deposit liabilities of deposit money banks in Nigeria. Data was collected from the annual reports of NDIC and Financial Institution Training Centre (FITC) for the period 1993-2010. Regression analyses using E-view statistical package was adopted in analyzing the data. The study found that there is a significant relationship between total amount involve in fraud cases, amount lost to fraud and deposit liabilities of deposit money banks in Nigeria. It was also established that fraudulent withdrawal is the most frequent type of fraud; and bank deposit is susceptible to clearing fraud while miscellaneous fraud inflicted the highest amount of financial losses on bank deposits in Nigeria. The study concluded that implementation of adequate internal control system and techniques, monitoring of operation of these controls and their effectiveness, creating conducive working environment and maintenance of anti-fraud culture will go a long way in fraud prevention.

Uchenna and Agbo (2013) investigated the impact of Fraud and Fraudulent Practices on the Performance of banks in Nigeria. The aim of the study was to ascertain the forms, volume and financial impact of bank frauds in Nigeria. Secondary data was generated from CBN and NDIC annual financial reports and account from 2001 to 2011. Pearson Product Moment Correlation and Multiple regression analysis were employed for the data analyses. Finding revealed that sufficient proportion of mobilized funds were lost to fraud with the period of the study. The study concluded that deposit money banks in Nigeria and the customers suffered quite a lot of financial difficulties with the period. The study also recommended reinforce of controls and procedures, improved and strengthened supervisory institution for adequate monitoring.

Taiwo, Agwu, Babajide, Okafor and Isibor (2016) empirically examined the growth of bank fraud and the impact on the Nigerian banking industry. The objective of the study was to investigate the growth of bank frauds, determine the amount of money involved, identify the causes, ascertain the types of frauds and test the impact of fraud on deposit mobilization and proffer solution to the problem. The study used time series annual data for the
period covering 2002 to 2014 generated from the Central Bank of Nigeria statistical bulletin, website, Journals and Newspapers. Multiple regression technique and the augmented Dickey-Fuller (ADF) Unit Root test were used for the data analyses. The study found that fraud inflicts severe financial difficulty on banks and their customers, leads to depletion of shareholders funds and banks' capital base as well as loss of customers' money and confidence in banks. Based on these findings, the study suggested circulating names of staff culprits among the banks, strict disciplinary action, blacklisting of staff, maintaining of a central data base by the supervisory authority of staff dismissed by banks and/or forced to resignation.

Inaya and Isiko (2016) conducted a study on the social impact of bank fraud in Nigeria. The aim was to examine the societal implication of bank fraud in Nigerian and the effect on banking sector. Data were obtained from Annual reports and Accounts of Nigerian Deposit Insurance Corporation (NDIC) and deposit money banks for the period 1990 to 2014. The Ordinary Least Square (OLS) and Best Linear Unbiased Estimate (BLUE) were adopted using SPSS. Finding revealed that fraud have negative social impact on Nigerian banks and the banks should be held responsible for the high rate of fraud in the industry. Therefore, the study suggested close monitoring of bank operation by the agencies responsible for tracking fraud in Nigeria.

Till date, there is no known study to the researchers that investigated insider threats in form of fraud and its impact on performance of banks in Nigeria. These previous studies have failed to question “who” is responsible for the increasing incidence of fraud in the banking sector. Again, previous studies noted insider as current employees of banks but on the contrary, insiders include former and current employees, suppliers, vendors and so on who have or have had privilege access to information, programs, and systems and have the specific capacity and knowledge to circumvent specific controls.

2.4 Theoretical Review

Scholars have made serious attempts to connect several factors and conditions that affect fraud into comprehensive theories. For instance, the Crime Opportunity theories suggests that criminal take logical decision on choices and however chooses options that offer greater return with little challenges and/or minimal risk (Cohen, and Felson, 1979). It suggests that two vital conditions must exist for crime to occur: the existence of motivated culprit that is willing to execute the criminal activity, and the existence of control weaknesses (opportunities) in the environment which the culprit is motivated to exploit.

Again, the Differential Opportunity Theory (DOT) propounded by Cloward and Ohlin in 1960, holds that people from poor socioeconomic surroundings, characterized by limited opportunities for success, may likely use any means to achieve success (Owolabi, 2010). The differential opportunity theory simply suggests that environment limitations create pressure and rationalization to commit fraud or crime. In organizations where environment deprive employees opportunity for growth and aspiration, criminal activity can be rationalized by the unequal opportunity created by the environment. This theory maintained that people faced with minimal opportunities could choose crime as alternatives for achieving success.

Conversely, the Fraud Triangle Theory (FTT) suggests that three conditions must be present for people to commit fraud. According to Donald Crassey, “Pressure, Opportunity and Rationalization” are conditions mandatory for possible breach of trust. He concluded that individuals that violate financial trust usually envisaged of themselves as being in financial distress which they cannot be discuss with others, and having the consciousness and understanding that the challenge could be resolved secretly, and also possesses ability to reasonably convince themselves to think as users of the trusted property but not as trusted persons (Crassey 1953:742 in Abdullahi, Mansor and Nuhu, 2015).

FTT suggested that most culprits knew that fraudulent act is illegal and wrong and intentionally decided to embark on it and convinced themselves to think that the behaviors are legal. In line with the FTT, the Fraud Diamond Theory (FDT), suggested that a criminal must have capacity to identify and exploit the opportunity even in the presence of the three elements of FTT (Wolfe and Hermanson, 2004). Opportunity unlock the door for fraud, Incentive or Pressure and Justification creates
motivation and draws the culprit closers but “Capability” is the required knowledge and skills to identify the opportunity and exploiting it (Abdullahi et al., 2015). Abdullahi et al. (2015) also noted that the elements of FDT are interrelated in that fraud cannot occur except that all the element are present. For instance, pressure (financial need) could be the motivation for seeking a loophole in the system “Opportunity”, and “Opportunity and Pressure” could also be the basis of “Justification” but all these can never result to fraud except the culprit possesses required “Capability” embark on it (Hooper and Pornelli, 2010 in Abdullahi et al., 2015). Therefore FDT suggested additional element of capability as critical factor in fraud investigation.

Finally the collusion theory suggests that two more people sometimes illegally agree to act secretly, in order to defraud the organization or public, to suppress other people and denial them of the entitlements, and to deceive, mislead and curtail opposition and competition or to gain unmerited benefits (Owolabi 2010). Therefore, employees having opportunities and motivation to commit fraud can connive and defraud the organization, stakeholders or third parties.

Consequently, this study is anchored on three major theories: differential opportunity theory, fraud diamond theory and collusion theory. These theories identified factors, conditions and possible situation which could encourage insider fraud in an organization. For instance, the differential opportunity theory provided insight of unfair employment conditions, hostile employee welfare scheme and other industrial pressures currently existing in the banking sector which represents motivation and rationalization of fraud by criminal insiders. This include: job insecurity, excessive target, disengagement of permanent staff and engagement of temporary and contract staff and so on. The fraud diamond theory pointed at “whom” to investigate or monitor strictly in building control activities and procedures or even fraud investigation and analysis. It noted that insiders with specified skill and capability are most vulnerable when motivated to committee fraud, therefore required strict monitoring. The collusion theory also included the possibility of possible conniving by employees, related insiders or even outsiders; therefore suggesting that internal control cannot be effective in this particular situation.

Thus, controlling these factors, conditions and possible situations identified in these theories are effective tools for management to control insider fraud risk as well as probing instruments for supervisory authorities, auditors, investigators and forensic personnel.

3.0 Methodology

The population of the study includes all deposit money banks in Nigeria 2003-2015. Due to the collapse of some banks in Nigeria, the population varied during the period as presented in appendix. The study employed expo-facto research design. This design was found appropriate because, it seeks to establish the association with variables or behavioral relationship between factors by evaluating existing past data of previous similar condition (Inaya and Isiko, 2016). Data were collected from published annual financial reports of Financial Institution Training Centre (FITC) for the various years and CBN Statistical Bulletin (2015) and CBN Statistical Bulletin various issues in Akpan (2017). The sources provided a higher quality data given that it was a permanent and published source of information, hence reliable. Multiple regression analysis was employed in analyzing the data via the Statistical Package for Social Sciences (SPSS, 20.0).

3.1 Model Specification

In order to investigate the extent to which insider threats affect performance of banks in Nigeria, we hypotheses thus:

i. Employees' fraud does not significantly affect performance of banks in Nigeria.

ii. Related insiders' fraud does not significantly affect performance of banks in Nigeria.

iii. Fraud losses on asset utilization and fraud success rate does not significantly affect performance of bank in Nigeria.

The dependent Variable of the study is Return on Asset (ROA) which was used as a proxy for bank performance. This is similar to the study of Sulaiman and Akeke (2012), Mohammed (2016), Oladele, and Fredrick (2016). ROA indicates how well assets are being used to generate profits. It is also a basic measure of profitability that corrects for the size of the organization. While the independent variables are the ratio of the Number of Employees Involved to the Total Number of Fraud Cases.
NEI/NFC, which captures the extent which bank employees contributed to bank fraud during the period in Nigeria; the ratio of Outsiders/Related Insiders involved to Total Fraud Cases (ORI/TFC), which we use to capture the impact of related insider frauds during the period in Nigeria; the ratio of Actual/Expected Fraud Losses to Total Assets of banks (AEL/TA), which we use to capture the losses on assets utilization by management due to fraud during the period in Nigeria and the ratio of Actual/Expected Fraud Losses to Total Amount Involved (AEL/TAI), which captures the success rate of fraud.

The model was employed to run in Nigerian Deposit Money Bank as a single entity in order to capture the effect of insider threat in banks performance in Nigeria. We adopted and adjusted this model in consistent to studies of Uche and Agbo (2013); and Taiwo et al (2016) as stated below: 

\[ ROA = f(NEI/NFC, ORI/TFC, AEL/TA, AEL/TAI) \] .... Eq. (1)

Where: 
- \( NEI/NFC \) = Ratio of Insiders Involved to Total Fraud Cases
- \( ORI/TFC \) = Ratio of Outsiders and Related Insiders Involved
- \( AEL/TA \) = Ratio of Actual and Expected Loss to Total Assets of Banks (Loss on Assets Utilization)
- \( AEL/TAI \) = Ratio of Actual Losses to Amount Involved (Success Rate of Fraud)

The model is further represented linearly as stated below:

\[ ROA = \beta_0 + \beta_1 NEI/NFC + \beta_2 ORI/TFC + \beta_3 AEL/TA + \beta_4 AEL/TAI + \mu \] .... Eq. (2)

Where: 
- \( \beta_0 \) = Constant parameter
- \( \mu \) = Error term

### 4.1 Findings

#### 4.2 Empirical Finding

<table>
<thead>
<tr>
<th>Table 1: Model Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Model 1</td>
</tr>
</tbody>
</table>

From Table 1 the model summary, we find that the adjusted \( R^2 = .004 \) and \( R^2 = .330 \). This means that the linear regression explains only 33% of the variance in the dependent variable (Return on Asset). The Durbin-Watson \( d = 1.853 \), which is between the two critical values \( 1.5 < d < 2.5 \). Therefore, we assume that there is no first order linear auto correlation in our multiple regression data.

The second output table is the Anova Table which presents the F-test. The linear regression's F-test has the null hypothesis that the model explains zero variance in the dependent variable (in other words \( R^2 = 0 \)). The F-test is not significant at \( p .05 \) given \( F = .987 \) and Sig .467, thus we can assume that the model explain insignificant amount of the variance on Return on Asset.

<table>
<thead>
<tr>
<th>Table 2: ANOVA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Regression</td>
</tr>
<tr>
<td>Residual</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

### 5.1 Discussion of Findings

This research evaluated the impact of insider threat on banks performance in Nigeria. Employee and related insider fraud represent insider threat to

Lastly, we checked for normality of residuals with a P-P plot. The plot shows that the points generally follow the normal (diagonal) line with no strong deviations. This also indicates that the residuals are normally distributed.
Nigerian banks and Return on Assets (ROA) was proxy to performance over the period 2003 – 2015. Interestingly, Employee Impact represented by the ratio of employee fraud to total reported fraud cases (NEI/TFC) and Loss on Asset Utilization represented as the ratio of Actual/Expected Loss to Total Asset (AEL/TA) has insignificant negative influence on ROA during the period. This implies that as employees fraud cases increases, ROA decreases and as loss to fraud increases, ROA decreases though in an insignificant magnitude. This results are in consistent with the previous studies of Taiwo et al (2016) which maintained that as the employees fraud increases, it will affect banks profitability negatively; Uchenna and Agbo (2013) that concluded that fraud losses have negative effect on banks performance in Nigeria and NDIC (2014) which maintained that the value of fraud losses did not significantly affect banks performance. The negative sign is an indication of priori expectation.

Surprisingly, the study found that Outsider/Insider related impact represented by the ratio of outsider fraud to total fraud cases (ORI/TFC) and the success rate of fraud represented by the ratio of Actual/Expected loss to Total Amount Involved (AEL/TAI) share positive insignificant influence on ROA. Thus as banks performance continues to improve, there exist the tendency of related insider and outsider to embark on several fraudulent practices especially with the current evolution in the information technology. Again, as banks hirer and fire contract staff, temporary staff, vendors, suppliers, contractors, downsizing its workforce and introduces other cost saving innovations (for instance: Bring Your Own Device (BYOD), there is the tendency for increased related insider threat due to for employees, vendors, suppliers, contractors, who have or have had privileged access to sensitive information and systems and have obtained professional capability to circumvent certain security procedures. These are some of the factors that may increase the related insider threats viewed from the outside. Similarly, the result showed that improved performance may result to insignificant increase in the success rate of fraud. This may be as a result of ineffective security governance, theft of ID credentials and abuse by authorized privilege users. There is also the possibility of the executive to breach the trust against the stakeholders which will have great impact on the bank.

5.2 Conclusion
We wrap up the implication of this research findings in this section. Obviously, there have been evidences on insider threat in Nigerian banks in form of employee and related insider fraud especially in this era of information technology advancement and usage in banking operation and payment system. However, this study has reached a consensus that insider threats affects bank performance negatively and intensely concludes that insider threat have insignificant influence on performance of Deposit Money Banks in Nigeria.

5.3 Recommendation
Based on the following findings, it is therefore important to make recommendations that would ensure that the incidence of fraud in Nigeria banks is drastically nipped to the bud.

- Banks should reduce pressure on its employees by ensuring that the banking environment did not discriminate or deprive employee opportunity for growth and aspiration. This is because when employees know that there are reasonable equal opportunities for growth, there are no unnecessary pressures from the management and they have reasonable assurance that their job is secured, they will consciously not compromise because of the fear of losing this privileges and not the fear of punishments. Again, in fraud investigation, there is an assumption that only 10 percent of the entire populace can never commit fraud and must comply to the laid down rule, 80 percent of the populace might commit fraud if motivated to seek opportunity; but only 10 percent of the populace is aggressively looking for opportunity to exploit. This means that when there is pressure and harsh working environment, 90 percent of the total employees automatically became potential fraudsters, therefore the risk of collusion and abuse of privileges will be high.

- Banks should ensure that vendors, suppliers and contractors undertake information security/secrecy compliance agreement which will be binding on them during and after the engagement period before allowing access to sensitive assets and systems. This is because these groups of insiders are not directly under the control of the organization. An express
contractual agreement at any level of privilege access right to sensitive information/systems with detailed compliance and confidentiality responsibilities will serve as deterrence measure.

- Banks should formulate policy which specifies the extent of use of personal devices for official duties if allowed and categories the level of information which could be access or stored in such devices. This is to ensure that sensitive information are adequately controlled in order to maintained confidentiality of such information. Personal devices should not be used to access or store sensitive organizational information incase of loss of the device, employment termination, and so no. When this happens, the organization will be more vulnerable to fraud and other forms of attacks.

- As a matter of urgency, access granted to disengaged, suspended and resigned employees should be disabled. This is to ensure that this group of insiders will not have access to the information system instantly. If possible, additional security procedure should be introduced to frustrate attempts from such former employees who might chose to use the professional knowledge to cause havoc. Once this is done, the new security measure will introduce new level of controls which this group of insiders might not have the capacity to circumvent or maneuver, thereby hindering any anticipated attack.

- Continuous online auditing, segregation of duties and access right. These activities must be part of routine internal control measure so as to effectively monitor the occurrence and usage of the system. Effective online auditing will expose high risk areas before much harm is done. Segregation of duties and access rights is an effective tool to checkmate fraud especially be single individual. Access should be granted on task bases and training of staff on job requirement and need to no know bases to limit excessive capacity building.

- Nigerian banks should regard information security as non-negotiable and a governance issue. Increased education and awareness among employees and customers will also increase recognition and willingness to report suspicious behaviors. As a governance issue, the board of director should ensure that the information systems of banks are adequately secured. Adequate investment in security measures will limit outsiders' fraud greatly because it will be very difficult for them to have access to the information system. Again increased security awareness among staff and bank customers is of great importance. This is because fraudsters rely on information which the trickery obtained from their victims. So educating the users of online banking platforms, mobile banking platform and other electronic payment system on the security challenges of these systems and how to manage their access/sensitive information will be more effective rather than issuing disclaimer notices as frequently used by Nigerian banks.

- Finally, speedy prosecution and punishment of culprits' especially senior officers and executives by regulatory authorities will serve as deterrent measure to those who may wish to abuse their privilege. The legal system should facilitate any reported cases as most of the executive officers are taking advantage of the delay in legal processes. There should also improve collaboration between the banks and agencies. The NDIC should increase sanctions on any bank who fail to report fraud committed in the bank because of the person/persons involved.

Reference:


Zaini, Z., Sherliza, P. N., and Abu-Bakar, M.,

Appendix 1

Table 1: Banks Return on Assets, Total Assets, Total Deposits and Incidence of Fraud in Nigerian Banks (2003 – 2015).

<table>
<thead>
<tr>
<th>S/ N</th>
<th>YEAR</th>
<th>NOB</th>
<th>ROA</th>
<th>TAI(N’ M)</th>
<th>TAE(N’ M)</th>
<th>TFC</th>
<th>NEI</th>
<th>ORI</th>
<th>AEL/TA</th>
<th>TAI/TA</th>
<th>AEL/TAI</th>
<th>NEI/TFC</th>
<th>ORI/TFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2003</td>
<td>90</td>
<td>5.02</td>
<td>3,047,856.30</td>
<td>9,383.67</td>
<td>850</td>
<td>106</td>
<td>744</td>
<td>0.0003</td>
<td>0.0070</td>
<td>0.0914</td>
<td>0.1247</td>
<td>0.1425</td>
</tr>
<tr>
<td>2</td>
<td>2004</td>
<td>89</td>
<td>4.59</td>
<td>3,752,277.80</td>
<td>11,754.00</td>
<td>1,080</td>
<td>487</td>
<td>541</td>
<td>0.0007</td>
<td>0.0071</td>
<td>0.2221</td>
<td>0.4509</td>
<td>0.9002</td>
</tr>
<tr>
<td>3</td>
<td>2005</td>
<td>25</td>
<td>4.15</td>
<td>4,515,117.57</td>
<td>10,606.18</td>
<td>1,381</td>
<td>521</td>
<td>857</td>
<td>0.0012</td>
<td>0.0052</td>
<td>0.0914</td>
<td>0.1247</td>
<td>0.1425</td>
</tr>
<tr>
<td>4</td>
<td>2006</td>
<td>25</td>
<td>4.05</td>
<td>7,172,932.14</td>
<td>4,832.17</td>
<td>2,768.67</td>
<td>297</td>
<td>547</td>
<td>0.0007</td>
<td>0.0015</td>
<td>0.5730</td>
<td>0.3879</td>
<td>0.6607</td>
</tr>
<tr>
<td>5</td>
<td>2007</td>
<td>24</td>
<td>2.78</td>
<td>10,981,693.58</td>
<td>10,005.81</td>
<td>1,039</td>
<td>403</td>
<td>857</td>
<td>0.0004</td>
<td>0.0020</td>
<td>0.0914</td>
<td>0.1247</td>
<td>0.1425</td>
</tr>
<tr>
<td>6</td>
<td>2008</td>
<td>24</td>
<td>2.71</td>
<td>15,919,559.82</td>
<td>53,522.86</td>
<td>17,543.09</td>
<td>1,637</td>
<td>500</td>
<td>1.020</td>
<td>0.0011</td>
<td>0.0067</td>
<td>0.3278</td>
<td>0.3054</td>
</tr>
<tr>
<td>7</td>
<td>2009</td>
<td>24</td>
<td>5.17</td>
<td>17,522,858.25</td>
<td>41,265.50</td>
<td>2,870.85</td>
<td>857</td>
<td>547</td>
<td>0.0004</td>
<td>0.0015</td>
<td>0.5730</td>
<td>0.3879</td>
<td>0.6607</td>
</tr>
<tr>
<td>8</td>
<td>2010</td>
<td>24</td>
<td>2.36</td>
<td>17,331,559.02</td>
<td>21,291.41</td>
<td>11,679.00</td>
<td>1,532</td>
<td>500</td>
<td>1.020</td>
<td>0.0011</td>
<td>0.0067</td>
<td>0.3278</td>
<td>0.3054</td>
</tr>
<tr>
<td>9</td>
<td>2011</td>
<td>24</td>
<td>2.98</td>
<td>19,396,633.76</td>
<td>28,400.86</td>
<td>2,605</td>
<td>608</td>
<td>1,989</td>
<td>0.0002</td>
<td>0.0025</td>
<td>0.1433</td>
<td>0.2334</td>
<td>0.3057</td>
</tr>
<tr>
<td>10</td>
<td>2012</td>
<td>21</td>
<td>3.02</td>
<td>21,288,144.39</td>
<td>17,965.00</td>
<td>4,517.00</td>
<td>5145</td>
<td>596</td>
<td>4,346</td>
<td>0.0002</td>
<td>0.0014</td>
<td>0.2514</td>
<td>0.1138</td>
</tr>
<tr>
<td>11</td>
<td>2013</td>
<td>24</td>
<td>2.78</td>
<td>24,301,213.88</td>
<td>21,795.00</td>
<td>5,757.00</td>
<td>630</td>
<td>8,051</td>
<td>0.0000</td>
<td>0.0016</td>
<td>0.2641</td>
<td>0.0725</td>
<td>0.0783</td>
</tr>
<tr>
<td>12</td>
<td>2014</td>
<td>24</td>
<td>4.05</td>
<td>27,481,522.65</td>
<td>25,608.00</td>
<td>6,192.00</td>
<td>12,641</td>
<td>529</td>
<td>12,110</td>
<td>0.0002</td>
<td>0.0015</td>
<td>0.2418</td>
<td>0.0418</td>
</tr>
<tr>
<td>13</td>
<td>2015</td>
<td>25</td>
<td>4.05</td>
<td>28,117,616.22</td>
<td>18,020.00</td>
<td>3,170.00</td>
<td>13,201</td>
<td>575</td>
<td>10,692</td>
<td>0.0001</td>
<td>0.0010</td>
<td>0.1759</td>
<td>0.0436</td>
</tr>
</tbody>
</table>

Source: *Financial Institution Training Centre (FITC) for Various Years*
*NDIC Annual Report and Accounts for Various Years*
*Authors Computation*

Where:
- NOB = Number of Deposit Money Banks in each Year
- ROA = Return on Capital
- TAI = Total Assets of the Banks
- TAE = Total Amount Involved
- AEL = Actual/Expected Loss
- TFC = Total Fraud Cases
- NEI = Number of Employees Involved
- ORI = Outsiders/Related Insiders Involved
- AEL/TA = Ratio of Actual and Expected Loss to Total Assets of Banks (Loss on Assets Utilization)
- AEL/TAI = Ratio of Actual Losses to Amount Involved (Success Rate of Fraud)
- NEI/TFC = Ratio of Insiders Involved to Total Fraud Cases
- ORI/TFC = Ratio of Outsiders and Related Insiders Involved
Appendix 2

Table 2: Categories of Staff that Abuse Privilege Access to Commit Fraud

<table>
<thead>
<tr>
<th>Years</th>
<th>Supervisors and Managers</th>
<th>Officers, Accountants and Executives</th>
<th>Clerks and Cashiers</th>
<th>Typist and Technicians</th>
<th>Messengers and Drivers not Specified</th>
<th>Temp. Staff</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>25</td>
<td>41</td>
<td>25</td>
<td>-</td>
<td>7</td>
<td>8</td>
<td>106</td>
</tr>
<tr>
<td>2004</td>
<td>157</td>
<td>129</td>
<td>61</td>
<td>18</td>
<td>15</td>
<td>3</td>
<td>383</td>
</tr>
<tr>
<td>2005</td>
<td>169</td>
<td>124</td>
<td>54</td>
<td>16</td>
<td>12</td>
<td>3</td>
<td>378</td>
</tr>
<tr>
<td>2006</td>
<td>118</td>
<td>90</td>
<td>50</td>
<td>16</td>
<td>7</td>
<td>50</td>
<td>331</td>
</tr>
<tr>
<td>2007</td>
<td>87</td>
<td>89</td>
<td>34</td>
<td>21</td>
<td>-</td>
<td>45</td>
<td>276</td>
</tr>
<tr>
<td>2008</td>
<td>48</td>
<td>127</td>
<td>48</td>
<td>20</td>
<td>-</td>
<td>70</td>
<td>313</td>
</tr>
<tr>
<td>2009</td>
<td>94</td>
<td>137</td>
<td>200</td>
<td>64</td>
<td>11</td>
<td>150</td>
<td>656</td>
</tr>
<tr>
<td>2010</td>
<td>92</td>
<td>79</td>
<td>115</td>
<td>23</td>
<td>15</td>
<td>33</td>
<td>357</td>
</tr>
<tr>
<td>2011</td>
<td>89</td>
<td>126</td>
<td>163</td>
<td>7</td>
<td>35</td>
<td>78</td>
<td>498</td>
</tr>
<tr>
<td>2012</td>
<td>78</td>
<td>89</td>
<td>117</td>
<td>5</td>
<td>16</td>
<td>226</td>
<td>531</td>
</tr>
<tr>
<td>2013</td>
<td>97</td>
<td>234</td>
<td>128</td>
<td>12</td>
<td>34</td>
<td>177</td>
<td>682</td>
</tr>
<tr>
<td>2014</td>
<td>58</td>
<td>176</td>
<td>78</td>
<td>-</td>
<td>02</td>
<td>151</td>
<td>465</td>
</tr>
<tr>
<td>1,087</td>
<td>1,400</td>
<td>1,048</td>
<td>200</td>
<td>147</td>
<td>985</td>
<td>4,976</td>
<td></td>
</tr>
</tbody>
</table>