REPUTATIONAL RISK IMPACT OF INTERNAL FRAUDS ON BANK CUSTOMERS IN NIGERIA

AGWU, M. EDWIN
Department of Strategic Management and Marketing
School of Business
Covenant University Ogun State, Nigeria
Email: edwinagwu@yahoo.co.uk

Abstract

Fraud in the financial sector is a growing business for fraudsters using increasingly innovative and creative ways of targeting any perceived weaknesses in the banks and credit granting systems. Fraudsters have become ever more sophisticated, which means that fraud prevention measures need to constantly evolve to ensure they are capable of handling the threat. The fight against fraud is of crucial importance to financial service institutions. Not only does it affect their business, but it also has a significant impact on consumers in particular and the economy at large. Using a case study and historical approach and relying heavily on secondary sources of information, this study among others found a horde of laxity, inconsistencies and knowledge gaps among practitioners, thereby creating loopholes with which the fraudsters commit their nefarious deeds. There is also the absence of the right policy framework and laws to coherently safeguard lenders and borrowers. The study recommends a stiffer control measures within all financial organizations in the country as well as the enactment of enabling laws by the government to checkmate these ugly incidences.

Keywords: Internal bank frauds, Forgeries, Internal control, Compliance, Customers

Introduction and Background of the Study

Fraud encompasses a wide range of illicit practices and illegal acts involving intentional deception or misrepresentation. Fraud impacts organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. The losses to reputation, goodwill, and customer relations can be devastating. As fraud can be perpetrated by any employee within an organization or by those from the outside, it is important to have an effective fraud management programme in place to safeguard organization's assets and reputation.

Definition of Fraud

According to Agwu (2013), fraud is any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage. It has also been viewed as an illegal act involving the obtaining of something of value through willful misrepresentation.

Selected EU country's Definitions of Fraud

In Italy, fraud is broadly defined as a crime committed in order to make an unlawful gain by using deceptions and tricks. The Italian Iaw transposing the Consumer Credit Directives includes a definition for identity theft, which is the misappropriation of the identity of another person without his knowledge or consent. Identity theft can be total, if it is committed by using only another person's identity, or partial, which means that the fraudster uses both his data and another person's data.

There is no specific definition of fraud in Polish law. However a definition of a deception in the context of a loan/credit can be found in Article 297 of the Polish Criminal Code which refers to any type of loan/credit. It reads as follows:
"Whoever, in order to obtain a loan, bank loan, loan guarantee, grant, subsidy or public procurement order for himself or for another person, submits false documents or documents attesting untruth, or dishonest statements regarding their circumstances that are of significance for the obtaining of such a loan, bank loan, loan guarantee, grant, subsidy or a public procurement order shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years"

The German definition of fraud can be found in the German Criminal Code: "Whosoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the property of another by causing or maintaining an error by [presenting] false facts or by distorting or suppressing true facts shall be liable to imprisonment of not more than five years or a fine." The German Criminal Code further provides definitions of especially serious cases of fraud. For instance: "An especially serious case typically occurs if the offender: 1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of forgery or fraud; 2. causes a major financial loss or acts with the intent of placing a large number of persons in danger of financial loss by the continued commission of offences of fraud.

Fraudulent activity has become a focal point for the UK government over the last 5 years. To reflect the increasing awareness of the problem, new legislation has been passed and new monitoring bodies have been formed to try to counteract the increasing number of cases of fraud. There is no single definition of fraud in the UK, but rather categories or types of fraud whose definitions can be extended to cover a variety of scenarios. Civil and criminal fraud in the UK consists of an act of deception, intended either for personal financial or proprietary gain or to cause financial or proprietary loss to another. The Fraud Act 2006, which is the starting point for the definition of fraud in the UK, brought in a new definition of fraud under three "umbrella" categories (which may be committed by individuals or companies): dishonest deception by knowingly

making a false representation, dishonest failure to disclose information and dishonest abuse of a position of responsibility. Most types of fraud in the UK will fall under one of these headings. The Fraud Act also establishes certain specific types of fraud which may not fit easily into the above categories. These include: possession of articles (including electronic data and programmes) for fraudulent use, manufacturing of such articles, obtaining services dishonestly (Okpara 2009). Other types of fraud are identified in other legislation and case law. It is not difficult to show that the actual transactions or acts involved in fraud have actually occurred (for example, that money has changed hands or a document has been tampered with). The difficulty in UK law arises in that fraud must involve both dishonesty and intent to either make a gain or cause a loss (which must be a gain or loss in terms of money or other property). These are essentially subjective classifications and are therefore difficult to justify objectively. When this is combined with the high burden of proof required for criminal fraud (the intent must be established beyond all reasonable doubt), then fraud can become difficult and expensive to establish (Sharma 2003; Agwu 2013).

Fraudsters have become ever more sophisticated, which means that fraud prevention measures need to constantly evolve to ensure they are capable of handling the threat (Agwu 2014). Lending institutions have to be able to check the validity of documents, verify the information supplied to them by applicant borrowers and detect inconsistencies.

Previous Literature: Types of Fraud

The symptoms of poor internal controls (Agwu 2013) increase the likelihood of frauds in bank branches. *Internal control symptoms* include a poor control environment, lack of segregation of duties, lack of physical safeguards, lack of independent checks and balances, lack of proper authorizations, lack of proper documents and records, the overriding of existing controls, and an inadequate accounting systems.

Bologna (1994) cites the environmental factors that enhance the probability of embezzlement, they are: inadequate rewards; inadequate internal controls; no separation of duties or audit trails; ambiguity in job roles, duties, responsibilities, and areas of accountability; failure to counsel and take administrative action when performance levels or personal behaviour fall below acceptable levels; inadequate operational review; lack of timely or periodic review, inspections, and follow-up to assure compliance with company goals, priorities, policies, procedures, and governmental regulations and failure to monitor and enforce policies on honesty and loyalty.

Identity Theft – This is when hiding one's own identity by using the identity of somebody else through a nominee (white horse). In most cases in Nigeria (Agwu 2014), it is the source of identification (voter's card, driver's license, or international passport) that is usually counterfeited). Of the most broadly defined of the three types of online banking fraud; identity theft gets the most attention from the media and is of highest concern to consumers. Identity theft can be very simple or quite complex, as these examples illustrate:

- A collection agency calls and tells a customer that she owes $5,000 in credit card debt. After doing some research, the customer finds that her identity was stolen and that the thief opened several credit card and checking accounts at different banks, passed bad checks, and accessed her online account and transferred the money out via bill pay.
- A customer receives a returned check notice in the mail and contacts customer service to find that his account was debited $1,350 via an electronic check. Research reveals that someone obtained his checking account number (perhaps an identity thief spotted the number in the grocery store) and then used the account number to make purchases through the internet.
- A customer has all of her savings withdrawn because someone in her doctor's office had a similar name and obtained access to her confidential data. Once the identity thief got the information, he or she depleted the victim's funds by transferring them into a new account and then withdrawing from that account.

Identity theft can be extremely difficult for its victims. It can take months or even years to correct the damage it can cause (Agwu 2013). If the thief has acquired enough information to satisfactorily answer the questions asked by the financial institution, he or she will be able to use the information to commit fraud. Because the level and types of questions asked can determine whether or not an identity theft succeeds, those questions must be crafted so that only the true person will know the answers (Sharma 2003).

Friendly Fraud – This kind of fraud, also known as "civil fraud" or "family fraud," refers to fraud committed using information that belongs to a trusted friend or family member. As much as financial institutions, independent organizations and the media communicate to consumers that they should not share confidential data, many people do share their information with close friends and family. A growing number of identity theft cases indicate that some close friends and family members will pretend to be the customer and steal from that individual (Bhasin 2007). These are very time-consuming cases to research, but they can present a lower risk to the institution if the case is referred back to the customer to handle in a civil (rather than criminal) manner. Because it can be devastating to an individual to learn that he or she has been deceived by a close friend or family member, these cases can be especially difficult for victims; here are some examples of how friendly fraud occurs:

- A customer calls the financial institution's call center because he can't access his account online. While the call center representative is talking with him, the representative can see someone is accessing the customer's account on the Internet. When the representative asks if anyone might know his password, the customer explains that he shared it with his daughter; the password is the same as his ATM password, which he had given to her so she could withdraw money. It turns out that the daughter just left home, not on good terms, and took all of her father's money.

- A customer calls the call center to inquire about her account, and finds that her soon-to-be ex-husband has transferred all of the funds out of her individual account into the joint account using her online user ID. He then went into the branch and withdrew the money from the joint account. The husband disappears with her money.

The strongest defense against this type of fraud is to emphasize to customers the importance of keeping their passwords completely confidential (Haugen and Selin 1999; Agwu 2012). If a customer wants a trusted friend or family member to have access to his or her funds, the customer should add that person to the account. If the customer does not trust the person enough to do that, and wants to give someone money, the customer should withdraw the money personally.

Internal Fraud – this is:

- Based on the relation of the perpetrator to the bank, fraud is classified as external (perpetrated by a customer or other third party) or internal (perpetrated by staff or management). In the case of collaboration of internal and external parties, fraud is classified as internal.
- Based on the objective and intention, it is classified as credit (the objective is to obtain finance; the intention is not to pay) or theft (the objective is to steal; the intention is never to pay).
- Based on the number of fraud cases per perpetrator or group of perpetrators, fraud is classified as single (one fraud per perpetrator; no relation to other frauds) or multiple (organized attack; several frauds linked to one perpetrator).

This type of fraud is not new, but online banking has added another channel through which an employee can steal. If a financial institution allows employees access to customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud. Because of this, financial institutions should require a password or PIN for online banking, and the password or PIN should be stored in an encrypted format. Another option is to truncate account numbers and customer data and limit employee access to the full numbers. Of the three types of fraud, internal fraud can be the most costly to financial institutions.

Cash and Cheques

Most organizations have procedures to safeguard cash, yet those procedures are often ignored where cheques are concerned. Despite a reduction in cheque usage following the transition to electronic fund transfer payments, ATMs, Internet Banking services, Mobile Banking, etc, within the Nigerian financial institutions, misappropriation of cheque receipts and cheque payments remains a problem (NDIC 2011). Most cheque theft occurs within the postal system. However, larger-scale cheque fraud can also occur inside organizations where bank reconciliation processes are weak and there is inadequate segregation of duties. It is on record that the vast majority of financial

organizations around the world have at least some specific fraud prevention measures in place.

Others include but not limited to:

- Money Transfer Fraud
- Clearing Fraud
- Account Opening Fraud
- Advance Fee Fraud
- Forged Cheques
- Cheque Kitting
- Counterfeit Securities
- Letter of Credit Fraud

Based on the scheme used, the following types of fraud are recognized:

A. Falsified information or forgery meaning falsehoods or false information. Forgery is used to gain a benefit, which would otherwise not be reached. In most cases, the false information presented to the banks with the aim of being granted loans, is the declaration made by the employer of the salary earned by the applicant, when the customer gets the salary in cash and not through the bank.

B. Collateral (price and/or other) manipulation. Namely, any manipulation with collateral such as inflated price, sale, non-existent collateral, 'bubble' financing, corrupted resale, etc. Appraisal companies that evaluate the collateral usually engage in this kind of fraud.

C. Theft of financial assets, namely stealing monetary funds belonging to the bank, such as cash, deposits, bonds, etc.

D. Theft of non financial assets, i.e. stealing non-monetary property of the bank (fixed assets, e.g. cars, etc).

E. Electronic fraud, i.e. unauthorized access, manipulation or disruption of systems, infrastructure or data, including denial of service attacks.
F. Plastic fraud. Card fraud or plastic fraud includes: all lost and stolen, counterfeit, not received mail, third party application fraud, invalid cards, etc. (Atherton 2010)

Major Causes of Fraud

Agwu (2013) categorized the major causes of fraud into institutional and environmental in nature. Within the institutional stratum, the author averred that the weakness of various structures within the financial institution sits squarely as an open sore to the daily slide in checks and balances and the application of stiff internal control measures expected of such an institution. And within the environmental strata, lie societal pressure and demands, and expectations. Bank staffs, or bankers as they are

called, are respected as money bags owing to the millions they earn as salaries, however, due to the positional differences; the annual packages often fall below expectations. Individuals concerned are much more interested in joining the class of the ''big boys'' within the society. This often led to involvement in nefarious deeds within the much respected financial institutions.

Selected Cases of Fraud in a Bank

Case 1

The branch manager (of a bank) initiated an application for an overdraft without the branch's customer's knowledge, being aware that the customer had a deposit, to be used as cash collateral. Additionally, the Personal Banker's password was known so as to proceed with the application. After the overdraft was made available in the customer's account, the branch manager compiled a transfer order, counterfeiting the signature of the branch customer, for transferring the amount of the overdraft into another customer's account to whom the branch manager had obligations. The transaction was easily performed by the branch's back office based on the transfer document with the counterfeited customer's signature. At the maturity date of this overdraft, the branch manager started another overdraft application with the scope of closing the previous one. The transaction was performed by using the password of the personal banker (for the overdraft application) and of the customer service manager (to transfer the amount) since the branch manager had no right to perform the above transactions. Then, to close the second overdraft, the branch manager again performed unauthorized transactions from another customer's account. The fraud was however, discovered when the last customer walked into the branch to withdraw the money and close his account and this was very devastating for the bank.

Case 2

A customer service employee performed unauthorized transactions from a customer's account by transferring amounts of money to his personal account (knowing that some of the customers were no longer alive). The transactions could be easily performed since no authorization was needed in the banking system up to a defined limit. Furthermore, some of these accounts were dormant and for their activation an override was required, which was formally given by the supervisor.

Case 3

A real customer applies for a loan, the loan is approved, but the customer is refused by the branch and the bank employee steals the funds.

Case 4

A non-material fraud case occurred, that is no bank losses occurred. Due to the target pressure for credit card products, bank employees started applications for credit cards on behalf of customers without customer awareness. They attached in the application system copies of the photocopied ID documents stored in the existing files of the

customers' current account, in order to have risk approval for the card limit. The 'fraud' was revealed when risk analysts interviewed the customers *via* phone. Even if the credit card limit had been approved, no loss would have occurred since the customers were unaware that they had been issued a card.

Case 5

A customer came to a bank to deposit a certain amount of money. Since the teller told him that the system was down, he gave the money on trust and came to the bank the next working day in order to sign the deposit slip. When the customer came to the bank, he noticed (verifying on the ATM) that the amount left on trust had only partly been deposited in his account. The customer asked for an explanation from the teller, who declared that she had his funds and immediately booked the difference. While the teller booked the difference into the account of the customer, she did not have all the funds in the cash box (she had used a part of them for personal purposes). Hence, the teller performed a withdrawal transaction from the account of another customer to cover the difference.

Fraud Management Processes

The fraud management process involves three steps: (1) fraud detection (2) fraud investigation and (3) fraud prevention. The best approach to fight fraud is to prevent it and prevention is mostly about improving the key risk processes.

Individual and Organizational Roles Given the sophistication, complexity and technicalities of cyber crimes, no sizeable organization can plan and implement the necessary responses alone. Information sharing is therefore extremely necessary amongst organizations. The telecom industry was deregulated in 1999-2000 (Agwu 2013). The internet appeals to all ages, ethnics, races and countries. The embrace of the internet, especially the social media networks by the youths and all comers and their naivety forms the basis for the widespread attack by these cyber criminals. Many users are unfortunately unaware of the different threats and dangers associated with the use of the internet. Most users often fall prey to some mouth watering adverts, emails, and websites and they end up leaving their personal details to the delight of these criminals. In the Nigerian context, it is on record that the solid foundation required for the introduction of such an innovation (internet technology) was never in place especially within the school curriculum, as ICT was not widespread in schools and colleges and even the universities. There is therefore an urgent need to create awareness about the different types of frauds.

Government's Role and Law Enactment Based on the Nigerian experiences and the extent to which this menace has dented the country's image in the international community, it is therefore imperative that the government takes a strong stance to curb its further growth and expansion. Unfortunately, no precise legal definition of fraud exists; many offences referred to as fraud are covered by the criminal codes. The term is used to describe acts such as deception, bribery, forgery, extortion, corruption, theft,

conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion (Atherton 2010; Agwu 2013). For practical purposes, and for this study, fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party.

The Nigerian Criminal Laws

Criminal Code Act 1990

The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form; it is an offence punishable under the Act. Although cyber crime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. The most renowned provision of the Act is Chapter 38, that deals with **"**obtaining Property by false pretences- Cheating." The specific provisions relating to cyber crime is section 419, while section 418 gave a definition of what constitutes an offence under the Act:

- (418) "Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence."

- (419)"Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years." (Part 6, chapters 34 &38, Laws of the Federation of Nigeria Act, 1990)

With the passage of time and the introduction of the internet which has culminated in the widespread use of emails as a method of soliciting money from the international community, it was observed that this was not covered within the law and perpetrators might always find a get-away clause, the government then came up with a commission with powers to arrest and prosecute offenders. The terms and conditions of this commission were widespread as explained below:

The Economic and Financial Crime Commission Act, 2004 (Source: National Assembly of Nigeria, 2004) The Economic and Financial Crime Commission Act (Laws of the Federation of Nigeria, 2004, as amended) provides the legal framework for the establishment of the Commission. Some of the major responsibilities of the Commission, according to part 2 of the Act, include:

- the investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.;

- the coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority;
- the examination and investigation *of* all reported cases *of* economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved;
- undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects *of* economic and financial crimes and advising government on appropriate intervention measures for combating same;
- Taking charge of, supervising, controlling, coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney-General of the Federation;
- the coordination of all investigating units for existing economic and financial crimes, in Nigeria;
- The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; the Advance Fee Fraud and Other Fraud- Related Offences Act 1995; the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended; the Banks and other Financial Institutions Act 1991, as amended; and miscellaneous Offences Act (EFCC, 2004)

Other Laws and Government Agencies Trade Malpractices (Miscellaneous Offences; Decree No. 67 of 1992(30); Although this Decree deals basically with those who sell things other than those which they have advertised, or those that have altered weights and measures to gain an unjust advantage over their customers, there is a section in this Decree that deals with another type of fraud similar to advance fee fraud. Where a foreigner ships goods to his Nigerian partners on trust and he is unable to collect his money back, he can successfully seek redress under this Decree.

Advance Fee Fraud and Related Offences Act 2006 (Source: National Assembly of Nigeria, 2006) According to Section 23 of the Advance Fee Fraud Act (Laws of the Federation of Nigeria, 2006): **'**False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.**'** Section 383 sub-section 1 of the Nigerian Criminal Code states: **'**A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing**'** (Advance Fee Fraud Act, Laws of the Federation of Nigeria, 2006).

The Nigerian Criminal Code (2007) described economic crime as " the non violent criminal and illicit activity committed with the objectives of earning wealth illegally, either individually or in a group or organized manner thereby violating existing

legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting, and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes and prohibited goods." However, Advance Fee Fraud and Other Fraud Related Offences Act 2006 is currently the only law in Nigeria that deals with internet crime issues, and it only covers the regulation of internet service providers and cybercafés, unfortunately it does not deal with the broad spectrum of computer misuse and cyber crimes. There are presently six bills on cyber crime being considered by the National Assembly (legislative arm) of Nigeria. These are:

- the Computer Security and Critical Information Infrastructure Protection Bill 2005,
- the Cyber Security and Data Protection Agency (Establishment, etc.) Bill 2008,
- the Electronic Fraud Prohibition Bill 2008,
- the Nigeria Computer Security and Protection Agency Bill 2009,
- the Computer Misuse Bill 2009 and
- the Economic and Financial Crimes Commission Act (Amendment) Bill 2010
- Money laundering (prohibition) Act, 2011

The lack of functional laws on which to base any form of arrest, trial and punishment presents an escape root for the perpetrators' of these crimes. It is however important to examine the actual role of the internet in the whole scheme.

Role of the Banks

The role of the banks should be to establish an anti-fraud culture covering working practices and business ethics culminating in formally documented procedures. A formal fraud policy statement indicates that the fight against fraud is endorsed and supported at the most senior level within the banks. Therefore, bank managers may wish to ensure that all employees are aware of a zero-tolerance attitude to criminal breaches of business practices which may be reported to the police. The fraud policy statement should be communicated to all employees, contractors and suppliers.

A Comprehensive Policy

In conjunction with an effective code of conduct, a comprehensive fraud control policy document should be distributed to all employees, who should be asked to sign a declaration that they have read and understood the policy requirements. The policy document should also set out other matters such as the responsibility for fraud control, employment screening, a fraud awareness programme, risk assessment programme, and the consequences of fraudulent action and/or withholding information concerning any such action. Such policies could be:

Policies and Principles The bank is committed to preventing fraud and corruption from occurring and to developing an anti-fraud culture. To achieve these, banks must comply with the requirements of government criminal codes to:

- develop and maintain effective controls to prevent fraud;
- ensure that if fraud occurs a vigorous and prompt investigation takes place;
- take appropriate disciplinary and legal action in all cases, where justified;
- review systems and procedures to prevent similar frauds;
- investigate whether there has been a failure in supervision and take appropriate disciplinary action where supervisory failures occurred; and
- record and report all discovered cases of fraud.

Further, the organization's policy should state clearly the intention to investigate suspicions and prosecute fraudulent acts. It should also explain the organization's rights in relation to such things as access to workplace email and computer systems and the intention to recover any money or property lost as a result of such action. It is therefore important for the employment of quality control staff in order to strengthen the internal control systems to be able to detect and prevent fraud and fraudulent activities and to protect its assets.

At the macro level,

- CBN and NDIC need to step up their supervision with the most sophisticated tools to appropriately checkmate; curtail and prevent the incidences of fraud and fraudulent practices within the Nigerian financial institutions.
- Furthermore, the Nigerian government should adequately empower all its established fraud fighting agencies namely, the Central Bank of Nigeria (CBN), Nigeria Deposit and Insurance Corporation (NDIC), Securities and Exchange Commission (SEC), National Insurance Commission (NAICOM), Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices Commission (ICPC), the Police, Judiciary, National Agency for Food, Drug Administration and Control (NAFDAC) and Standard Organization of Nigeria (SON), among others, should ensure the enforcement of various legal provisions in the fight against fraud in Nigeria.

Discussion

Fraud investigations are not like standard police-type investigations into criminal activity. This is because the majority of fraud investigations begin only with a mere suspicion that a fraud has occurred. In many cases, there is little initial evidence of that fraud, as the nature of most fraud is such that deception is involved in committing and then covering up the crime. However, it is also true that most frauds leave a trail, or a series of indicators which suggest a fraud has occurred. The key is to locate those indicators as early as possible in the investigation process. Fraud investigation resources generally fall into four categories or skill-sets as discussed above. In the majority of cases, most if not all of the banks are required to fully investigate a suspected fraud no matter how minimal.

Reputational Risks

This study dwelled on fraud and the risks it poses to banks reputations. In most cases, the reputations of the affected banks could nose-dive within a short period of time if fraud issues are not dealt with accordingly. There are several ways the reputation of a bank can be smeared and these could be:

- Loss of valued customers, some of whom might view the occurrences as signs that their money is not safe within the banks
- By extension, fraud cases might take its toll on staff turnovers, leading to loss of efficient and hardworking employees of various cadres. This will by extension lead to an increase in hiring, training as well as longer years of fitting into and understanding the system
- Business partners might also shy away from doing businesses with the concerned banks due to the smeared reputation from frauds.
- Some bright persons might shy away from applying to the banks in order to protect their reputations
- Therefore, reputational risk either wears away the bank's expected future cash flows or increases the market's required rate of return

Managerial Implications

In order to minimize the problem of fraud it becomes imperative to train bank staff in the prevention of bank frauds. It is also important to employ and train staffs adequately so that guidelines and instructions laid down by the banks can be strictly adhered to. The communication process between the manager and staff should be improved so that proper information about frauds is disseminated easily and quickly. The attitude towards bank procedures should be improved through proper communication channels. The bank employee should be educated as to why a particular procedure is followed and what can be the implication if it is not adhered to strictly. A policy of compulsory leave in a month should be introduced so as to unveil the unscrupulous deeds performed by corrupt officer. The personal life style of the employees should also be checked from time to time in order to see any discrepancy between their incomes and expenses. Signatures are always vulnerable to forgery and thumb impression should be introduced along with signatures. In relation to banking industry, there is need for greater sharing of information between financial institution on trends and practices of fraudster and fraud topologies, especially those frauds that are committed in computerized environments.

Conclusion

Fraud is a concept that is generally understood but whose characteristics are often not recognized until it is too late. The incidence of fraud has been on the increase since the global crisis all over in the world as well as in Nigeria. The economic cost of frauds can be huge in terms of likely disruption in the working of the markets, financial institutions, and the payment system. Besides, frauds can have a potentially debilitating effect on confidence in the banking system and may damage the integrity and stability of the economy. It can bring down banks, undermine the central bank's supervisory role

and even create social unrest, discontent and political upheavals. The vulnerability of banks to fraud has been heightened by technological advancements in recent times. Most fraudulent acts are perpetrated by employees who understand the internal operations at their workplace and take advantage of internal control weaknesses. The bank employees do not give due importance to the problem of frauds. The awareness level of bank employees regarding bank frauds is not very satisfactory, and majority of them do not dispose favourable attitude towards stipulated bank procedures as they find difficulty in following them due to workload and pressure of competition. Moreover employees are not well trained to prevent bank frauds. Training positively affects the compliance level of employees and improves the attitude towards bank stipulated procedures. In common with any crime prevention strategy, the key to minimizing the risk of fraud lies in understanding why it occurs; in identifying business areas that are at risk and implementing procedures addressing vulnerable areas. Combating fraud risk should therefore be a two-pronged approach. First, ensuring that the opportunities do not arise and, second, ensuring that the fraudster believes that he will be caught and that the potential rewards do not make the consequences of being caught worthwhile. With the aim of preventing fraud, the central bank should consider imposing regulations on the banks by enforcing their framework for fraud risk protection. To sum up, it is worthy to note that the advantages of technology, communication and accessibility of data must be leveraged to put in place a system wide fraud mitigation mission. Any house is only as strong as its foundation and as weather proof as its insulation. It is necessary, therefore, that a strong foundation is built by leveraging robust information technology systems, framing effective policies and procedures, laying down strict compliance processes, setting high integrity standards, developing efficient monitoring capabilities and initiating strict punitive action against the culprits in a time bound manner. It is also imperative that bank must insulate itself from unscrupulous activities by strengthening the fraud detection, mitigation and control mechanism through prompt identification, investigation and exchange of information. This is necessary not just for the safety of banks but for ensuring the stability and resilience of the overall financial system and sustaining the confidence that various stakeholders have in its strength and integrity.

Recommendations

Stiffer Internal Control Measures

Conduct periodic surprise audits and annual reviews of procedures.

- Provide for the physical security of all cheques
- Maintain cheque images in preference to paper copies
- Ensure appropriate security over signature plates, cards, and software.
- Require additional review process for all cheque over a specified amount.
- Ensure two party authorizations (initiation and release) on all transactions. Ensure proper segregation of duties among staff initiating, authorizing, preparing, signing, and mailing payments and reconciling bank statements.
- Review all bank accounts at least annually. Consolidate or eliminate bank accounts that are not frequently utilized.

- Ensure that controls exist for the storage and destruction of all documents that contain account and other related information.

➢ ***Managers Should be Responsible for:***

- Identifying the risks to which systems and procedures are exposed.
- Developing and maintaining effective controls to prevent and detect fraud.
- Ensuring that controls are being complied with.

➢ ***Individual Members of Staff Responsible for:***

- Acting with propriety in the use of official resources and in the handling and use of corporate funds whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers
- Reporting details immediately to (their line manager or next most senior manager) if they suspect that a fraud has been committed or see any suspicious acts or events.

Future Research

Future studies can focus on the evaluation of effectiveness of training programmes, procedures and measures in preventing frauds in computerized environment and rapidly changing Information technology. Identification of various psychological characteristics of potential offenders and the use of those results in formulating better recruitment and selection policies can be a focus for future research.

References

Albrecht, W.S. (1996). Employee fraud. Internal Auditor, October, p. 26.

Adogamhe, Paul G. (2010) ''Economic Policy and Poverty Alleviation: A critique of Nigeria's Strategic Plan for Poverty Reduction'', *Poverty and Public Policy*: Vol. 2: Iss. 4, Article 4

Agwu, E. (2012) Generations X and Y's adoption of internet and internet banking in Nigeria: a qualitative study, *International Journal of Online Marketing*, 2 (4): 68-81.

Agwu, E.M. (2013) Cyber criminals on the internet super highways: A technical investigation of different shades and colours within the Nigerian cyber space - *International Journal of Online Marketing, 3(2): 56-74.*

Agwu, E. M. (2014). An investigative analysis of factors influencing E-business adoption and maintenance of commercial websites in Nigeria; *Basic Research Journal of Business Management and Accounts ISSN 2315-6899 3(1): 05-16 Available online http//www.basicresearchjournals.org*

Akpoyomare, O. (1996). The Use of Management Control Strategies in Defection and Prevention of Fraud. *The Nigeria Management Review*, 10 (1): 68-69.

Almogbil, A. (2005). Security, Perceptions, and Practices: challenges facing Adoption of Online Banking in Saudi. Unpublished Ph.D. Thesis, George Washington University, Washington

Atherton, M. (2010) Criminals switch attention from cheques and plastics to internet transactions. *The Sunday Times* of March 10, 2010.

Berger, H.S. and Gearin W.F. (2004). Due diligence: two important words for all those who wear the white hats. RMA Journal, Oct.

Bhasin, M. (2007). The Bank Internal Auditor as Fraud Buster. The ICFAI Journal of Audit Practice, 4(1).

Barnes, R.W., (1995). The value of quality education to banks and bankers. The Journal of Indian Institute of Bankers, 66(3): 55-59.

Banking Division, Ministry of Finance: File. No.18/9/2005/Vig.)

Bologna, J. (1993) Handbook on Corporate Fraud, Butterworth-Heinemann, Stoneham, MA.

Bierstaker, J. Brody, R.G. and Pacini, C. (2006). Accountants" perception regarding fraud detection andprevention methods. Managerial Auditing Journal, 21(5): 520-535.

Bologna, J.G., (1994). How to Detect and Prevent Embezzlement? *The White Pap*er, August/ September, p 4.

Calderon, T. and Green, B.P. (1994). Internal Fraud Leaves its Mark: Here's How to Spot, Trace and Prevent it.

CBN (2009) ''Economic Report for the Fourth Quarter of 2009'' Vol. 4, Issue 4, December 2009. Abuja, CBN Collier, P. & A

Commercial Angles Newsletter.(2001). Fraud Prevention. July, available at www.commercialangles.com/articles/fraud_control.htm.

Ekenna, G. (2003). Nwude, wealthiest "419" kingpin in the net. New Watch, May 6. 2003. Available online at http://admin.corisweb.org/index.php. Accessed 16/11/2009

Fagbemi, O.A. (1989). *Fraud in Banks*: *The Law and the Legal Process*. Lagos, FITC.

Ganesh, A. and Raghurama, A. (2008). Status of training evaluation in commercial bank- a case Study. Journal Of Social Sciences And Management Sciences, XXXVII (2): 137-58.

Geer, D. (2003). Security: Risk management is still where money is. *IEEE Computer Societ*y, 36(12): 129-131.

Haugen, S. and Selin J.R.(1999). Identifying and controlling computer crime and employee fraud. Journal: Industrial Management & Data Systems, 99 (8): 340-4.

Jeffords, R.; Marchant, M.L. and. Bridendall, P.H. (1992). How Useful are the Tread Way Risk Factors? *Internal Auditor*, June, p. 60.

Mitra, N.L., (2001). The Report of Expert Committee on Legal Aspects of Bank Frauds.

Nigerian Deposit Insurance Scheme (NDIC) Annual Reports and Statement of Accounts (Various Issues) (2008-2011)

Nwankwo, G.O. (1992). *Banking Fraud*. Lecture delivered at the 5th Anniversary of Money market Association of Nigeria.

Nwaze, C. (2006). *Bank Fraud Exposed with Cases and Preventive Measures*. Lagos: Control and Surveillance Associates Ltd.

Ogbu, C (2003) Banks Lose N13 billion To Frauds, *The Punch*, Vol.17, No. 18860.

Ojei, A. (2000): "Frauds in banks", A paper presented at the effective bank institute course organized by FITC, Lagos

Ojo, A. (2006). *Curbing Fraud within the Banking System*:*A banker's Perspectives*. Lagos: A.M. Continental Ltd.

Okpara, G.C. (2009) ''Bank failure and persistent distress in Nigeria: A Discriminant Analysis". *Nigeria Journal of Economic and Financial Research*. 2 (1).

Olasanmi, O.O. (2010) Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Journal of Internet Banking and Commerce*, 15 (1): 1-10. Available at: http://www.araydev.com/commerce/jibc Accessed January 29, 2014

Oyelola, O. (1996): Internal control and management of frauds in the banking industry, a paper presented in ICAN mandatory continuing professional education programme (MPCE) Seminar

Who, O. (2005). *Bank Frauds, Causes and Prevention: An Empirical Analysis*. Ibadan: ATT Books Ltd.

Sharma, B.R.(2003). *Bank Frauds- Prevention & Detection*. Universal law Publishing Co. Pvt .Ltd.

Sharma, S. and Brahma (2000) *A Role of Insider in banking Fraud*. available at http;// manuputra .com

Slewe, T., & Hoogenbom, M. (2004). Who will rob you on the digital highway? Traditionally at the forefront of security awareness, financial organizations must maintain this status as they move further into the internet realm. *Communication of the ACM*, 47(5): 56-60.

mith, E. R. (1995). A Positive Approach to Dealing with Embezzlement. *The White Paper,* August/September, pp 17-18.

Soludo, C.C. (2006). The Outcome of Banking Sector Recapitalization and the Way Forward for the Undercapitalized Banks. *Central Bank of Nigeria, Press Conference.*

Transparency International (2011) Corruption Perception Index; Retrieved February 17, 2014 from http://www.transparency.org

Willson, R. (2006).Understanding the offender/environment dynamics for computer crimes. Information Technology and people Vol, 19, No.2, pp170-186.

Ziegenfuss, D.E. (1996). State and Local Government Fraud Survey for 1995. *Managerial Auditing Journal*, 9: 49.