



JOGIIS

Journal of
**GLOBAL ISSUES AND
INTERDISCIPLINARY STUDIES**

ISSN 97700000



Published by
**INSTITUTE OF HEALTH SCIENCE,
RESEARCH AND ADMINISTRATION NIGERIA**



THE RELATIONSHIP BETWEEN ICT UTILIZATION AND FRAUD LOSSES IN COMMERCIAL BANKS IN NIGERIA

¹Samuel, E.U., ²Oluwatosin, J.A., ³Muhammad, A.M

¹University of Parakou: Department of Information management System

²Institute of Health Science, Research and Administration Nigeria: Department of Information Communication Technology

³ISM Adonai University, Benin Republic: Department of Computer

Corresponding author: Ejindu Samuel U, +229 98 56 53 49

Article history: Received 21 February 2023, Reviewed 21 June, 2023, Accepted for Publication 30 June, 2023

ABSTRACT

Background: Bank fraud has grown with advent of the banking industry, and has been facilitated by the technological innovations and the widespread use of the Internet. The main driver of financial innovations in banks is adoption of ICT. It enables banks to develop sophisticated products, implement reliable techniques for control of risks and to reach geographically distant and diversified markets.

The purpose of this study was to establish the relationship between ICT utilization and fraud losses in commercial banks in Nigeria.

Method: Data was collected from reports at central bank, Banking Fraud Investigation Unit and audited financial reports of the 22 commercial banks in Nigeria. Data was analyzed using SPSS through correlation analysis and regression analysis.

Result: The findings were presented in tables and graphs. The major findings of the study indicated that total values transacted through EFT, RTGS and ATM had a positive correlation with the total fraud costs of commercial banks. The level of staff wages also had a positive correlation with fraud losses.

Conclusion: ICT utilization has exposed commercial banks in Nigeria to more fraud. This is due to the speed of execution of transactions. Adoption of ICT tends to increase the chances of Identity theft due to the fact that transactions are online and real time. The levels of staff wages are also a motivation for fraud from the employee side. The researchers recommend more robust fraud mitigation practices and policies to ensure that all elements of fraud are captured in the adoption of ICT. Banks should consider increasing their staff costs to mitigate frauds. Bank employees have access to all information relating to customer accounts hence should be well rewarded and motivated in order to prevent them from falling into traps of fraud. The researcher suggests that a similar study be carried out targeting MFIs to get their perspective of the effect of ICT utilization on fraud losses.



INTRODUCTION

Fraud has been in existence throughout history and has taken many different dimensions. Bank fraud has grown with advent of the banking industry, and has been facilitated by the technological innovations and the widespread use of the Internet. According to the fraud triangle (Cressey, 2021), for fraud to occur the three factors; pressure, rationalization and opportunity should be present. Bank employees have knowledge of the systems as well as classified and confidential information which together with technological advancement can give them the opportunity to commit frauds. All they need is some pressure and the rationalization and that way they become part of fraud cartels that are fleecing millions of shillings from the banks.

According to a report by consultant firm, Deloitte Nigerian banks were victims of more than half the N4.1 billion (\$48.3 million) fraud that hit East African banks in 2012 as technology made the crime easier. At least N1.5 billion (\$17.64 million) was stolen from Nigerian banks in the past one year, in schemes hatched by technology-savvy bank employees. This can be attributed to failure by both the bank processes and the employees to detect and control fraud. Security experts say the amounts reported reflect only a small portion of the real losses suffered since banks prefer internal disciplinary measures in cases involving thieving employees (Kimani, 2013). This means that banks should be on an alert and should also revise their controls to keep up with fraud and technology.

Information technology has been around for a long, long time. Basically as long as people have been around, information technology has been around because there were always ways of communicating through technology available at that point in time. ICT has transformed the lives of

people as well as organizations. It is no surprise that ICT revolution has proven a powerful source for creative vision by utopian thinkers the world over. The reach ICT around the world has been expanding for decades. The recent past has seen particularly rapid rollout of access to communication facilities like telephones and the Internet, as technology advance has driven down costs (Nyokabi, 2012). Like other countries Nigeria has recognized the potential and enabling element of ICT as a tool for social and economic development.

ICT is increasingly seen as a means of enabling other developmental needs rather than as an end in itself hence some types of financial innovation are driven by improvements in ICT. Weremchi, (2000) claimed that only banks that overhaul the whole of their payment and delivery systems and apply ICT to their operations are likely to survive and prosper in the new millennium. He recommends that banks should re-examine their service and delivery systems in order to properly position them within the framework of the dictates of the dynamism of ICT.

Fraud is an intentional deception made for personal gain to damage another individual. It is a crime and is also a civil law violation. Many hoaxes are fraudulent, although those not made for personal gain are not technically frauds (Wanemba, 2011). According to The American Heritage Dictionary, (Second College Edition), fraud is defined as “a deception deliberately practiced in order to secure unfair or unlawful gain”. In a nutshell, “Fraud always involves one or more persons who, with intent, act secretly to deprive another of something of value, for their own enrichment” (David et al., 2000). Wells, (2005) also stresses deception as the linchpin to fraud. Defrauding people of money is presumably the most common type of fraud, but there have also been



many fraudulent discoveries, in art, archaeology, and science.

Bank fraud on the other hand, is the use of fraudulent means to obtain money, assets, or other property owned or held by a financial institution (Glaessner and Mass, 1995). Bank fraud is a crime that has been around for as long as banks have been in operation. Anytime there is a large amount of money floating around, there will be people trying to figure out ways of getting it. Fraud can be committed through many methods, including mail, wire, phone, and the internet (computer crime and internet fraud). The difficulty of checking identity and legitimacy online, the ease with which hackers can divert browsers to dishonest sites and steal credit card details, the international dimensions of the web and the ease with which users can hide their location, all contribute to making internet fraud the fastest growing area of fraud. Estimates are that just twenty percent of frauds are exposed and made public. The remaining frauds are either undetected or discovered and not made public because of reputation risk (Bartlett and Ballantine, 2002). Leuchtner, (2011) identified the common fraud schemes in banks as general ledger fraud, identity theft, account takeover and collusion with external criminals.

Effiong and Juhi, (2007) defined bank fraud as a deliberate act of omission or commission by any person carried out in the course of banking transactions or in the books of accounts, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank. They concluded that bank frauds are the failure of the banker and mentioned the major elements responsible for the commission of frauds in banks; active involvement of the staff-both supervisor and clerical either independent of external elements or in connivance with outsiders, failure on the part of the bank staff to follow

meticulously laid down instructions and guidelines and external elements perpetuating frauds on banks by forgeries or manipulations of cheques, drafts and other instruments. There has been a growing collusion between business, top banks executives, civil servants and politicians in power to defraud the banks, by getting the rules bent, regulations flouted and banking norms thrown to the winds.

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

The application of networks is also vital part of an effective ICT-enabled system, which is especially true in the case of banks with a branch network. Local Area Network (LAN) may also be seen as a basic indicator of the minimum infrastructure required to enable banks to conduct e-banking at a substantial level. Wire-based LAN is currently the dominating technology. Wireless LAN is a relatively new technology in the Banking Industry, and is used to permit bank employees to access network resources from nearly any convenient location. Instant notification of transactions made is another innovation brought by ICT through the use of smart phone in conjunction with the internet facility in the Banking Industry. There has also been the digitalization of formerly paper-based processes. Electronic mail is increasingly



being applied for especially non-legal correspondence like account statements, marketing and sales (Agboola, 2001).

The security issue which is the basis of ICT related fraud is of special concern in the Banking Industry, as banking is highly based on trust from its customers. The risk of hackers, denial of service attacks, technological failures, breach of privacy of customer information, and opportunities for fraud created by the anonymity of the parties to electronic transactions can be managed by enhancing security of information. Depending upon its nature and scope, a breach in security can seriously damage public confidence in the stability of a financial institution or of a nation's entire banking system. By introducing the appropriate security measures and putting security concerns at ease, banks might be able to attract the segments among consumers who previously were not inclined to use e-banking. Furthermore, it is also in the banks' own interest to improve security, as digital fraud can be costly both in financial losses, and in terms of the damage it does to the brand of the bank in question. The common concern among users of ebanking is related to the authentication of users and data connections. This includes the use of digital signatures, PIN codes and encryption (Agboola, 2001).

Appelbaum and Shapiro, (2006) felt that top management plays a major role in fraud control. They concluded that the concept that is stressed by those in positions of authority will determine how workers react to situations that have ethical implications, thus the message of zero tolerance to fraud has to flow downwards from the top. Hollman, et al, (2003) suggested that every organization should have a manual that should clearly define behavior expectations, i.e., what activities are unacceptable, the internal controls in place to prevent fraud, and the punishment for those who do not comply.

This ethics policy should become operative at the time of new hire orientation and continue until the employee separates. However various conditions may exist within an organization or business which can give an individual that feeling of opportunity. If an organization has a lack of policy to control various activities which could allow an individual to take part in fraud and espionage activity then the offender can become embolden to take part in a criminal action because of the lack of a formal written policy as a means of authority for enforcement (ACFE, 2008). Policies should be viewed as a social fabric which provides guidelines to hold the organization together.

According to the Journal of Economic Crime Management, the Fraud Management Lifecycle is made up of eight stages. Deterrence, the first stage, is characterized by actions and activities intended to stop or prevent fraud before it is attempted; that is, to turn aside or discourage even the attempt at fraud through, for example, card activation programs. The second stage is prevention which involves actions and activities to prevent fraud from occurring. In detection, which is the third stage, actions and activities, such as statistical monitoring programs are used to identify and locate fraud prior to, during, and subsequent to the completion of the fraudulent activity. The intent of detection is to uncover or reveal the presence of fraud or a fraud attempt. The goal of mitigation, stage four, is to stop losses from occurring or continuing to occur and/or to hinder a fraudster from continuing or completing the fraudulent activity, by blocking an account, for example. The next stage analyses losses that occurred despite deterrence, detection, and prevention activities are identified and studied to determine the factors of the loss situation, using methods such as root cause analysis.



The sixth stage of the Fraud Management Lifecycle, policy, is characterized by activities to create, evaluate, communicate, and assist in the deployment of policies to reduce the incidence of fraud. Balancing prudent fraud reduction policies with resource constraints and effective management of legitimate customer activity is also part of this stage. The seventh stage, involves obtaining enough evidence and information to stop fraudulent activity, recover assets or obtain restitution, and to provide evidence and support for the successful prosecution and conviction of the fraudster(s). Covert electronic surveillance is a method used in this stage. The final stage of prosecution is the culmination of all the successes and failures in the Fraud Management Lifecycle. There are failures because the fraud was successful and successes because the fraud was detected, a suspect was identified, apprehended, and charges filed. The prosecution stage includes asset recovery, criminal restitution, and conviction with its attendant deterrent value. (Wilhelm, 2004)

Tremblay, (1997) studied credit card counterfeiting and offenders along with displacement, as opposed to the methods, procedures, and policies employed by the victims to prevent the fraud. He concluded that when fraud management professionals fail to balance the various stages of the Fraud Management Lifecycle successfully, and do not integrate new technologies into each of the Lifecycle's stages, they expose the companies they represent to unnecessary fraud losses and/or excessive expenses, and create a negative externality effect on society.

A whistle blower line provides an avenue for early detection of fraud. It also acts as an avenue for a concerned employee to anonymously voice his or her concerns. The existence of a hotline may not be enough hence management should also consider conducting periodic evaluations

to determine whether the whistle-blower hotline is effective, including benchmarking analysis against competitors. Banks should consider the use of an experienced outside agency managing the whistle-blower hotline to enhance the perception of confidentiality. The policy can simultaneously create an incentive program for associates who uncover misconduct. (Kemi, 2008)

METHOD

Research Design

A descriptive survey was employed to gather a broad range of information regarding utilization of ICT and fraud in commercial banks in Nigeria

Study Area: This study was conducted among 22 banks in Nigeria, which include: Access Bank Plc, Citibank Nigeria Limited, Eco bank Nigeria Plc, Fidelity Bank Plc, First Bank Nigeria Limited, First City Monument Bank Plc, Globus Bank Limited, Guaranty Trust Bank Plc, Heritage Banking Company Ltd, Keystone Bank Limited, Paralex Bank Ltd, Polaris Bank Plc, Premium Trust Bank, Providus Bank, Stanbic IBTC Bank Plc, Standard Chartered Bank Nigeria Ltd, Sterling Bank Plc, SunTrust Bank Nigeria Limited, Titan Trust Bank Ltd, Union Bank of Nigeria Plc, United Bank For Africa Plc, Unity Bank Plc.

Study Population: The target population was made of the 22 commercial banks licensed by the Central Bank of Nigeria as at 31st December 2017.

Sample: The study targeted the whole population of all the 22 banks.

Method of Data Collection: Data on fraud was collected from records at the Banking Fraud Investigation Unit (BFIU) and Economic and Financial Crime Commission (EFCC). CBN reports were



reviewed to collect data on amounts transacted through ATM, RTGS and EFT. Data on staff costs was extracted from audited financial statements of banks for the period 2011-2015.

Method of Data Analysis: The collected data was analyzed using the Statistical Package for Social Sciences (SPSS) version 16. Regression analysis was used to quantify the relationship between the dependent variable and the independent variables. The technique assisted in coming up with estimated coefficients in the empirical equation that measure the change in the value of the dependent variable for each one unit change in the independent variable, holding the other independent variables constant.

Empirical Model: Regression analysis was used to analyze effect of ICT utilization on bank fraud. The regression model was as follows;

$$Y = a + b_1X_1 + b_2 X_2 + b_3X_3 + b_4X_4 + \epsilon$$

In order to measure the dependent variable (Y) the researcher used the annual amount lost through fraud in commercial banks. The researcher sought to establish the relationship between the total fraud (dependent variable) and the total value transacted through ICT related payment systems (ATM, RTGS and EFT) and Staff costs being the independent variables. Staff costs were used as a control for financial pressures faced by bank employees.

The components and measurements of the variables were as follows: Y= amount lost through fraud a = constant (The fraud Factor that exists without any adoption of ICT related transactions) b_1, \dots, b_4 are co-

efficient of the independent variables (X_1, \dots, X_4) respectively.

X_1 = Total Value Transacted through ATM per month as per CBN reports

X_2 =Total Value Transacted through RTGS per month as per CBN reports

X_3 = Total Value Transacted through EFT per month as per CBN reports

X_4 = Staff costs (Annual wages and salaries as reported in audited statement of comprehensive income) ϵ = the error term, it represents the noise effect of all variables excluded from the regression model plus the effect of measurement error in the variables included in the model.

Mean scores were appropriately used to establish how ICT utilization affects fraud in commercial banks in Nigeria as was indicated by scores put against each descriptive statement. The findings of the study were presented in tabular form for ease of interpretation and reporting. SPSS output of multiple regressions was used to establish existing relationship between the dependent and independent variables. The ANOVA tables were also established to indicate the level of fitness and validity of the model with the existing set of independent variables. The correlation coefficients were used to measure the degree to which the variables are related ranging from 0 to +1 if positively correlated and 0 to -1 if negatively correlated.

Ethical permission: The researchers got approval from the banks prior to the research. The approval for this research was signed by the Banker manager of each Bank.

RESULT

Checking Multi-collinearity

Normal regression results indicated multi-co linearity problem where independent variables i.e. RTGS, ATM and EFT values were highly correlated. This was indicated by several Eigen value close to zero meaning that the predictors are highly correlated and that a small change in the data values may lead to large changes in estimated coefficients. This problem was also revealed through co linearity diagnostics by high condition indices of beyond the 15 mark considered benchmark. To fix the multi-co linearity problem, the regression was re-run using standardized values and the step-wise method of model selection. The table below shows that RTGS values was excluded in the overall model due to multi collinearity.

Table 1: Excluded Variables

	Model	Beta In	t	Sig.	Partial Correlation	Collinearity Statistics		
						Tolerance	VIF	Minimum Tolerance
1	RTGS	.161a	3.596	.001	.430	.977	1.023	.977
	EFT	-.061a	-1.026	.309	-.135	.663	1.508	.663
	ATM	.402a	7.972	.000	.726	.448	2.234	.448
2	RTGS	.041b	1.064	.292	.141	.757	1.322	.347
	EFT	.153b	3.437	.001	.417	.482	2.075	.325
3	RTGS	.053c	1.500	.139	.198	.750	1.333	.278

Since the stepwise regression excluded RTGS values in the model due to multi-collinearity as shown in table 1 below, the beta coefficient for RTGS is not necessary here as a predictor of fraud losses. This means that the variables that will be in the model to predict fraud costs are ATM values, EFT values and Staff costs.

Table 2: Descriptive Statistics

Descriptive Statistics					
	FRAUD LOSSES	STAFF COSTS	EFT VALUES	RTGS VALUES	ATM VALUES
N	60	60	60	60	60
Mean	90.91583333	4334.145865	262300	1501146	9595.09023
Median	89.41666667	3983.768497	213000	1456240	9673.5
Mode	68.49583333	3453.131436	214000	107235	7439
Std. Deviation	18.6944243	743.3516288	95498.21189	383805.9	2778.49922
Range	55.67083333	2115.55851	276000	2510105	9745.35538
Minimum	68.49583333	3453.131436	152000	107235	5276.64462
Maximum	124.1666667	5568.689946	428000	2617340	15022
Sum	5454.95	260048.7519	15738000	90068746	575705.414

Source: Analysis of research data-2021

Table 2 above, analyzes the descriptive statistics which included the mean, standard deviation, minimum, median and maximum value for fraud losses, staff wages, EFT values, RTGs values and ATM values. The statistics were computed for 60 monthly observations.

The difference in fraud losses in terms of highest and lowest fraud figures was N55.67 million. This indicates that fraud is not uniform monthly. The mean fraud losses were N90.9 million. The deviation from the mean monthly fraud losses was N 18.69 million. The minimum and maximum fraud losses were N68.49 million and N124.17 million respectively. The mean EFT, RTGS and ATM values were N4,334 million, N262,300 million, N1,501,146 million and N9,595 million respectively for the study period. The minimum and maximum ATM values were N5276.64 million and N15,022 million respectively. The difference in these monthly values was N9745.35 million. The difference in values transacted could be attributed to the fact that more bank customers were more comfortable with the use of ATMs as technology advances.

Table 3: The Analysis of variance

The analysis of variance				
Model		Sum of squares	F	Significance
	Regression	56.78597906	28.615**	0.000
	Residual	3.214	329.806	0.0000
	Total	60		
Adjusted R square	0.944			

In general, from table 3 above which shows the regression results corrected for multicollinearity indicates that about 94.6% of the variation in fraud losses can be accounted for by the model (adjusted R² of 0.944). The ANOVA table also shows regression sum of squares of 56.78597906 out of total variation of 60 also pointing to the fact that about 94.6% variation in bank fraud is explained by the model. In addition, the significance value of the F-statistic is less than 0.05 which means that the variation in the dependent variable explained by the model is not by chance.

Table 4: Regression coefficients

Coefficients				
Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
(Constant)	-0.000000000000000022		-0.000000000000000071	1
WAGES	0.646659124	0.646659	13.91421	0.000
RTGS	-	-	-	-
ATM	0.49931875	0.499319	9.210045	0.000
EFT	0.153114573	0.153115	3.437177	0.001115

Source: Analysis of research data-2021

From table 4, In order to determine the relationship between the fraud losses and the four independent variables at the commercial banks, the researcher conducted a multiple regression analysis. As per the SPSS generated table 4., the equation ($Y = a + b_1X_1 + b_2 X_2 + b_3X_3 + b_4X_4 + \epsilon$) becomes: $Y = 0.000000000000000022 + 0.499 X_1 + 0.153X_3 + 0.647X_4$:



Where Y is the dependent variable (fraud losses), X_1 is Total Value Transacted through ATM per month as per CBN reports, X_2 is the Total Value Transacted through RTGS per month as per CBN reports, X_3 is the Total Value Transacted through EFT per month as per CBN reports and X_4 is the annual staff costs as reported in audited financial statements.

DISCUSSION

The stepwise algorithm chose, value transacted through ATM, EFT and staff wages as the predictors of fraud losses in banks as shown in table 4 below. As per the regression equation established, if all ICT utilization factors were taken to be constant at zero, fraud losses at the commercial banks will be 0.00000000000000022 which is almost zero. The β coefficient of staff costs is positive indicating that there exists a significant positive relation between staff costs and fraud losses. The data findings analyzed also shows that if all other independent variables are taken at zero, a unit increase in the Value Transacted through ATM will lead to 0.499-unit increase in the fraud losses at the commercial banks. Further, a unit increase in the Value Transacted through EFT will lead to 0.153 increases in the fraud losses at the commercial banks and a unit increase in the annual staff costs will lead to a 0.647 increase. The results of the test show that the coefficient estimates of all the independent variables are positive conveying the message that these three independent variables (ATM, EFT and staff costs) have positive effect on the fraud losses.

From the above analysis of the betas, it can also be inferred that the level staff costs, contributes a lot on the fraud losses at the commercial banks followed by ATM transactions and EFT transactions respectively. The level of staff wages contributes to fraud losses because of the fact that employees who are not well motivated financially will most likely fall into traps of fraud originating within the banks or even through collusion with outsiders. EFT and ATM values contribute

to fraud in that as more customers transact a lot of data is exposed to identity theft. This is due to the speed of processing and the fact that the transactions are online and real time. From the analysis the significance value of staff wages, ATM and EFT as a predictors are less than the p-value of 0.05 indicating that these variables are statistically significant in predicting fraud losses.

These findings support the theory of the fraud triangle which concluded that individuals commit fraud when three factors are present: (1) a financial need that cannot be shared, (2) a perceived opportunity for illicit gains, and (3) a personal rationalization of the act. Adoption of ICT by banks may have increased the opportunity to commit fraud. These findings are also consistent with those in studies by (Wanjiru, (2011) who did a case study at Access of Nigeria Limited with the aim of getting detailed information regarding the strategic responses to increasing fraud related risks. The Bank's IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The study also revealed that a whistle blowing facility is existent in the Bank.

The findings of this study also support findings by Wanemba, (2010) who carried out a study with an objective to establish the challenges of fraud faced by commercial banks in Nigeria and to identify the strategies that commercial banks in Nigeria use to combat fraud. The study concluded that it's necessary for a bank to have an anti-fraud unit that employs various strategies to curb fraud. The researcher suggested that banks should invest in advancing their



technology in order to prevent fraud. The KYC (Know Your Customer) strategies are also equally important, and if applied together with regular auditing, will be able to curb cases of fraud. The internal controls within the banks should also be looked at keenly to ensure that they are in line with fraud prevention. The findings in this study also agree with Agboola, (2001) who studied the impact of computer automation on the banking services in Lagos. He discovered that Electronic Banking has tremendously improved the services of some banks to their customers in Lagos. He also concluded that ICT improved bank efficiency but at the same time exposed banks to fraud.

The significance value of staff costs as a predictor is less than the p-value of 0.05 indicating that the variable is significant in predicting firm value. This supports the fraud scale theory developed by Adeyemi, Howe, and Romney, (2004). They stressed on an element called personal integrity instead of rationalization. This personal integrity element is associated with each individual's personal code of ethical behavior. The findings are also consisted with the study by Appelbaum and Shapiro, (2006) who felt that top management plays a major role in fraud control. They concluded that the concept that is stressed by those in positions of authority will determine how workers react to situations that have ethical implications, thus the message of zero tolerance to fraud has to flow downwards from the top.

LIMITATIONS OF THE STUDY

The study relied on secondary data collected from audited financial statements and reports at the CBN and BFIU. A limitation of this is the accuracy and reliability of the financial statements of the commercial banks. The figure of staff coats in such statements may have been inaccurate.

The integrity of the findings is affected by the fact that banks do not report all fraud to BFIU. Some banks choose not to report fraud to BFIU but instead deal with such cases internally to avoid reputational risk.

Some banks were not in operation during the entire period of study. Examples include Jamii bora Bank which was licensed in 2010.

Strength of the study: This study employed a distinguished design and was subjected to validation by 2 different supervisors.

RECOMMENDATIONS

The researchers recommends more robust fraud mitigation practices and policies to ensure that all elements of fraud are captured in the adoption of ICT. Part of the investment in ICT should include fraud detection and control. Before an ICT system is adopted, it should be thoroughly tested for possibility of both internal and external fraud. In addition to this, there should be continuous monitoring of bank systems to ensure that fraud is detected and controlled at the earliest possible time.

Banks should also consider increasing their staff costs to mitigate frauds. Bank employees have access to all information relating to customer accounts hence should be well rewarded and motivated in order to prevent them from falling into traps of fraud. All bank employees should be vetted before employment and during employment. Vetting before employment will ensure that only those with high moral standards are taken in for employment. This may include background checks and recommendations from previous employers. Vetting during employment would include looking out for changes in the employees' lifestyle that cannot be explained by their income. Management could also introduce hot lines for reporting fraud. This can be open to both bank



employees and outsiders. Such a hot line can help banks in cutting down fraud costs as they can be able to control fraud once it is reported.

CONCLUSION

From the above findings the researchers concluded that in the period between 2008 - 2012; commercial banks recorded great increases in both ICT utilization and fraud costs. The minimum and maximum fraud losses were N68.49 million and N124.17 million respectively. The mean EFT, RTGS and ATM values were N4,334 million, N262,300 million, N1,501,146 million and 9,595 million respectively for the study period. The minimum and

maximum ATM values were N 5276.64 million and N15,022 million respectively. The difference in these monthly values was N 9745.35 million. The difference in values transacted could be attributed to the fact that more bank customers were more comfortable with the use of ATMs as technology advances.

The coefficient of determination (R^2) at 94.6 % and F' statistic at 329.8 indicated that the model was fit and valid with the existing set of independent variables. This therefore signified that ICT utilization was the main determinant of the fraud losses at commercial banks.

REFERENCES

Agboola, A. A. (2001). Impact of Electronic Banking on Customer Services in Lagos, Nigeria. *Ife Journal of Economics and Finance*, 5 (1&2)

Ajzen, I. & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior* Englewood Cliffs, NJ: Prentice-Hall, Inc.

Adeyemi, W., Howe, K. & Romney, M. (2004). *Deterring fraud: The internal auditor's perspective.*: The Institute of Internal Auditors Research Foundation. Altamonte Springs, FL


Adeyemi, W. S., Hill, N. C. & Adeyemi, C. C. (2006). The ethics development

model applied to declining ethics in accounting. *Australian Accounting Review*, 16(1), 30-40.

Effiong, Y. & Juhi, M. (2007). *Bank fraud in India*. National Law Institute University, Bhopal India.

Appelbaum, S. & Shapiro, B. (2006). Diagnosis and Remedies for Deviant Workplace Behaviors. *Journal of American Academy of Business, Cambridge*; 14-15

Cressey, R.D. (1973). *Other people's money: A study in the social psychology of embezzlement*.



In the rapidly evolving landscape of academic and professional publishing, the dissemination of knowledge through journals and articles stands as a cornerstone of scholarly communication.

IHSRAN Manual on Publishing Journals and Articles serves as an indispensable guide, offering an in-depth exploration of the multifaceted process that transforms ideas into published works of significance. This manual not only unravels the intricate threads of manuscript preparation, peer review, and publication ethics but also navigates the digital age intricacies, including open access paradigms and online platforms.

Whether you are a novice researcher seeking to navigate the complexities of publishing or a seasoned scholar aiming to refine your approach, this manual promises to be a beacon, illuminating the path to impactful and responsible dissemination of research.

Join us as we blend tradition and innovation, enabling writers to make valuable contributions to global array of expertise. We approve and release journal papers, ensuring your work is well-cared for.

Initiating the process of publishing in an IHSRAN journal involves ensuring the publication of high quality manuscript and journal. Throughout the publication, there are guidelines to support you, allowing you to write, release and publish your articles.

Allow us to assist you in enhancing the potential of your upcoming publication!

ISSN 97700000