

Electronic Banking Fraud and Commercial Banks' Performance: An Empirical Prove of Nigeria

J.A. Obadeyi¹ A.A. Akande ² & Y. S. Jekayioluwa³

^{1,2,&3}Department of Accounting & Finance, Elizade University, Ilara-Mokin, Ondo State, 340112, Nigeria

Corresponding email: jekayinoluwayemi@gmail.com

Abstract

There is no doubt that integration of electronic banking system has increased quality of service delivery of banks but frauds perpetrated on the electronic platforms have become a menace to businesses and institutions; as fraudsters employed the electronic devices for nefarious activities. In view of this, this study investigated electronic banking frauds and Commercial bank's performance with an empirical prove of Nigeria. The research work adopted secondary sources of data. Simple regression technique was used to analyse the extent at which electronic banking frauds have affected banks' performance for a period of fourteen years (2006-2019). The study revealed that electronic banking fraud activities perpetrated have been impeding on returns of the banks during the period. The study concluded that there were more electronic banking frauds committed through Internet banking than other electronic channels.

Keywords: Electronic banking Fraud, Commercial banks, Return on Assets, Nigeria

JEL Classification: G2, G21

1. Introduction

Globally, electronic banking has improved and facilitated quality of services / products provided by banks. Electronic banking is related to banking service that is available anytime and is carried out online with a protected bank identifier against fraud. It is directly opposite the traditional banking system and with similar appellations such as internet banking, cyberspace banking, virtual banking and online banking. Ololade et al. (2020), posited that due to the present growth of electronic banking in Nigeria, criminals have now discovered other methods to enlarge their nefarious strategies of tricking sincere victims of their funds. They engaged in various methods like forgery, identity theft, cloning, malware attack, BIN attack, skimming and phishing to dupe end users of electronic payment. However, customers are not the only victims of electronic banking fraud, but other institutions that make use of individuals' data to conduct businesses and governments; and all these scenarios could be tailored towards electronic banking fraud. It is interesting to know that no possible target is exempted by the defrauders.

The computer usage has aided organisations' performance by electronically keeping proper documentation of clients. Though, performance helps to ascertain available resources that were efficiently and effectively employed to measure the financial status of banks. Organisations like banks employ electronic devices such as computers for managing financial deals and abets the banks to provide electronic banking services to enable clients inspect account balances online. Several organisations carried out business engagements easily and

quickly with computerised systems to facilitate settlements (Taiwo et al. 2006; Obadeyi, et al. 2018). Electronic banking uses devices to provide services more conveniently with quality service delivery (Taiwo et al. 2006). According to Adewale et al. (2014), internet banking permits trading without actual cash and physical deposits with ease to help achieve a cashless economy.

The upsurge in electronic banking fraud practices in Nigeria has become a source of concern to customers due to weak institutional structures, porous regulatory framework and poor internal control practices resulting to depletion in banks' ratio of profit after tax to total assets (Taiwo et al. 2006; Olaleye and Fashina, 2019; Ololade, *et al.* 2020). Electronic banking has been favourable to the financial system but not without security threats to banks and non-banks financial institutions and other stakeholders. Neff (2011) claimed that electronic banking fraud was a deceitful behaviour linked to computerisation where people / a person intend(s) to benefit from deception. For every electronic banking service requires the use and adoption of access codes to carry out the services. In spite the introduction of access cipher/code and Personal Identification Number (PIN), these have not completely prevented frauds. There are cases of bank customers that decline the use of electronic banking without any reason, but for the fear of not being hoodwinked. There are some internet fraudsters who adopted phishing to lure victims without in-depth confirmation from the bank by such customers. The chances of identifying the operators and users of electronic transaction systems each time transaction occurs, the fear of being recognised might prevent deceitful plans (Bassey, 2015).

The studies of Abdulrashid et al. (2012), Raja (2012), Adepoju and Alhassan, (2010) agreed that there was a positive relationship between electronic banking fraud and performance of commercial banks in Nigeria. But these studies have not thoroughly examined the exact impact of electronic banking frauds on banks' return on bank performance between 2006 and 2019. Therefore, this research work becomes highly important in filling the existing gap by empirically examining the specific electronic banking fraud platform systems (ATM, POS, mobile banking, internet banking and WEB) on the performance of banks.

Considering the purpose of this study, there is need to construct a null hypothesis (H_0), which is stated as electronic banking frauds have no exact influence on banks' performance. The results of this study would also be invaluable to researchers and scholars, as it would form a basis for further research. The students and academics would use this study as a basis for discussions on influence of electronic banking frauds on banks. Furthermore, the study would also serve as a source of reference material for future researchers.

The second segments of this study captured the literature review, followed by the third segment, methodology, while the fourth segment concentrates more on results and final segment centres on analysis and discussion of findings, conclusion and recommendations.

2. Literature Review

2.1 Electronic Banking Fraud

Universally, the dependence on technology by corporate entities, businesses and access to cyberspace arguably has provided numerous opportunities for electronic deceptions and other forms of manipulations. Fraud is described as sharp practice with intention to cheating others (Nwaze, 2012). Nigeria electronic fraud forum - Neff (2016), described bank fraud as the purposeful execution, or attempts to secure funds, capitals savings, credits, or other investments possessed by or under the guardianship of fraudulent acts', or assurances. To this

extent, the study believed that there is no exact, accepted and specific definition of electronic fraud. The convenience means of completing any task via electronic transactions promotes and increase demand for electronic products and services; and this platform remained an attraction to potential, new and existing clients that have accepted the modern-technological approach of a payment system.

- **The Point-Of-Sale (POS).**

This is a computerised movable machine with a lay out monitor, a barcode scanner, and a card reader that often allows customers with debit / credit cards to conduct banking business both within and outside the banking premises. Besides, the point of sale services qualify customers to negotiate with merchants to trade through cashless payments straightly into the merchant's financial book. The point of sale also assists to display account balances as well as to reproduce small bank financial statement with the use of electronic cards (Owolabi, 2010; Sang, 2012).

- **Automated Teller Machines (ATMs)**

Automated Teller Machines incorporate monitors of computer programme and money basement, which authorises banks' clients the ability to gain entry into its financial recording components with a malleable card that is carved with PIN each time on the condition that there is an internet link and unfluctuating power. Likewise, the machine could be used for both withdrawal and remittances with ease.

- **Telephone Banking**

The number of Nigerians that use telephones is at least one hundred and sixty-five million (165,000,000) and more than nine percent (9%) of the total population use smartphones. The information and communication technology allows bank clients to easily involve in banking business through the use of telephones. It is believed that telephone banking plan guarantees clients comfort during any deal or transactions. There is a very strong association between last long telephone batteries and stable networks; while internet availability and accessibility might be an option. The telephone banking promotes retail banking transaction every time and even the utilisation of unstructured supplementary service data - USSD (Ahmad and Buttle, 2002).

- **World Wide Web**

According to Dong et al. (2010), World Wide site fraud could be identified as Internet banking fraud and perpetrated by employing a cyberspace technology method to illicitly take out funds from an active account and convey same to different accountholder(s). This platform undertakes the use web sites to present dishonest adjurations to eventual victims, to carry out deceitful deals or to transfer the gains of fraud to banks or to others linked with the plan.

- **Internet Banking**

Internet banking fraud relates to specification theft that is carried out by employing online tech and often helped with phishing method to unlawfully take out funds from one accountholder and move it to another separate accountholder (Agboola, 2006; Polasik and Wisniewski, 2008).

2.1.1 Commercial Banks Performance Indicators

Owolabi (2022) and Abdurasheed et al. (2012) defined performance as the way and manner a firm allocates and mobilises resources to generate revenues and achieve its ultimate goals with least resources. Performance claimed to be the achievement of exact corporate intent that is measured against stipulated standards, procedures, practice and cost (Abdurasheed et al. 2012; Dada, et al. 2013). The performance index is Return on Asset (ROA). It controlled and managed commercial banks' assets to boost gain. It helped to exhibit the gainfulness of the

commercial banks prior to leverage. Moreover, it estimated the quantum of yields the Deposit Money Banks (DMBs) would realise on each naira invested on the assets and ascertain the optimisation level of returns on investment that is available to firm's assets (Dada *et al.* 2013).

2.2 Theoretical Framework

2.2.1 Technology Theory

The theory focused on the design and adoption of computer as an acceptance framework to proffer the best solutions that would authenticate, verify, non-repudiate and validate. Fred Davies (1989) propounded theory of Perceived ease-of-use (PEOU). The theory explained degree to which a person believes that using a particular system would be free from effort. The theory emphasised that technology was easy to use, therefore all the barriers were assumed conquered, and suppose it was not easy to use and the interface got complicated, this means no one has a constructive attitude towards it. The theory also assumed that immediately users are able to understand that a type of technology is useful and easy to use, they would be eager to operate it. PEOU was planned to measure the adoption of new technology based on either customers' perspective, belief or attitudes. The implication of this is that if the expectation of an application is to be adopted, the more likely it is that it would be considered appropriate for the user and could stimulate the acceptance of the technology.

2.2.2 Fraud Triangle Theory

The Fraud Triangle Theory was postulated by Donald Ray Cressey (1973). The theory comprised three elements such as pressure, opportunity, and rationalisation. The most pivotal factor was an opportunity. This is as a result of chances available for perpetrating the fraud prompt the fraudsters to execute the fraud. The theory helped to employ an empirically valid clarification of fraud, explaining three basic conditions for atrocities to occur, which include, pressure (perceived unshareable financial need), perceived opportunity (lack of internal controls), and rationalisation (the ability to justify one's actions). This explained how electronic banking frauds were perpetrated in the banks not because of mere peer or societal pressure but because of available opportunities found to commit fraud. The best theory for this study is the technology theory. This is because all over the world, every sector and economies are driven by use and adoption of technology and financial institutions (i.e. banks) are not excluded.

2.3 Empirical Review

Owolabi (2010), studied fraud and fraudulent practices in Nigerian banking industry. Data was retrieved through secondary sources, trend analysis and descriptive analysis were chosen, the findings indicated a very high involvement of employees in fraud between 2004 and 2006 up to 2010. The core fraudulent employee activities were, granting unauthorised loans, posting of fictitious credit, fraudulent withdrawals and forged cheques. Olugbade and Kehinde (2012) investigated adoption of point of sale terminals in Nigeria: Assessment of consumers' level of satisfaction. The study indicated the level of consumers' satisfaction with adoption of e-payment system in Nigeria. Data was elicited from bank's clients that patronise the product / service and collected data were interpreted using descriptive. Findings suggested more opportunities would emanate for people who interface with POS technology in order to achieve the aim of cashless state.

Ololade, et al. (2020) researched on electronic banking fraud in Nigerian banks: Why and how? The study believed that the usage of e-payment platform was a comfortable mode of payment that have increased the extent of occurrence of electronic banking fraud and internet-attacks in banks. The research work adopted survey research design and results showed that

job losses were occasioned by disruptive technologies and economic challenges which led to employees' disengagement without compensation and this might have created fear in the mind of employees to commit electronic banking fraud. Olaleye and Fashina (2019) examined electronic banking fraud in Nigeria: effects and controls. The research adopted case study research design and secondary source of data. The study revealed that there was a significant relationship between e-banking practices in Nigeria and the rate of increase in the security of banking transactions, which has successfully assisted quality service delivery of banks. Amaefule and Onu (2019) studied electronic banking fraud prevalence in Nigeria banking system. Survey research, primary- questionnaire and secondary sources of data were used. The research study recommended the need to concentrate on the best approaches to curtail the problem of electronic banking fraud by reexamining, and strengthening existing security policies that would ensure safety for end-users.

Ibanichuka and Oko (2019) investigated electronic fraud and financial performance of quoted commercial banks in Nigeria. The study employed expost- facto research design and secondary data from 2013 to 2017. The data collected was analysed using basic descriptive, Pearson Product Moment Correlation and multivariate regression in a panel data setting with econometric models were as well adopted. The results showed negative and insignificant relationship between electronic fraud channels and financial performance variables. The conclusion depicted no significant relationship between the electronic fraud and financial performance of quoted commercial banks in Nigeria in the period under review. Owolabi, (2022) examined the relationship among cash flow, firm's size and financial performance of food and beverage companies listed on the Nigerian Stock Exchange. The study concluded that cash flow is more efficient and pragmatic in measuring firm's effectiveness and competitiveness in the financial market.

Nyakarimi, (2022) investigated probable earning manipulation and fraud in banking sector with an empirical study from East Africa. The work examined financial reports of thirty-four (34), thirty (30) and twenty (20) banks in Kenya, Tanzania and Uganda respectively. Beneish and probit regression model were used. Results displayed that 20.6%, 23.3% and 20% of Kenyan, Tanzanian and Ugandan banks respectively involved in fraudulent practice and few banks might be engaging in fraud. Cavaliere et al. (2021) evaluated the impact of internet fraud on financial performance of banks in Lebanon. The research adopted quantitative approach. Results reflected that an increase in number of frauds, adversely affect and depletes the accomplishment of banks.

3. Data and Methods

The Ex post facto research design was employed in the study. The population of the study was twenty-four (24) commercial banks. The sample size was seventeen (17) commercial banks composed of old and new generation banks. The banks were selected due to their high net worth. Secondary data was collected from reports on Frauds and Forgeries in Nigerian Banks, Nigerian Electronic Fund Forum, Nigerian Bureau of Statistics and Central Bank Bulletin for 14 years (2006 -2019). The purposive sampling technique was also used in the study. The collected data was analysed by simple linear regression.

3.1 Model Specification

The specification was based on the hypothesis as earlier stated in the study. The statistical model presented was to determine the extent at which electronic banking frauds affect bank's performance in Nigeria and regression analysis was adopted. Regression analysis was statistical techniques that allowed to forecast a value of one variable on the basis of their scores on other numerous variables (Asika, 1991; Gujarati, 2004; Kiplinger, 2007). To generalise the

model for the study, variable population regression function was expected to be stated thus to achieve objective.

$$Y_i = a + b_1X_{1i} + b_2X_{2i} + b_3X_{3i} + b_4X_{4i} + \mu_i \text{ ----- (1)}$$

Where

Y_i = ith observations on the dependent variables,

a and a_i = are the intercept terms

b_1, b_2, b_3 , and b_4 = partial regression coefficients respectively, whose values are unknown and were to be estimated.

$X_{1i} \dots X_{4i}$ = explanatory variable (or regressor),

$X_{1i} = 1$, for all 'i'

μ_i = the corresponding ith value of the disturbance or error term

'i', = the ith observation.

Where,

ROA = criterion variable measured assets that generated returns for the bank;

f = Specified function

X = regressor variables.

From equation 1 above, it could be adjusted as:

$$ROA_i = \beta_0 + \beta_1ATM_1 + \beta_2WEB_2 + \beta_3POS_3 + \beta_4IB_4 + \beta_5M_5 + \beta_6E_6 + \mu_2 \text{ ----- (2)}$$

A priori, $\beta_1 < 0$; $\beta_2 < 0$; $\beta_3 < 0$; $\beta_4 < 0$; $\beta_5 < 0$; $\beta_6 < 0$.

Table 1: Measuring the variables

S/No	Variables	Measurement	Expected Sign	Apriori
	Bank Performance (ROA) ⁽ⁱ⁾ - Dependent variable	It determines resources that were efficiently and effectively employed to measure the financial status of bank.		
	Independent Variables			
1	Automated Teller Machine- ATM	Electronics device that permits banks' customers to either make cash withdrawals or payments or check account balance(s) at any time.	-	$\beta_1 < 0$
2	World Wide Electronic Banking- WEB	Banking Services enjoyed through websites	-	$\beta_2 < 0$
3	Point of Sale – POS	A terminal and electronic portable device that allows customers to transact with credit / debit cards.	-	$\beta_3 < 0$
4	Internet Banking	Services provided through online banking	-	$\beta_4 < 0$
5	Mobile	Banking transaction through telephone (Unstructured Supplementary Service Data- USSD)	-	$\beta_5 < 0$
6	Ecommerce	Trading that occurs through the usage of electronic banking mechanism	-	$\beta_6 < 0$

Source: Researcher's survey (2022)

4. Analysis and Discussion of Findings

4.1 Descriptive Statistical Analysis of the Data

It is therefore observed that on average as reflected in table 2. PAT was 2.20e+09 with a standard deviation of 2.04e+09. The minimum PAT recorded was 1.42e+08 and a maximum PAT of 5.13e+09. ROA among these banks was approximated at 0.696 while the standard deviation (SD) from this value was approximated at 0.132. It was further revealed that the minimum value (MV) was 0.517 with the highest being 0.902. ATM reported on 1.98e+08 average with standard deviation of 1.98e+08. The least figure recorded was 1.98e+07 while the maximum was 1.98e+08. E-commerce reported on average 7.18e+07 and standard deviation was 8.41e+07. The least figure recorded was 1.43e+07 while the maximum was 3.21e+08. Also, internet banking reported on average 1.22e+08 and a S.D of 1.37e+08. The MV recorded was 2480000 while the maximum is approximately at 3.21e+08. Mobile among these banks was approximated at 8.57e+07 with approximated SD at 1.13e+08. It was further

shown that the minimum value was 1790000 with the highest being 2.48e+08. POS recorded an average worth of 3.95e+07 with a standard deviation of 4.80e+07. The minimum figure recorded was 1530000 while the highest was 1.58e+08. Finally, WEB has its mean value to be 2.18e+08 together with a deviation of 2.35e+08. This is followed by a minimum and maximum values of 1.21e+08 and 1.03e+09 respectively.

In this study, the skewness and kurtosis showed positive values which indicates the basic nature of the variables that are measured. According to Wooldridge (2006) and Gujarati (2004), neither a positive nor negative value poses a problem unless the values fall within a usual limit.

Table 2: Descriptive Statistics

Variable	Obs	Mean	Std.Dev.	Min	Max
PAT	14	2.20e+09	2.04e+09	1.42e+08	5.13e+09
ROA	14	.696	.132	.517	.902
ATM	14	1.98e+08	1.98e+08	1.98e+07	4.98e+08
ECOMMERCE	14	7.18e+07	8.41e+07	1.43e+07	3.21e+08
INTERNETBANKING	14	1.22e+08	1.37e+08	2480000	3.21e+08
MOBILE	14	8.57e+07	1.13e+08	1790000	2.48e+08
POS	14	3.95e+07	4.80e+07	1530000	1.58e+08
WEB	14	2.18e+08	2.35e+08	1.21e+08	1.03e+09

Source: Stata output, 2022

4.2 Normality of Data

The study tested for normality of the residual. Result displayed that residual is non-skewed as illustrated by its scientific significance with a p-value of 0.0000, considering 0.0005 level of significance.

Table 3: Normality test of data

Variables	Obs	adj chi2(2)	Prob>chi2
MODEL Residual	14	2.082	0.353

Source: Skewness/Kurtosis (Jacque Bera) test for Normality STATA output, 2022

4.3 Test for heteroskedasticity

In table 4, the study employed white test that is Cameron & Trivedi's heteroskedasticity which is superior when the error term is in a skewed form as found in table 4. The model revealed that there was no problem of heteroskedasticity as indicated by a p value of 0.1614, which was more than 5%.

Table 4: Cameron & Trivedi's decomposition test for heteroskedasticity

ROA	
chi2	3.65
Prob> chi2	0.1614

Source: Stata output, 2022

4.4 Linear regression Result (ROA)

The table 5 showed the effect of electronic banking fraud payment on ROA. A composite

index representing electronic banking fraud payment was generated from the variables using a principal component analysis (see appendix). The regression result showed electronic banking fraud and how it has affected ROA. By implication, a unit change in fraud payment would bring about 0.039 unit change in ROA. Furthermore, electronic banking frauds activities affected returns on assets generated by the banks. Therefore, for every electronic banking fraud committed, 0.039 returns on assets of banks were impeded. Result was statistically significant, $p < 5\%$. The combined variables explained 37.3% of the variation in the returns as revealed by the value of R^2 . Moreover, other variables justified the remaining 62.7%. This means there were many other variables not captured in this study.

Table 5: Linear regression (Variance covariance estimate robust)

ROA	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
electronic banking fraud payment	0.039	0.015	2.70	0.019	0.008	0.071	**
Constant	0.696	0.029	23.92	0.000	0.632	0.759	***
Mean dependent var	0.696		SD dependent var		0.132		
R-squared	0.373		Number of obs		14.000		
F-test	7.276		Prob > F		0.019		
Akaike crit. (AIC)	-20.539		Bayesian crit. (BIC)		-19.261		

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

Source: Stata output, 2022

4.5 Extent at which Electronic Banking Frauds Affect Bank's Performance in Nigeria.

The coefficient of determinations $R^2 = 0.373$ (37.3%) reported the variations in bank's performance. The result of 37% could be accepted for the study. Overall result was statistically significant at 5%. Therefore, it could be concluded that electronic banking frauds affect bank's performance in Nigeria.

The study explained the extent at which electronic banking frauds affect bank's performance in Nigeria adopting bank's return on assets (ROA) as performance measuring indicator. Findings revealed that by implication, a unit change in electronic banking frauds would bring about 0.039 unit change in ROA; that is, electronic banking frauds activities committed has the chances of affecting the returns on assets by 0.039. The implication of the result is that for every electronic banking fraud perpetrated, 0.039 returns on assets would be hampered to the detriment of the banks.

Findings depicted that combined variables represented 37.3% in the returns' variations as reflected in the value of R^2 . While other variables accounted for the remaining 62.7%. Findings depicted statistical significance ($p < 5\%$) of the variables. This implied that some other factors that were not accounted for in this study that could also affect the bank's performance.

5. Conclusion and Recommendations

The study investigated electronic banking frauds and commercial bank's performance with an empirical prove of Nigeria. The study discovered the different extents at which electronic banking frauds have affected banks' performance through selected electronic payment channels. It was also pertinent to know that banks have intensified efforts in the area of security to protect customers and the banks itself against electronic banking frauds, which were perpetrated by fraudsters, impostors and scammers. It was also important to know that

technology came with its own challenges. Therefore, banks would never stop from providing security to protect customers and entire society against financial risk (e.g. provision of security codes by banks, Personal Identification Number – PIN, Bank Verification Number –BVN, etc.).

Consequently, banks through its electronic transaction mechanisms have remarkably improved on the quality-of-service delivery and satisfying the needs of customers (e.g., customers could transact business without necessarily approaching the bank, this was more obvious during the lockdown as a result of the pandemic outbreak). The study concluded that there were more electronic banking frauds committed through internet banking than other channels.

Based on the findings the following recommendations were made;

- i. Electronic banking fraud (electronic banking fraud) portends a serious exposure risk to the banking subsector and there is need to undertake an efficient and effective risk management procedure, principles and practice to tackle it by policymakers, operators, regulators and other relevant stakeholders.
- ii. There should be concrete collaboration among economic agents; households (citizenry), firms (corporate entities) and governments to effectively and efficiently checking electronic banking frauds. This is because security is not the work of security agencies alone but every stakeholder.
- iii. Management of banks should intensify efforts to improve the issue of security in order to reduce the rate at which electronic banking frauds seriously affected banks' returns during transactions when employing the electronic payment platforms.

References

- Abdulrasheed, A., Babaita, I. S., & Yinusa, M. A. (2012). Fraud and its implication for bank performance in Nigeria. *International Journal of Asian Social Science*, 12(4), 382-387.
- Adepoju, A. S., & Alhassan, M. E. (2010). Challenges of automated teller machine usage and fraud occurrences in Nigeria: A case study of selected banks in Minna metropolis. *Journal of Internet Banking and Commerce*, 15(2), 1-10.
- Adewale, A., A., Ibunni, A., S., Badejo, J., and Odu, T., (2014). Biometric enable e-banking in Nigeria management and customers' perspectives. *Journal of Information and Knowledge Management*, 4(11), 23-28.
- Agboola, A. A. (2006). Electronic payment systems and tele-banking services in Nigeria. *Journal of Internet Banking and commerce*, 11(3), 1-10.
- Ahmad, R., and Buttle, F. (2002). Retaining telephone banking customers at frontier bank. *International Journal of Bank Marketing*, 20(1), 5 -16.
- Amaefule I.A., and Onu F.U. (2019). Prevalence of electronic fraud in Nigeria banking system. *International Journal of Computer Trends and Technology*, 67(3), 77 – 83.
- Asika, P. (1991). *Research methodology and behavioural sciences*. Ikeja: Longmans.
- Bassey, I. E. (2015). Development of a Model of Intrusion Detection Systems for Local Area Networks. A Ph.D Thesis presented to department of computer science, faculty of Science, Ebonyi State University, Abakaliki.
- Cavaliere, L.P., Subhash, N., Rao, P.V.D., Mittal, P., Koti, K., Chakravarthi, M.K, Duraipandian, R., Rajest, S., Suman, S., & Regin, R. (2021). The impact of internet fraud on financial performance of banks. *Turkish Online Journal of Qualitative Inquiry*, 12(6), 8126 -8157.
- Dada, S. O., Owolabi, S. A., & Okwu, A. T. (2013). Forensic accounting a panacea to alleviation of fraudulent practices in Nigeria. *International Journal of Business, Management, Economics and Research* 4(5), 787-792.
- Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information

- technology. *MIS Quarterly*, 13(3), 319-340.
- Dong, X., Clark, J. A., & Jacob, J. L. (2010). Defending the weakest link: Phishing websites detection by analysing user behaviours. *Telecommunication Systems*, 45(2-3), 215-226.
- Gujarati N. (2004). *Basic econometrics* (4th ed.). New Jersey: McGraw-Hill Companies.
- Ibanichuka, E.A.L., & Oko, I. A. (2019). Electronic fraud and financial performance of quoted commercial banks in Nigeria. *International Journal of Advanced Academic Research and Management*, 5(4), 15 -21.
- Kiplinger, P. (2007). *Foundations of research method* (2nd ed.). New York: Macmillan.
- Nigeria Electronic Fraud Forum –Neff. (2016). A changing payments ecosystem: The security challenge.
- Nwaze (2012). Due process and accountancy: Advanced fee fraud. *Zenith Economic Quarterly*, 8(2), 24-28.
- Nyakarimi, S. (2022). Probable earning manipulation and fraud in banking sector. Empirical study from East Africa. *Cogent Economics & Finance*, 10: 2083477, 1 -20.
- Obadeyi, J. A., Oladejo Moruf O. & Adesuyi, I. O. (2018). Evaluating microfinance banks' capacity to purvey credits to micro and small enterprises (MSEs) in South-West, Nigeria: Adopting financial ratio technique. *European Journal of Business and Management*, 10(35), 16-31.
- Olaleye, J. O., & Fashina, A. F. (2019). Electronic banking fraud in Nigeria: Effects and controls. *Global Scientific Journal*, 7(8), 52 – 60.
- Ololade, B.M., Salawu, M.K., & Adekanmi, D.A. (2020). Electronic banking fraud in Nigerian banks: Why and how? *Journal of Financial Risk Management*, 9: 211-228.
- Olugbade, A., & Kehinde, O. (2012). Adoption of point-of-sale terminals in Nigeria: Assessment of consumers' level of satisfaction. *Research Journal of Finance and Accounting*, 3(1), 34 -47.
- Owolabi, S. A. (2010). Fraud and fraudulent practices in Nigerian banking industry. *An International Multi-Disciplinary Journal*, 4(3), 240-256.
- Owolabi, O.Y. (2022). The relationship among cash flow, firm's size and financial performance of food and beverage companies listed on the Nigerian Stock Exchange. *International Journal of Innovative Research & Development*, 11 (6), 42 – 55.
- Polasik, M. & Wisniewski, T.P. (2008). Empirical analysis of internet banking adoption in Poland. *International Journal of Bank Marketing*, 27(1)32 – 52.
- Raja, V. (2012). Global e-banking scenario and challenges in banking system. *Asian Journal of Research in Banking and Finance*, 2(3), 92-101.
- Sang, M. J. (2012). Determinants of fraud control measures in commercial banks: A Survey of selected commercial banks in Nakuru town, Kenya. *International Journal of Science and Research*, 3(10), 2178-2183.
- Taiwo, J., N., Agwu, M., E., Babajide, A., A., Okafor, T., C., & Isibor, A., A., (2006). Growth of bank frauds and the impact on the Nigerian banking industry. *Journal of Business Management and Economics*, 4(12), 1-10.
- Wooldridge, J.M (2006). *Introductory econometric: A modern approach*. International Student edition, (3rd ed.). Canada: Thomson South–Western.

Appendix

Linear regression

ROA	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
logATM	-1.081	0.639	-1.69	0.135	-2.593	0.430	
logECOMMERCE	0.283	0.112	2.53	0.039	0.018	0.547	**
logINTERNETBANKING	0.471	0.318	1.48	0.181	-0.280	1.222	
logMOBILE	0.171	0.129	1.33	0.227	-0.134	0.476	
logPOS	-0.039	0.299	-0.13	0.901	-0.746	0.669	
logWEB	0.180	0.212	0.85	0.423	-0.321	0.682	
Constant	1.834	3.845	0.48	0.648	-7.257	10.926	
Mean dependent var		0.696	SD dependent var		0.132		
R-squared		0.585	Number of obs		14.000		
F-test		12.873	Prob > F		0.002		
Akaike crit. (AIC)		-16.330	Bayesian crit. (BIC)		-11.856		

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

Jarque-Bera normality test: 2.082 Chi(2) .353
Jarque-Bera test for Ho: normality:

Omitted Variable Bias Test

Ramsey RESET test for omitted variables
Omitted: Powers of fitted values of logPAT

H0: Model has no omitted variables

F(3, 9) = 3.31
Prob > F = 0.0712

Heteroscedasticity
Cameron & Trivedi's decomposition of IM-test

Source	chi2	df	p
Heteroskedasticity	3.65	2	0.1614
Skewness	6.03	1	0.0141
Kurtosis	0.09	1	0.7599
Total	9.77	4	0.0445

Principal components (eigenvectors)

Variable	Comp1	Comp2	Comp3	Comp4	Comp5	Comp6	Unexplained
ATM	0.4829	-0.1090	-0.1189	-0.4443	0.1197	0.7274	0
ECOMMERCE	0.3895	-0.2534	0.8687	-0.0076	0.0425	-0.1662	0
INTERNETBANKING	0.4772	-0.0049	-0.3575	-0.2948	0.4106	-0.6236	0
MOBILE	0.4383	-0.3348	-0.2668	0.7834	-0.0325	0.0991	0
POS	0.4154	0.4379	-0.0471	-0.0765	-0.7804	-0.1362	0
WEB	0.1504	0.7874	0.1736	0.3099	0.4530	0.1612	0

Principal Component Analysis