Combating insider fraud in Financial Institutions/impact

[1]DR Yaya Itai [2]Emmanuel Onwubiko

[1]Non-Executive Director at ITAIN Bell School Ikeja Lagos Nigeria, [2]Ojo LGA of Lagos State Nigeria

yaya591@yahoo.com, emmadesaint@yahoo.co.uk

Abstract

The fear of fraud is constant. Unfortunately, now more than ever before, fraud is being committed by employees on the inside, the very people who are supposed to be supporting and protecting an organization. Even though the financial industry is one of the most regulated, financial institution are still getting with the highest rate of internal fraud. Insider threat has always existed within each Financial Institution. In the recent years, insider threat has become a more prominent issue because of the emerging trends in the workplace. This change to a more flexible and productive workplace environment allows employees to easily gain access to an organization's critical and sensitive information. While the risk of insider threat has certainly increased, Financial Institution have not deployed enough controls to mitigate this risk either because they believe that the frequency of such threat is very low or because they feel powerless to do so.

This paper tends to employ techniques that would abate the spate of Insider fraud and cybercrime on customer transactions and insider processing which is in full compliance with most regulatory mandate of Countries Government bank.

Keywords: Insider threat, Insider fraud, Incidence response, Log, Monitor, Crime.

1.0 Introduction

Black law Dictionary (6th Edition, 1990) defines fraud as "An intentional perversion of truth for the purpose of inducing another relying upon it to part with some valuable thing belonging to him or to surrender a legal right. A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegation or by concealment of that which deceives and is intended to deceive another so that he shall act upon it to his legal injury. Anything calculated to deceive, whether by a single act or a combination or by suppression of truth or suggestion of what is false whether it be by direct falsehood or innuendo, by speech or silence, word of mouth, look or gesture."

This definition has not changed, rather fraud has become sophisticated and IT driven which makes its detection more arduous.

Fraud in the banking sector is estimated at billions of naira annually, and diverts resources from organization's profitability objectives as fraud losses reduce the amount of profit that would otherwise be available to shareholders. Fraud also undermines public confidence in banks as losses could be of monies belonging to bank's customers. Fraud losses can also impact negatively upon staff morale as the benefit of value created by dedicated and hardworking staff is lost to fraud incidents. Fraud impair the bank's financial health and constrains its ability to carry out its business of lending and investment, and in extreme instances, fraud losses can lead to insolvency. Financial institutions are now committed to ensuring probity and accountability to its shareholders, customers, and employees, by building a positive organizational culture that deters, prevents, promptly detects, investigates and takes steps to correct deficiencies that could lead to fraud.

Insider fraud is perpetrated by a malicious insider, which is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality. Essentially, insider fraud takes place when someone uses his/her position within an organization

to steal money or information and/or to threaten security, insider fraud is "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

Perpetrators are often employees or contractors who gain access to data and use it to commit fraud. Unfortunately, because these people have usually been screened during the employment process and "vetted" by the organization, they've been given access to important information as part of their job, so it's more challenging for companies to catch.

Insider fraud are costliest and hardest to detect of all data breaches Jasmine Henry (2018). Two-thirds of total data records compromised in 2017 were the result of inadvertent insiders, according to "2018 IBM X-Force Threat Intelligence index," and insider threats are the cause of 60 percent of cyberattacks. Meanwhile, misconfigured cloud servers and networked backup incidents caused by employee negligence collectively exposed over 2 billion records last year.

While organizations focus significant resources on the mitigation of external threat actors, insider risks are likely to pose an even greater financial threat to the enterprise. According to Ponemon Institute's "2018 Cost of Insider Threats" report, the average cost of insider-caused incidents was $8.76 million in 2017 — more than twice the $3.86 million global average cost of all breaches during the same year.

Accordingly, to Jasmine Henry (2018), Traditional approaches to managing insider threats have focused extensively on the use of awareness training and access governance to reduce risks. While these activities are critically important, they're likely not enough to mitigate all types of employee risk. Humans are enormously variable, and failing to account for all types of insiders could result in costly security incidents.

1.2 Type of Insider Fraud

Insider fraud can take place in almost any organization, but two industries where it's common – and highly damaging for both employers and consumers – are **banking and insurance**. In these organizations, employees have access to extremely sensitive and personal data, including customers' social security numbers, account information, driving and criminal records, etc., which can lead to identity theft and the loss of funds.

- **Nonresponders:** A small but significant percentage of the employee population is made up of nonresponders to awareness training exercises. While these users may not intend to behave negligently, they're among the riskiest members of the population since their behaviors can fit consistent patterns. In 2017, Verizon found that an average 4.2 percent of people targeted in any given phishing campaign will click the malicious link. Individuals with a strong history of falling prey to phishing campaigns are most likely to be phished again. While employees who consistently behave in insecure ways are generally a minority of the populace, the total impact of employee mistakes is staggering. Ponemon research found that 63 percent of incidents recorded last year were caused by all categories of negligence.

- **Inadvertent**: Simple negligence is the most common form of insider threat, and also the single most expensive category of employee risk. Insider threats who fit this category might generally exhibit secure behavior and comply with policy, but cause breaches due to isolated errors. Basic misjudgment — such as storing intellectual property on insecure personal devices or falling for phishing schemes — caused two-thirds of breached records in 2017, according to the X-Force report. Threat actors are increasingly savvy to the vulnerabilities caused by inadvertent insiders. X-Force analysis of the most common criminal tactics used to exploit employee error

- **Insider Collusion**: Insider collaboration with malicious external threat actors is likely the rarest form of criminal insider risk, but it's still a significant threat due to the increased frequency of attempts by professional cybercriminals to recruit employees via the dark web. Fraud rings tend to be highly sophisticated and organized and may embed their members in a number of roles within a bank. A fraud

ring may seek to place a member in Human Resources, for instance, to make it easier to get members hired as loan officers, tellers … or even loss prevention officers. Or knowing that the collections department has a weak background screening process and broad access to customer information, a fraud ring may try to place one of its members there solely to steal customer data.

- **Disgruntled Employees**: As a final category of criminal insiders, disgruntled employees who commit deliberate sabotage or intellectual property theft are also among the costliest risks to an organization. The Gartner analysis of criminal insiders found 29 percent of employees stole information after quitting or being fired for future gains, while 9 percent were motivated by simple sabotage. Disgruntled employees can fit many behavioral sub-patterns. Some frustrated employees may start digging for information access without specific goals. Other employees may have very specific data intent from the moment they give two weeks' notice, and set out to sell trade secrets to competitors.

- **General Ledger Fraud** Insiders may take advantage of the fact that while many employees have working knowledge of the accounts they access daily, they are often unfamiliar with other parts of the general ledger accounts. Certain insiders may have exclusive access to accounts payable or suspense accounts, which are used to temporarily record items such as loans in process, interdepartmental transfers, or currency in transit.

- **Account-Takeover**

Account takeover is another common internal fraud scheme, and often involves employees acting in collusion with outsiders for instance, a bank employee may open a deposit account for a customer and later set up online banking on the account without the customer's knowledge. The employee may then make unauthorized withdrawals from the account or give the online credentials to an external fraudster, who can use them to siphon money out of the account. In another scheme, the employee may sell a customer's PIN and account number to an external fraudster, change the address for the account and request a new check card.

1.3 Impact on Insider Fraud

According to Dr. Mike Gelles, a director with Deloitte Consulting, many financials today agree that insider fraud threat have a very high impact, but at the same time, believe that the likelihood of occurrence is very low. Thus, managing insider fraud threat does not become a priority for many organizations today. On the other hand (Blades M,2010) some security professionals, such as chief security officers, do recognize the importance of protecting against this type of threat but feel that insider threat is too difficult to manage. CSOs feel powerless to defend against insider threats because insiders can access the network without passing through the perimeter. The attacks are planned much in advance which allow them to cover their tracks and these insiders act based on a wide range of motivations that may be hard to predict. Since insider attacks are much more targeted because they know where the information is located, these attacks are likely to impose a greater impact compared to external attacks. As we can see from the growing number of insider threat incidents (Jennings, Frank 2008), such attitudes that organizations have against insider threats are no longer permissible. In fact, the 2010 Verizon Data Breach Investigations Report along with other studies concluded that it is costlier to fix insider attacks compared to external attacks.12 This is also confirmed by the e-crime Survey and Ponemon Institute's 2010 Cost of Cyber Crime Study. Therefore, it is critical for organizations to shift their mindset towards implementing a plan that will proactively prevent and detect these insider attacks (Kaplan, D 2011).

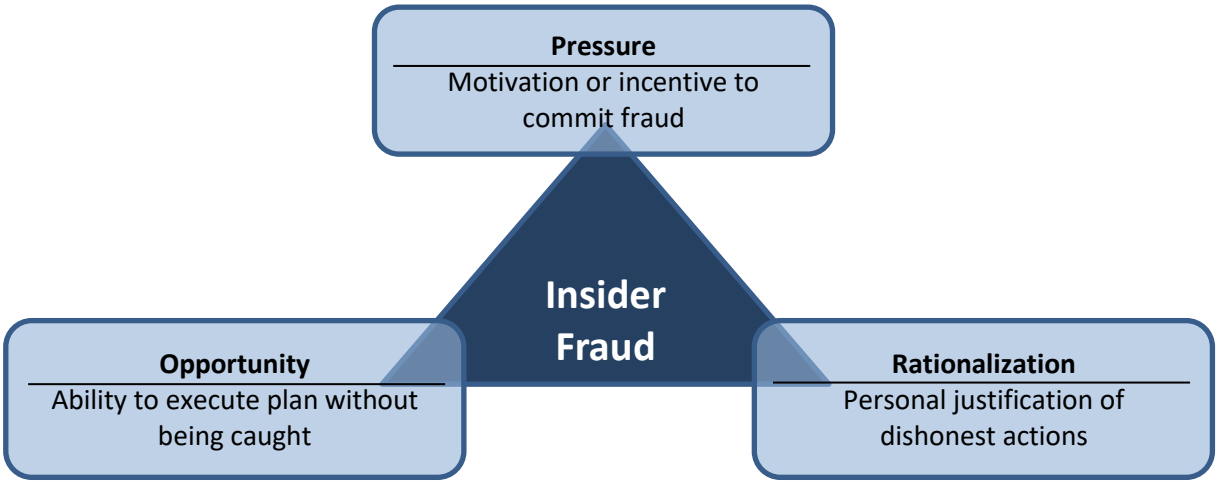
The impact of Insider Fraud on financial Institution could include the following:

- Loss of resources (financial, staffing and other assets);
- Reputation and brand damage;
- Negative organizational culture;

- Damage to financial Institution relationship with partners and stakeholders;
- Disruption to service delivery;
- Investigation costs; and Recruitment, retention and morale issues.

1.4 Insider Fraud Policy

The Insider Fraud Policy outlines how Financial Institutions will manage the risk of around Insider fraud. In minimizing incidents of fraud, Financial Institutions takes into consideration the three elements of the fraud triangle as shown below. The emphasis of the Insider Fraud and policy is the reduction of opportunities to commit fraud. Additionally, Financial Institutions policies and procedures as it relates to staff welfare shall also aim to minimize the pressure and rationalization elements.



1.5 Risk Mitigant Approach to Insider Fraud Management/Handling

Financial Institution approach to Insider fraud risk management is to develop a corporate anti-fraud culture and to prevent fraud by designing, implementing and continuously reviewing policies and systems that aid the achievement of these objectives. This is further supported by the Financial institution work to detect and investigate fraud and to seek to apply sanctions and as much as possible, recover losses arising therefrom.

The Insider Fraud Risk Mitigant Approach shall combat the risk of fraud by:

- Awareness and training;
- Deterrence, prevention, detection and correction;
- Investigation;
- Log, monitor, and audit employee online actions.
- Restrict access to personally identifiable information
- Develop an insider incident response plan.
- Sanction

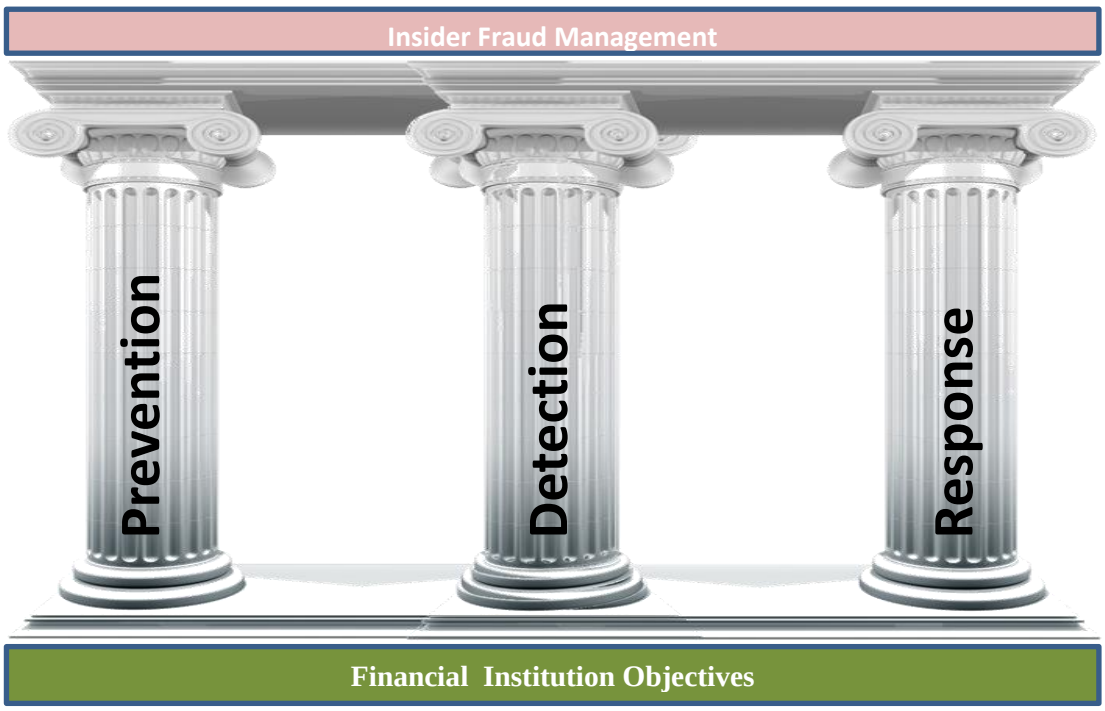
- Prosecution
- Recovery of losses.
- Implementation of behavioral monitoring systems

Awareness and training;

Financial Institutions are now committed to ensuring that staff and management are aware of their responsibilities with regards to preventing fraud. To this end, the Financial Institutions will ensure that there is an on-going training programme for staff regarding measures to minimize the risk of fraud. The Financial Institutions also recognizes that it is exposed to risk from external partners and suppliers or third parties working for or on behalf of the Financial Institutions. To this end, the Financial Institutions will ensure there is an on-going programme of awareness to ensure external partners and suppliers are aware of the Financial Institutions commitment to protect its funds against fraud. The Financial Institutions will continually utilize lessons from past experiences in fraud cases or attempted cases to build its knowledge management system, sharing same and using it for robust awareness campaigns.

Deterrence, prevention, detection and correction;

Financial Institutions should recognize that the most efficient way to protect its assets is to undertake a scheduled plan of prevention work. This plan will include a programme of work directed at deterring fraud. It will also include Insider fraud assessment work which will form part of the Insider Fraud annual routine process. The Fraud Prevention Plan shall be the responsibility of Key stakeholders and shall form an integral part of the Financial Institution fraud risk management, and shall include targeted deterrence, prevention, detection and fraud risk actions. Corrective actions are taken based on lesson learned from fraud cases to prevent reoccurrence.



Investigation

Financial Institutions are committed to investigating all suspected occurrences of Insider fraud. The Financial Institutions will undertake all investigations pursuant to the Insider Fraud Policy and Response Plan contained in this manual and other relevant protocols.

Log, monitor, and audit employee online actions.

Enforce account and password policies and procedures to associate online actions with the employees who performed them (Douglas Maughan 2012). Use logging, periodic monitoring, and auditing to discover and investigate suspicious insider actions early. Use data-leakage tools to detect unauthorized changes to systems and the download of confidential or sensitive information, such as intellectual property, customer or client data.

Restrict access to personally identifiable information.

Do not allow employees to accumulate privileges over time from moving across projects, between departments, or from taking new positions (Douglas Maughan 2012).. Ensure that employee privileges are necessary for their current job responsibilities. Protect PII from unauthorized access and establish controls that alert the proper personnel when PII is accessed, modified, or transmitted.

Develop an insider incident response plan.

Develop an insider incident response plan to control the damage that results from malicious insider activity. Ensure that only those responsible for carrying out the plan understand and are trained on its execution (Douglas Maughan 2012). If an insider is suspected of committing fraud, ensure there is evidence in hand to identify the insider and follow up appropriate

Sanctions

Financial Institutions are committed to pursuing all possible sanctions for proven cases of fraud. The Financial Institutions shall pursue disciplinary, civil and criminal sanctions where there is evidence to support the occurrence of fraud. These sanctions will be sought on a case by case basis pursuant to the Bank's Anti-Fraud Policy and Response Plan which shall provide guidance on the appropriate level of investigation of suspected cases. Sanctions shall be applied where applicable to the Financial Institutions staff in line with the Disciplinary Policy.

Recovery of Loses

The Financial Institutions is committed to minimizing potential losses due to fraud, and in cases of suspected fraud, take action to minimize the risk of further loss by recovering any funds lost due to fraud in line with the provisions of the Financial Institutions Insider Fraud Policy and Response

Implementation of behavioral monitoring systems

Conceiving the increasing number of insider fraudulent activities associated with the financial employee; the need to define a possible control to check the growing threat necessitated the Financial Institutions to upscale its controls to monitor the increasing number of customers' accounts and internal employee activities on the core application of every Financial Institutions. To this end, the Financial Institutions are expected to engage an Enterprise Fraud Management vendor to provide an all-encompassing solution designed to monitor customer accounts, employee activities on core application, improve efficiency, and reduce insider frauds.

The Enterprise Fraud Management system engine should have rules library, business Rules/logic evaluations that analyzes the bank's information (transaction, profiles and, reference data) using statistical calculations and machine learning capabilities such that when the rule conditions/set patterns are met, an exception incident is

generated and circulated to the assurance functions in Financial Institutions. The alerts are immediately acted on to abort fraudulent intents / safeguard the interests of the Financial Institutions.

Some suggested business scenario recommended for Financial Institutions,

1. Account has excessive transactions of a certain category involving the same internal account (e.g. accounts with excessive credits from dormant accounts or internal accounts)
2. Employee performs an irregular activity compared to employees with the same role type (e.g. teller posting foreign currency,
3. Employee performs an irregular activity compared to employees with the same role type e.g. teller debiting into income accounts and expense accounts)
4. Employee's related account has a monetary transaction in a certain category in an account that is not related to the employee (e.g. other inflows apart from salary)
5. Employee's related account has a deposit with an above average amount for the category
6. Employee performs an excessive number of withdrawals on a customer's accounts over the past day
7. Employee changes the phone number on their related customer
8. Employee performs fee reversal(s) on their related account
9. Employee performs refund(s) on their related account
10. Account has excessive transactions in a certain category that meet certain conditions.

1.6 Contribution to the Knowledge

The paper will contribute to the body of existing knowledge through the following ways: The paper contributes to the existing knowledge by expressing the views of different academic scholars with the regards to the Risk Mitigant Approach to Insider Fraud Management as such the paper may serve as a source of academic literature. The study will help the forensic accountants, auditors, fraud examiners and other anti-fraud bodies to understand the insider fraud management techniques thoroughly and approaches recommended, which will assist them in identifying and investigating the remote cause of fraud concealment and effective assessment of fraud risk. The paper may serve as guidance for further research to be carried out on the subject matter in areas that the study did not address.

1.7 Conclusion

To tackle insider fraud, financial Institutions must be sure that they understand their first responsibilities are to protect the privacy of their employees and the integrity and confidentiality of their corporate data. The global economy is becoming increasingly predicated on the storage and leverage of intangible assets, so organizations must go to great lengths to protect their data.

Furthermore, by creating an inclusive culture of security and compliance that considers all aspects of the firm's leadership, financial Institutions will set themselves on the right path. But they must do more. Technology solutions that will complement internal risk mitigation can be invaluable; biometrics such as fingerprint scanning should be explored and implemented if feasible. financial Institutions should also ensure that concepts such as the 'principle of least privilege' are enforced across their entire workforce to ensure that employees or users are given access to the minimum amount of data access to be effective at their roles. Multi-factor authentication

processes should also be enabled. As the insider threat level rises, financial Institutions need to be more proactive

References

1. Hoyer, S., Zakhariya, H., Sandner, T. and Breitner, M. H. (2012) Fraud Prediction and the Human Factor: An Approach to Include Human Behavior in an Automated Fraud Audit, 45th Hawaii International Conference on System Sciences Proceedings, IEEE Computer Society, 4-7 January 2012, Grand Wailea, Maui, HI, USA

2. CPNI: CPNI insider data collection study – report of main findings. http://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_ data_collection_study.pdf (2013)

3. Salem, M., Hershkop, S., Stolfo, S.: A survey of insider attack detection research. In Stolfo, S., Bellovin, S., Keromytis, A., Hershkop, S., Smith, S., Sinclair, S., eds.: Insider Attack and Cyber Security. Volume 39 of Advances in Information Security. Springer US (2008) 69–90

4. Glasser, J., Lindauer, B.: Bridging the gap: A pragmatic approach to generating insider threat data. IEEE Symposium on Security and Privacy Workshops (2013

5. Hunker, J., Probst, C.W.: Insiders and insider threats – an overview of definitions and mitigation techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2(1) (2011) 4–27

6. Blades, M. "The Insider Threat." Security Technology Executive. 1 Nov. 2010: ABI/INFORM Trade & Industry, ProQuest. Web. 25 June. 2011

7. Jennings, Frank. "Beware the Enemy Within." SC Magazine. Jul. 2008: Business Source Complete.

8. Kaplan, D.. "Internal Review." SC Magazine. 1 Feb. 2011: ABI/INFORM Trade & Industry, ProQuest.

9. Cappelli, Dawn, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeall. "Common Sense Guide to Prevention and Detection of Insider Threats." CERT, Jan. 2009. Web. 20 June 2011.

10. High Tech Crime Investigation Association http://www.htcia.org/

11. Department of Justice Cybercrime Information http://www.usdoj.gov/criminal/cybercrime/searching.html

12. "Monitoring Employee Computer Use v. Privacy." HR Compliance Insider. 2010. Web. 30 June 2011..

13. Baker, Neil. " Big Brother doesn't always know best." Director. 2006: Business Source Complete. Web. 26 June 2011..