CARD International Journal of Management Studies, Business & Entrepreneurship Research
ISSN: (Print): 2545-5907 (Online): 2545-5885
Volume 2, Number 4, December 2017
http://www.casirmediapublishing.com

Employee Fraud Methods in Electronic Accounting Systems (Issues and Challenges)

Nwadighoha Chinedum Ephiraim

Department of Accounting
Michael Okpara University of Agricultural Umudike, Abia State
E-mail: Chinedumnwadighoha@yahoo.com

ABSTRACT

Certain factors in the corporate culture can increase the likelihood of theft including poorly compensated employees, excessive pressure on employees to perform, a hostile work environment, corporate financial troubles, and negative examples from top management. Consequently, the study is aimed at investigating employee fraud methods in electronic accounting system. A population of 214 corporate organizations in Nigeria was chosen and non probability sample was applied to use the same 214 corporate organizations as the sample size. Ordinary Least Square (OLS) Regression Analysis was used to test the hypotheses with the aid of Durbin Waston F. Statistic model. The following findings were discovered, that the employee Fraud methods (EFM) coefficients of 3.811e-5 indicates a positive relationship with employee methods of theft (EMT) is not statistically significant and hence, the following recommendations were made, all employees must be assigned password for their log in, the audit trail must be regularly and promptly reconciled and staff users should not be allowed to have access to other staff data for their own work except the data that are relevant to their own functions.

Keywords: Employee Fraud Methods, Electronic Accounting System, Direct File Alteration, Program Alteration, Data Theft and Employee Sabotage.

INTRODUCTION

In electronic accounting systems, employee frauds tend to involve attack against the computers and computer databases. These attacks can be classified into five categories: input manipulation, direct file alteration, program alteration, data theft, and sabotage.

This study focuses on employee fraud within the context of computerized accounting systems. Various computer- related frauds deserve special attention because the nature of computerized system is such that frauds can completely by pass standard controls or destroy, eliminate, alter or obscure the audit trail related to the fraud. In other words, the principles discussed here for identifying employee fraudsters are very critical. For this reason, the forensic accountant must not only understand individual fraud schemes but also be able to recognized and deal with situations in which there is a compromised audit trail of course, not all computerized attacks compromise the audit trail, but the forensic accountant needs to recognize when they do and when they do not. The focus of this study as stated earlier is on the schemes themselves and their impact on audit trail and also issues and challenges relating to identifying individuals involved in electronic fraud related cases and the method used in electronic accounting system.

STATEMENT OF THE PROBLEM

Research has shown that about 10 to 15 percent of employees fundamentally dishonest about 66 percent are normally honest but will cheat under the right circumstances, and above 20 percent to 25 percent are fundamentally honest are unlikely to steal under any circumstances. Those who do defraud the company are unlikely to have a prior criminal record. Another problem is that obtaining convictions can be very difficult in many fraud cases, especially those involving computerized accounting records often the evidence is not tangible but exists only in complicated computer files and a weak audit trail.

OBJECTIVES OF THE STUDY

The broad objective of the study is to determine the employee fraud methods in electronic accounting systems.

The specific objectives are as follows:-

1. To investigate direct file alteration by employees
2. To ascertain the amount of money lost to program alteration
3. To determine the amount lost as a result of data theft.
4. To assess the amount lost by the sabotage of employees

RESEARCH HYPOTHESES

Ho_1: Employee Fraud methods in Electronic Accounting System has no significant relationship with direct file alteration

Ho_2: Employee fraud method has no significant relationship with program alteration.

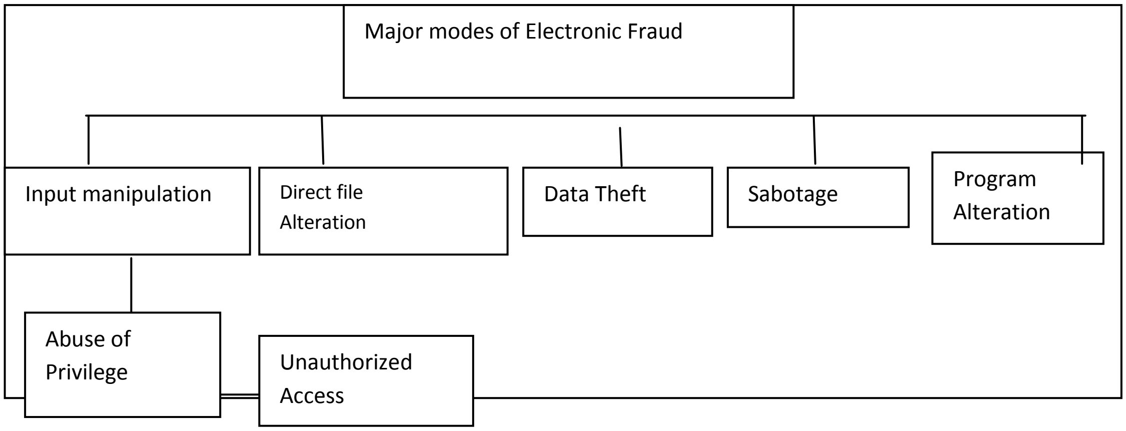
Ho3: Employee fraud method has no significant relationship with data theft
Ho4: Employee Fraud method has no significant relationship with sabotage of employees.

REVIEW OF RELATED LITERATURE

Conceptual Framework

The employee fraud methods in electronic accounting systems in this type of fraud, an employee with legitimate access to a portion of the system enters fraudulent data. For example someone in the credit department could enter into the system a new credit account approval without the proper supporting documentation. If the system has an appropriate audit trail, the related approval details will appear in the customer's account record. However, if the supporting documentation is not electronic but on paper, it could end up in some distant warehouse after the account is inactive for a year or two. Then the company could have no practical means to verify the account approval. The account could then be abused by another dishonest employee without putting the credit department employee at risk of being caught.

Fig. 1: Diagram major modes of electronic fraud



Source: ***Forensic Accounting and Fraud Examination Hopwood, Leiner & Young (2014)***

Simple automated reconciliations detect several types of access privilege abuse. For example, an account receivable clerk who issues an unauthorized cash receipts credit to a customer's account is likely to be identified if and when the system reconciles total cash receipts posted to the cash account versus the total credit to customers accounts. Many times, employees are not aware of such reconciliations, and so they commit crimes they cannot possibly get away with. The worse case could involve an employee's account and then abuses that account. This fraud can render the audit trail useless in catching the perpetrator.

Direct File Alteration

Employees normally need an account login and password to access accounting data bases and files and this access method normally leaves an audit trail. In some cases, however, sophisticated employees manage to use system type tools to directly access and modify accounting records without using the accounting system. This type of fraud leaves no audit trail in accounting system, but it could leave an audit trail in the general computer system logs of course, a sophisticated user might be able to doctor the general system logs.

Program Alteration

Program alteration occurs when a programmer takes authorized changes to the accounting software. The most famous case of program alteration involved the "round-off thief" who put a patch in the payroll processing code that rounded off payments to the nearest kobo and transferred the fraction kobos to an account that he controls. This happened in a large company that had large numbers of rand-off to steal and the programmer ended up stealing thousands of Naira.

A forensic accountant might not easily spot program alteration fraud in the normal audit trail or miss it completely. Consider, for example, a fraudulent program patch that incorrectly computes one employee's paycheck to be higher than it should be. Depending on the situation, this fraud could go unnoticed unless someone double-checks the employee's payroll calculations; something might or might not happen in an audit situation. Because audits focus only on samples of transactions, in many cases the audit concentrates on transactions that substantially differ from the norm, in cases of programe alteration, the audit trail of special importance to the forensic accountant is the program change log. In well-controlled systems, all changes to programs are made to nonworking copies of the programs. The changes are then reviewed, tested, approved and entered into a program change log before they are implemented.

Data Theft

Data theft is usually easier to prevent than to identify, trace to a perpetrator, and prosecute. Corporate information systems usually hold high-value information such as customer lists, trade secrets, internal budgets, employee profiles and strategic plans. Even with sophisticated security systems, there is often little that can be done to stop trusted employees from stealing valuable data and selling it to competitors or others. In a well designed system, users are not permitted to access or print more data than required for their job functions. This means that data access log reveal only normal access patterns. That is there may be nothing helpful for the forensic accountant in the audit trail.

Sabotage

Sabotage especially electronic sabotage, is usually carried out by disgruntled or recently fired workers. In one case, a programmer added a piece of malicious programming code to the payroll program to check each pay period to see whether the programmer was still an employee. It was found out that he was no longer an employee, it began erasing critical files.

RESEARCH METHODOLOGY

Research Design

The research design used in this study is descriptive one, with conceptual plan and theoretical analysis; these are some of the strategies used to arrive at the best justification for the study

Types and Sources of Data

The research work tends to rely mostly on the use of aggregate secondary data (ASD) key factory and indices that are incidental to corporate fraud prevention, detection and investigation are some of the control measures. Investigations are some of the control measures.

Information from textbooks, professional accounting journals of the institute of chartered accountants of Nigeria (ICAN), the Association of National

Accounting of Nigeria (ANAN) and other official sources of information are also used.

Populations/Sample Size of the Study

The population is made up of 214 companies selected from different sectors of the economy such as Agriculture and extraction, manufacturing, marketing, production and service industries. Non-probability sampling of the same 214 was used as the sample size since the researcher can comfortably mange it.

Measure of Variables and Data Analysis

The key variable for this study are the financial statement of these companies operationalized into employee fraud methods in electronic accounting system using such independent variables as direct file alteration, program alteration, data theft and employee sabotage.

To operationalize the conceptual model

The first objective is to establish measures against file alteration

Model 1: EFM = flao log+$b_1$log FAP+B_2 Log PAT +B_3 log DAT+b_4 Log SOE + B_5 log off + ….ui

Model 2: The second objective is to establish measures against program alteration

FIA = Flao log +B_1 Log FPA+B_2 Log FDT=B_3Log EST+log off + B_5 log ICst…ui

Model 3: the third objective is to establish measure against employee sabotage

EST = Floa log+B_1 Log FAP = B_2 Log PAT = B_3 Long DAT B_4 Log goe + B_5 log off - + ui

Presentation of Results

Test of Hypotheses1, 2 &3 combined:

Ho_1 2&3: Employee Fraud methods have no significant relationship with direct file alteration, data theft and sabotage of employee.

Table 1: Amount lost from employee fraud

Years	(N' billion)
2014	30657.32
2015	34296.32
2016	34714.32
TOTAL	99667.96

Source: researcher's computation 2017

Fig 2

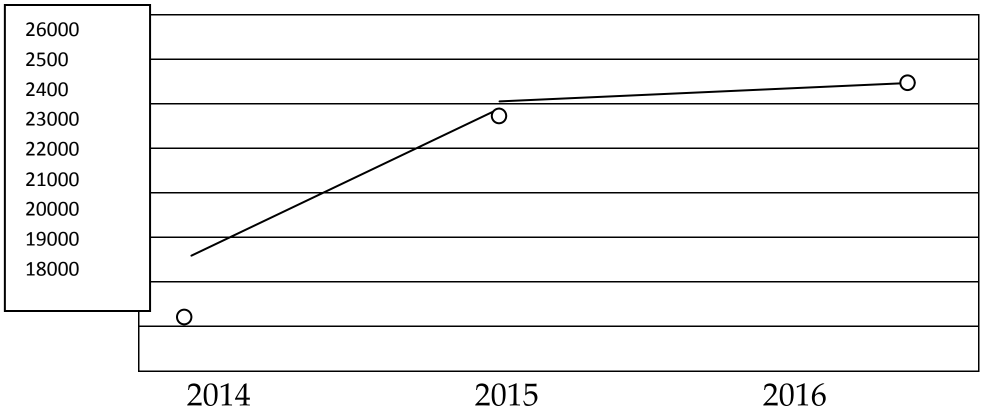


Table 2 above is regression diagram of amount lost to employee's fraud which is at increase from 2014 to 2016 without sign of reduction as years go by Regression

Descriptive Statistics Impact of Fraud on the company's assets

	Mean	Std. Deviation	N
Not file alteration loss (N billion) Program alteration loss	2.3222.7867 3.7298E8	2231.58667 5.77387E7	3 3

Table 3 Correlations

	Data Theft (N'billions)	2013-2015
Pearson Correlation. (N billion) Program alteration	1.000 .986	.986 1.000
Sig. (1-tailed) (N'billion) 2013 – 2015 program alteration	.053	.053
N File alteration (N' billion) 2013-2015 program alteration	3 3	3 3

Table 4:
Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. error of the estimate	Durbin Watson
1	.986[a]	.972	.945	525.37290	2.368

a. Predictors: (Constant), Employees theft
b. Dependent Variable: Employees fraud methods

Tables
ANOVA

Model	Sum Squares	Df	Means Square	F	Sig.
1 Regression	9683941.426	1	9683941.426	35.085	.106 [a]
Residual	276016.681	1	27601.681		
Total	9959958.107	2			

a. Predictors: (constant), 2014 2016 Employees theft
b. Dependent variable: employees fraud methods

Table 6:
Coefficients

Model	Un-standardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
1 (constant) 2013-2015	9008.328	2418.876		3.724	.167
Employees theft	3.811E-5	.000	.986	5.923	.106

a. Dependent Variable: Employees Fraud Methods (N'billion).

EFM = 9008.328+3.811ES EMT

Where: = EFM Employees Fraud Methods
= EMT Employees Theft
R = 0.986
R2 = 0.972
F = 35.085
DW = 2.2.368

The regression sum of squares (96839411) is greater than the residual sum of squares (276016.681) which indicates that more of the variation in the dependent variable is explained by the model. The significance value of the F statistics (0.106) is greater than 0.05, which means that the variation by the model is due to chance.

R the correlation coefficient, which has a value of 0.986, indicates that there is an extremely strong relationship between the dependent variable and the independent variable. R. square, the coefficient of determinations, shows that 97.2% of the variation in the dependent variable is explained by the model.

With the linear regression model, the error estimate is high, with a value of about 523.37290. The Durbin Watson statistics of 2.368, which tends to 2, indicates there is autocorrelation.

The EMT coefficients of 3.811E-5 indicates a positive relationship EFM and, EMT which is not statistically significant (with t = 5.923). Hence, Employees fraud methods do has a positive but not significant impact on the EMT

CONCLUSION

Direct file alteration fraud is generally difficult or impossible to commit if the accounting files are properly encrypted. However, some encryption scheme especially those based on simple passwords, can be broken. In addition, encrypted systems store temporary data in randomizes memory. This substitution would amount to piggybacking fraudulent data into a legitimate transaction. In this case, the audit trail would be misleading and the unfortunate originator of the legitimate transaction could even be considered the perpetrator. The important point is that audit trails can be meaningless when a sophisticated fraudster is involved. Fortunately, however, the average company employee is not able to perform such sophisticated schemes.

The fraud triangle is helpful in explaining motivations for employees to defraud the company; pressure, opportunity, and rationalization. Pressure is typically caused by sudden financial needs arising from things such as medical bills, gambling problems, drug habits and extravagant living. The opportunity depends on the employee’s position and the strength of the company’s internal control processes. Rationalization depends on the type of criminal. The pure sociopath may need little or no rationalization. The fundamentally dishonest employee may give some conscious thought to rationalizing crimes, but the rationalization comes easily because the person is accustomed to dishonesty. Finally, the normally honest employee could give the most effort to rationalization of the crime, and often this type of person will think that he is only borrowing the money.

REFERENCES

Banks and other Financial Institutions Acts (BOFIA 1991)
Insurance Act of 2003

Bayer Group (2007). Annual Report, Bayer Ag AG, Germany, retrieved from www.bayer.com

Bright, F. (1997). Preventing Corporate embezzlement: Boston, Butterworth.
BPP (2010) . Financial Reporting. London: Drydem Press.

British Airways (2008). Annual Report and Accounts. Retrieved from www.ba.com

Crumbley, D.L. Heitger L.E, and Smith G.S. (2007) Forensic and investigative accounting, 3rd ed. Chicago, CCH).

Deloitte (2010). Deloitte global Service Limited. Retrieved from www.deutschetelekom.com

Esirt (2008). Annual Report, Esprit Holdings Limited, Germany. Retrieved from www.espritholdings.com

Fatimahim, A.E. (2004)Introduction to Bankruptcy Executive ship and trusteeship. Lagos: Fatimehin and Associates.

Federal inland revenue Service Act 2007

Financial Reporting Council of Nigeria Act 2001

Fubabce (Control and Management) Act 1958 as amended.

Gary, S (1999). Crime in our changing society: New York, Holt, Reinhardt and Winton.

Helmk. (1997). Collaring the crime not the criminal, American Sociological Review: 55, 346-365

Hennie, G. (2010), International Financial Reporting Standards- A practical guide 5th ed. Washington: The World Bank.

Hirschi, T. and G. H, Fredson M. (1987). "Causes of white crime". Criminology 25,949-974.

LASCF(2008). Review of the Constitution Public Accountability and the composition of the LASB-proposals for charge.

ICRC (2007), International Committee of the Red Cross Annual Report
Switzerland. Retrieved from www.icre.org

Hopwood, Leiner & Young (2012) Forensic Accounting and Fraud Examination second edition, Singapore.

Reference to this paper should be made as follows: Nwadighoha, C. E. (2017), Employee Fraud Methods in Electronic Accounting Systems (Issues and Challenges)**.***Intl J. of Management Studies, Business & Entrepreneurship Research,* Vol. 2, No. 4, 2017, Pp 1-11