EFFECT OF ELECTRONIC FRAUD ON THE FINANCIAL PERFORMANCE OF BANKS IN NIGERIA

Abstract

The study investigated the effect of electronic fraud on the financial performance of banks in Nigeria. The specific objectives were to investigate the effect of electronic fraud through online web transactions, evaluate the effect of electronic fraud through automated teller machine, to determine the effect of fraud through point of sale machine, and to investigate the effect of fraud through mobile phone USSD transactions on the financial performance of selected deposit money banks in Nigeria. Panel Generalized method of moments (GMM) was used to analyze the panel series of the model. The Hausman test indicated the random effect model as most fit for the estimation. The major findings of the study revealed that fraud through the automated teller machine (AEF) has significant negative impact on the financial performance of the deposit money banks in Nigeria. The panel regression result also revealed that fraud through the mobile phone channel (MPEF), and fraud through the online banking channel (OBEF) had significant negative effect on the financial performance of the banks studied. The study concluded that electronic fraud has significant negative relationship with the performance of banks. The policy implication of these findings holds for both management of banks and the financial sector authorities to engineer strategic fraud mitigation technology to strengthen confidence in the financial system. Based on the findings, the study recommended that there is an urgent need for effective monitoring of bank fraud which will allow for the growth of Nigeria deposit banks performance. This is necessary especially this period that the world is going cashless and e payment instrument are used for cashless banking system. And failure to do that, will affect customer's confidence in the industry. It is also recommended that Bank fraud shall be reduced through effective supervision and regulation of banks by the monetary authorities so that financial industry will contribute to the economy.

Keywords: Fraud, Electronic channels, Deposit Money Banks, Performance

1. Introduction

The channels of financial service delivery by Deposit Money Banks (DMB) and businesses in general have changed dramatically in recent years. The change has afforded customers the ability to transact business, check their account balances, pay power bills and a whole lot more other things using electronic banking right from the comfort of their homes (Muoghalu, Okonkwo & Ananwude, 2018). Electronic banking, according to Tijani and Ilugbemi (2018), has provided the business world with limitless transaction opportunity. Customers and other stakeholders the opportunity to benefit from the flexibility and convenience provided by technology-driven payment solutions. In recent times, transactions between buyers and sellers are conducted

through the use of internet technologies, rather than using cash. “The increased use of e-payment platforms as a preferred method of payment around the world has resulted in an increase in e-fraud incidents in Nigeria. This CBN’s cash-less policy, aims to reduce the amount of cash in circulation and set daily cash limit set by the CBN for both individual and corporate bank customers through channels such as Automated Teller Machines (ATM), Point of Sale Terminals (POS), Mobile payment systems, Internet Banking, Smart TV, and Electronic Fund Transfer” (Tade & Adeniyi, 2018; Elumaro & Obamuyi, 2018). The expansion of the use of technology resulting from the potential enhancement of E-banking and its associated services, has continued to make it easier for clients to conduct monetary transactions

“Electronic banking fraud occurs when the criminal gains access to and transfers funds from an individual’s online bank account. In some cases, an individual may be duped by a criminal into making a fraudulent money transfer themselves. For this to take place, victims are directed, by the criminal to fake websites usually by emails which appear to originate from legitimate sources. The victims are then tricked into revealing personal information, including bank details, this is called phishing or vishing. Vishing takes place when the criminal phones a potential victim and poses as someone from a legitimate organization, such as a telephone company or internet provider” (Hoffmann & Birnbrich, 2012). “The criminal will then attempt to get the customer to disclose personal or financial information, this information can be used by criminals to access online accounts and make fraudulent payments. The criminal uses phishing or other forms of social engineering to obtain the victim’s personal information and then dupes the victim’s bank into believing the victim has changed their address. This allows the criminal to take over the victim’s account. The upward swing in the occurrence of e-fraud in the Nigerian business environment which ranges from identity theft, phishing, to online security breaches through manipulation of account holders by fraudsters has been a major concern to service providers and users of electronic payment platforms in conducting businesses including the regulators” (NDIC, 2018).

“Electronic banking fraud is a major issue that can cause serious financial losses for individuals, businesses, and financial institutions” (Elumaro & Obamuyi, 2018).” It is a serious crime that can occur in many different forms, particularly through electronic modes. These frauds can range from small-scale operations to large, multi-million-dollar operations. It can involve a variety of

techniques, such as creating false accounts, using false identities, or manipulating account records. It can also involve using stolen credit cards, ATM cards, or other forms of unauthorized access to a financial institution's funds. Bank fraud is a major problem for financial institutions and can have a serious impact on their customers. It can lead to the loss of customer funds or the exposure of confidential information".(Elumaro & Obamuyi, 2018)

According to the NDIC annual reports of 2022, it was indicated that electronic financial fraud cases have increased from 26,182 in 2017 to 37,817 in 2022, representing an increase of 44.4%. Besides, the amount involved in the fraud increased significantly by 224% to ₦38.93 billion in 2022 from ₦12.01 billion in 2017. Similarly, the actual amount lost to fraud incidences increased significantly in 2022 to ₦15.15 billion as against ₦2.37 billion and ₦2.4 billion in 2021 and 2020 respectively. Electronic payment channels driven by internet and advanced technology are drivers of these electronic frauds and forgeries that were not only perpetrated by outsiders but also the Staff of the banks. NDIC (2022) reported that 899 Staff of banks were involved in frauds and forgeries in 2022 compared to 320 Staff in 2021.

Scholars have opined that electronic banking have positive correlation with bank performance recent research have also provided evidence that electronic banking is negatively correlated with the financial performance of banks due to electronic fraud. This divergence in opinion motivated the researcher to further investigate the effect of electronic fraud on the financial performance of banks in Nigeria

1.2 Statement of the Problem

Despite the gains of electronic banking through automated teller machines, mobile phone USSD transactions, point of sale banking transactions and the online web transactions, Babatunde, Salawu and Adekanmi (2020) suggested that the adoption of these electronic payment platforms as a convenient means of payment have increased the extent of occurrence of electronic fraud and cyber-attacks in Nigerian Banks.

Every channel of electronic commerce (the ATM, POS, Mobile phone USSD and Online wen transactions) is vulnerable to electronic fraud. Electronic fraud, according to Agboola, (2017), has caused banks' liquidity to plunge and their performance to deteriorate. The rate at which electronic fraud is growing is disturbing, and the options for reducing it aren't promising. This

has resulted in a significant decline in the productivity and performance of Nigeria's deposit money institutions. According to Ikpe and Sinebe (2023) the impact of financial loss caused by electronic fraud on banks' performance in Nigeria has not been fully addressed in studies, and the impact or weight of various channels or tools of electronic fraud on banks' financial performance in Nigeria have not been considered. The broad objective of the study is to investigate the effect of electronic fraud on the financial performance of banks in Nigeria. The specific objectives are:

1. To investigate the effect of electronic fraud through online web transactions on the financial performance of banks in Nigeria
2. To evaluate the effect of electronic fraud through automated teller machine on the financial performance of banks in Nigeria
3. To determine the effect of fraud through point of sale machine on the financial performance of banks in Nigeria
4. To investigate the effect of fraud through mobile phone USSD transactions on the financial performance of banks in Nigeria

2. Review of Related Literature

2.1.1 Financial Fraud

Electronic financial fraud has been variously defined. Fraud can be defined as any illegal act that is characterized by any deceit, concealment or violation of trust (Agwu, 2013).According to Barnabas (2011) fraud is an act or course of deception, deliberately practiced to gain unlawfully or unfair advantages to the detriment of another. Any act of unfair dealing, whether against the bank by his customers or against the customers by the bank (including its officials) is regarded as fraud. Another scholar Idowu, (2009) also sees "fraud as a deliberate falsification, camouflage, or exclusion of the truth for the purpose of dishonesty/stage management to the financial damage of an individual or an organization". "Fraud in its effect reduces organizational assets and increases its liabilities. With regards to banking industry, it may engender crises of confidence among the banking public, impede the going concern status of the bank and ultimately lead to bank failure" (Adeyemo, 2012).

According to Nwobia, Adigwe, Ezu and Okoye (2021), Fraud is an intentional act or omission that aims to benefit one party at the expense of another, whether by misrepresenting the truth or

any other way. Fraud has historically had detrimental effects on banks as well as society at large (Muritala, Ijaiya & Adeniran, 2017). The concern for the banking sector is that if clients choose one bank over another based on its security history—or lack thereof—it may help in increasing its customer base (Aliyu, Tasmin & Takala, 2017; Sinebe, 2021). Although there are many definitions of electronic fraud, they all have as their primary reference the use of an electronic platform and the associated losses since all the transactions necessitate the input of card information (Ibanichuka & Oko, 2019).

The bank fraud does not only effect customers' confidence but also, increase organization's liabilities and by implication reduce it assets which will also reduce the earning per share of organization. According to Kimani (2011) "a way of making money is to stop losing it. The level of fraud in the present day Nigeria has assumed an epidemic dimension. It has eaten deep into every aspect of our life to the extent that a three years old child talks about 419, the name given to the newly discovered advanced fee fraud that is hunting our nation".

According to Abiola, Adedokun and Oyewole (2013) "bank fraud can be categorized in two main groups, namely; internal and external fraud. internalfraud: frauds committed by employees and managers of an organization, either acting alone or in groups or though collusion with outside parties. Management fraud can be quite difficult to detect because managers have access to most information and system and have the power to disguise their actions because they know that their decisions may not necessarily be questioned by others. They can also intimidate junior employees to commit fraud on their behalf; external fraud: fraud committed by third parties of organizations such as suppliers, competitors, partners and customers. Other offenders include potential customers, governments and criminal organizations. The perpetrators can work independently or can collude with staff to defraud the bank. The various types of external fraud witnessed by the bank are money laundering; identify theft and use of lost or stolen documents, use of counterfeit cards, theft and confidential information etc. These types of fraud can be relatively costly if not detected quickly. The probability that the bank could unknowingly be transacting with criminal gangs is very challenging. If for instance such a transaction was to come in the limelight, the bank could face a great damage to its reputation and customer confidence"

2.1.2 Sources of Electronic Financial Frauds

Automated Teller Machine

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 un-fluctuating power. Likewise, the machine could be used for both withdrawal and remittances with ease.

Customers of a bank may now check their account balances and withdraw cash whenever they want without having to go to a human teller thanks to this electronic equipment. Along with cash withdrawals and check deposits, many ATMs also let users transfer funds between bank accounts and even purchase mobile phone recharge cards. Some ATMs charge an additional fee or extra for transactions made at distant locations or by non-members of their organization. When customers of DMB use their credit facilities, their credit cards are linked to their credit accounts rather than their debit cards, which are linked to their DMB accounts via debit cards (Tade et al, 2017).

These are electronic purses that are preloaded by DMB's customers for making payment and settlement of bills. The card could be used on Automated Machine and Point-of-Sales (POS). Pharming or Malware to harvest the security features of the card could be launched by e-fraud perpetrators against the victims. While debit cards are linked to the account of the customers in DBM, credit cards are linked to the credit account on availment of credit facilities to customers of DMB. They are secured with chip and PIN and could be used on ATM, POS and WEB to carry out banking services. Pharming and Skimming attacks. Theft of cards and PIN by the insider e-fraud perpetrators. Unsuspecting victims of e-frauds could also be called over the phone for his security details of the cards by e-fraudsters

Point of Sale Machine

Point of sale is a computerized 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).

Point of Sales Fraud The POS e-banking channel enables customers to pay clients, also known as merchants, for products and services received on the merchants' property (Okechi & Kepeghom, 2017). Customers with cards, such as ATM cards, can conduct financial transactions outside of the bank's premises using a portable device called a POS terminal (Grazioli & Jarvenpaa, 2017). Customers can use the POS services to make cashless purchases of products and services into the merchant's account while transacting with merchants. A credit card or a debit card can be used by the customer to complete other tasks including checking their account balance and printing small bank statements (Khan 2017). Customers and businesses who favour cashless transactions primarily use this route.

Internet Web Banking

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.

The Internet is used to provide financial services to customers through the use laptops, desktops and mobile devices that are internet connected to conduct their banking activities. Fraudsters employ the use of email Phishing to get login information and other system security bypass using a highly skilled and superior understanding of cyber security infrastructure of the bank (Nwakoby & Ananwude, 2019). Since these electronic payment methods enable DMB consumers to make purchases of products and services over the internet from merchant websites without using physical credit or debit cards, the criminals who commit e-fraud steal and use these information for their criminal activities (Omotosho, 2018).

Financial services are delivered to consumers through the Internet (World Wide Web). Consumers transact their banking services (Payment to third parties for goods and services,

confirmation of account balance etc.) through laptops, desktops and mobile devices connected to the internet. The banks provide login details (username, initial password) and physical tokens for transactions' authentications to the consumers. This is e-payment systems that allow DMB customers to pay for goods and services online through the internet without the use of the physical cards on the websites of the Merchants (Airline operators, supermarkets, Telco operators, Government agencies, Schools etc.). It requires the knowledge of the card numbers, PIN and CVV at the back of the e-cards.

Fraud exposure is by phishing Phishing through scam email to harvest login details and subsequent bypass of system security through expert and superior knowledge of cyber-security infrastructure. It also involves wrong account mapping with the intent to commit e-fraud by financial institution employees. Similarly, unsuspecting victims of e-frauds could also be called over the phone for his security details of the cards by e-fraudsters.

Mobile Phone USSD

These are banking services provided by banks via mobile phone technology to its consumers. At the time of opening the account in the bank, Personal Identification Numbers (PINs) are issued and are required from clients for authentication. An e-fraud perpetrator may be able to gain access to this sensitive account information through the theft of the Personal Identification Number (PIN) (Hoffmann & Birnbrich, (2017).

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 smart phones. 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 utilization of unstructured supplementary service data - USSD (Ahmad and Buttle, 2002).

These are banking services delivered to customers of the banks through mobile phone technology. It requires the use of a registered telephone line of the banks' customers at the account opening stage. The GSM line will receive banking transaction alerts and Unstructured

Supplementary Service Data (USSD) platform could be used to transfer fund, pay bills, check account balance and request for account statement. SIM swaps either through theft or in collusion with Telcom agents which will allow the e-fraudster to take over the account from the real owner

2.1.3 Financial Performance

The general definition of a bank's performance is how well the bank has managed its deposits over a given time (often a year) while engaging in trade operations to achieve its goals. A company's performance is typically seen to be reflected in its stock prices and other market activity. Specifically, the value of total assets (TAS) was employed in this study's profitability measures to evaluate bank performance (Abaenewe, Ogbulu,& Ndugbu, 2017). According to Mawutor, Enofe and Embele (2019), a company's ability to utilize its financial resources effectively can be judged by how much net income it generates in comparison to its total assets.

The accomplishment of a given task measured against present known standards of accuracy, completeness, cost, and speed. In a contract, performance is deemed to be the fulfilment of an obligation, in a manner that releases the performer from all liabilities. Performance is an execution carrying out in action the act of performing of doing something successfully using knowledge as distinguished. A company's financial statement is used to show a company's performance over a certain period of time, generally every fiscal quarter. The financial statement really consists of three different statements: statement of financial position, cash flow statements and income statements. By being able to read a financial statement, you can determine where a company has made or lost money, where the money went and how the company stands financially. The financial statement gives shareholders an accounting of how their investment is performing. A company's financial statement is used to show a company's performance over a certain period of time, generally every fiscal quarter. The financial statement really consists of three different statements: balance sheets, cash flow statements and income statements.

The performance of Deposit Money bank’s (DMB’s) exist because of the various services they provide to sectors of the economy, for example, information services, liquidity services, transaction cost services, maturity intermediation services, money supply transmission, credit allocation services, and payment services. Failure to provide these services or a breakdown in

their efficient provision can be costly to both the ultimate sources (households) and users (firms) of savings, as well as to the overall economy. The effect of a disruption in the provision of the various services on firms, households, and the overall economy when something goes wrong in the Deposit Money bank sector makes a case for the need to monitor performance and market value and to impose regulations that in turn affect bank performance and market value (Review of Financial Economics, 2004).

For example, deterioration in Deposit Money bank's performance and value to the point that the bank fails may destroy household savings and at the same time restrict a firm's access to credit. Further, individual Deposit Money bank's failures may create doubts in savers' minds regarding the stability and solvency of Deposit Money banks in general and cause panics and even runs on sound institutions. Although regulations may be beneficial to households, firms, and the overall economy, they also impose private costs that can affect the performance and market value of Deposit Money banks.

There are many ways to determine the financial performance of Bank, depending on the context and also the nature of the research. For the purposes of this research earning per share was considered as the variable to measure bank's financial performance. According to Sani and Alani (2013) financial performance variables that are used to measure banks performance are many, which include earning per share, return on asset, dividend per share and return on equity.

2.2 Empirical Review

Ikpe and Sinebe (2023) examined the effect of electronic fraud on deposit money bank's financial performance in Nigeria from the period of 2009 to 2020 (12 years). In other to achieve this, electronic fraud was measured with Automated Teller Machine Fraud (ATMF), Mobile Payment System Fraud (MPSF), Web/Internet Banking Fraud (WIB), Point of Sale fraud (POSF) against financial performance proxy with Return on Assets (ROA) of Deposit Money Banks in Nigeria. The study made used of aggregate secondary data from Nigeria Deposit Insurance Corporation (NDIC) for the period under study. The correlation analysis was used to ascertain the co-movement of the independent variables in relation to the dependent variable while the Multiple Regression analysis was employed.

Obadeyi, Akande and Jekayioluwa (2022) 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 analyze 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".

Rabiu, Abbah and Lawan (2021) examined "the impact of Bank fraud on the financial performance of Banks in Nigeria, where total actual loss on fraud was used as independent variable. Whereas, earning per share was used as a proxy of Bank financial performance. Secondary data was used from NDIC annual reports and annual financial statement of the Banks. Regression analysis was used to analysed the data with the aid of Eviews 7 software. It was found that, the total actual loss on fraud has significant impact on the earnings per share. It is recommended that, there is an urgent need for effective monitoring of Bank fraud that is done through the various forms of fraud in the Nigerian banking industry, in order to allow for the growth of the Nigerian deposit money banks".

Omodero (2021) assessed how fraud affected the FP of Nigeria's DMBs. Additionally, it looked into the connection between bank performance and ATM fraud, forgery, and clearing check fraud. Regression analysis was the testing methodology used in this research to test its objectives. The research's findings indicated that fraud has a major impact on Nigeria's DMBs FP. The implication is that if commercial banks' levels of fraud do not drop to the absolute lowest, they might not be able to operate effectively and contribute to the expansion of the Nigerian economy.

Babatunde, Salawu and Adekanmi (2020) investigated "why and how e-frauds are perpetrated in the Deposits Money Banks in Nigeria by employees. The survey research design was adopted. Primary data were sourced from 120 fraud investigation officers in the Banks through the administration of structured questionnaires. Data were analyzed using simple percentages. Results revealed that e-frauds were perpetrated by the employees whose employment was threatened as a result of not achieving deposit targets and using either expert or legitimate power

to connive with other employees to commit e-fraud against the Banks. Furthermore, findings revealed that job losses were occasioned by disruptive technologies and economic challenges which often lead to employees' disengagement without or little compensation created fear in the mind of employees to commit e-fraud through Phishing, Pharming, and breach of internal checks. The study recommended that unachievable deposits and sales targets should be discouraged in the Banks through our labour laws. Also, the human resources department of the Banks should institute whistle blowing policy that can assist employees to get a reprieve from a supervisor that may want to influence them using any form of power to commit e-fraud. Finally, it was recommended that e-fraud consciousness of the general users of e-payment channels and employees' sensitization on negative consequences of employees' e-frauds should be heightened through frequent education and continuous training".

Elumaro and Obamuyi (2018) investigated "the relationship between card frauds and customers' confidence in alternative banking channels (e-channels) in Nigeria and found a negative relationship between the two. This is because e-fraud breeds uncertainty in the financial ecosystem and subsequently leads to lack of trust in the alternative banking channels. This will result in the avoidance of e-channels by the public. The study recommended collaborations among the banks and their regulatory agencies to nib at the bud card frauds occurrences. The findings of Elumaro and Obamuyi also conformed with that of Hoffmann and Birnbrich (2012) who asserted that victims of card frauds' confidence and trust in using alternative banking platforms to conduct their business transactions become shaken with a perception that the e-platforms are not safe for their financial transactions". This study is different from the study of (Elumaro & Obamuyi, 2018) in that it focuses on why and how employees of Deposit Money Banks (DBM) commit e-fraud rather than the effect of e-fraud on customers' confidence to use alternative banking channels which is the focus of Elumaro and Obamuyi (2018).

2.3 Theoretical Framework

The fraud triangle theory was adopted for the theoretical framework. The Fraud Triangle Theory was postulated by Donald Ray Cressey (1973). The theory comprised three elements such as pressure, opportunity, and rationalization. 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 rationalization (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.

3. Method, Model and Data

The research design adopted for this study is the *ex post facto.* This choice of this design is due to its suitability in forecasting time series variables. In this design, the use of past values to explain future outcomes is made possible. The processes to be followed will begin with the unit root test of stationarity, followed by the test for co-integration using the Johansen approach and then the ordinary least squares analysis.

The data used for the study were time series and cross-sectional (panel data) sourced from the the annual financial reports of the banks, CBN statistical bulletin, and the Nigerian Stock Exchange annual reports. The data are time series data on the performance of the banks (proxy by value of the total asset of banks); and the electronic fraud (proxy amount of money lost to fraud through ATM, POS, mobile USSD and the Online web banking). The data covers the period 2010-2022.

Model Specification

Functionally, the model is specified below:

TAS = (AEF, PEF, MPEF, OBEF) … 1

Where: TAS = total assets; AEF = automated teller machine electronic fraud; PEF = point of sale machine electronic fraud; MPEF = mobile phone transaction electronic fraud; and OBEF = online banking electronic fraud

The linearized (econometric) model is specified to capyure the time series and cross-sectional effect thus:

$TAS_{it} = \beta 0 + \beta_1 AEF_{it} + \beta_2 PEF_{it} + \beta_3 MPEF_{it} + \beta_4 OBEF_{it} + Ut_{it}$ …2

Where β1, β2, β3 and β4 are the estimated coefficients of the of the financial fraud variables; it= the cross-sectional and time series notations

4. Results and Discussion

4.1 Unit Root Test

Stationarity is an important concept in time series analysis. It usually implies that the statistical properties of a time series (or rather the process generating it) do not change over time. Stationarity is important because many useful analytical tools and statistical tests and models rely on it. Unit root tests can be used to determine if trending data should be first differenced or regressed. Moreover, economic and finance theory often suggests the existence of long-run equilibrium relationships among non-stationary time series variables. Hence, in order to ensure the policy forecasting reliability and suitability of the data employed in this, it was subjected to unit root diagnostic test. For comparison and better standing, the ADF-Fisher Chi-square ant the Philips-Peron unit root tests were carried out, the summary of the result is presented in table 4 below:

Table 1: Unit Root Test Result

ADF-FISHER CHI-SQUARE			**PHILIPS-PERON TEST**			
Variable	**t-stat**	**p-value**	**t-stat**	**p-value**	**Cross section**	**Observation**
TAS	67.2863	0.0000	56.2449	0.0001	11	198
AEF	58.5268	0.0004	63.1297	0.0000	11	198
MPEF	37.1948	0.0225	68.1855	0.0000	11	198
OBEF	52.7101	0.0001	46.5803	0.0017	11	198
PEF	37.9775	0.0184	51.0519	0.0004	11	198

Source: Author's computation (E-views)

The results in table 1 above show that (@ level, the model variable became stationary. Hence, they are integrated of order 1(0). The conclusion of stationarity is based on the fact that following the rule for unit root testing, p-value of the individual (ADF-Chi-square test statistic and the Philips-Peron Test statistics) of the variables is less than the 5% significance level. The

implication of stationary process or series is that the model employed can be relied upon for policy analysis and decision making.

4.2 Descriptive Test

Previewing the descriptive properties of the series (model variables is necessary in order to improve reliability of the findings of the study. The researcher conducted the descriptive test (table 2 below) showing some selected measures of central tendency and dispersion in the model variables (return on assets, fraud through automated teller machine channel, fraud through the interbank settlement channel, fraud through the online banking channel, fraud through the point of sale terminal and the fraud through the mobile phone USSD channel. Measures of central tendency helps to view the points of convergence of the variables and their points of divergence. The major statistics of importance are the mean, the standard deviation, skewness, kurtosis and the Jarque-Bera normality statistic.

Table 2: Descriptive Test Result

	AEF	**MPEF**	**OBEF**	**PEF**	**TAS**
Mean	1.657400	-0.291245	-3.162604	-2.150100	1.483322
Std. Dev.	0.033070	0.036073	0.199344	0.276630	0.139981
Skewness	-1.329976	-0.179273	-1.376382	3.137359	-1.394573
Kurtosis	0.504232	3.321145	2.605273	1.098873	3.071475
Jarque-Bera	77.03896	1.911436	321.7236	2460.310	64.22168
Probability	0.000000	0.004536	0.000000	0.000000	0.000000
Observations	198	198	198	198	198

Researcher's Computation using (E-views)

From the result of the descriptive test above, the return on asset averaged 1.483% annually across the banks studied. The amount of fraud through the various channels averaged 1.657 billion naira, 1.681 billion naira, 3.163 billion naira, 2.150 billion naira and 0.291 billion naira for ATM channel, interbank settlement system, online web banking, point of sale, and the mobile phone USSD channels respectively.

To check the spread or changes in the series, the standard deviation test produced the result as seen on table 2 above. The standard deviation statistic indicated values of 0.139, 0.033, 0.199, 0.276, and 0.036 for TAS, AEF, OBEF, PEF and MPEF series respectively.A higher standard deviation value indicates greater spread in the data and negates joint influence. The safe value

tends towards zero so that the closer the deviation is to zero, the better the result. As indicated in the result, the values were in tendency towards zero, hence the series are from a normal distribution. Also, skewness defines the extent to which a distribution differs from a normal distribution, when data are skewed, the majority of the data are located on the high or low side of the graph. The descriptive result showed that the series were negatively skewed and concluded they have a normal distribution.The statistical result equally indicated that all the variables have a positive kurtosis. The Jarque-Bera normality statistic also confirms the series to be from a normal distribution (as indicated by the p-values) for each of the model series.

4.3 Correlation Test

Correlation test was used to ascertain the strength and magnitude of the relationship between the dependent and independent variables. The result of the correlation test is presented in table 3.

Table 3: Correlation Test Result

	TAS	AEF	MPEF	OBEF	PEF
ROA	1.000000				
AEF	0.402103	1.000000			
MPEF	-0.386854	0.415546	1.000000		
OBEF	-0.669121	-0.126016	-0.117657	1.000000	
PEF	-0.162316	0.070808	0.135212	-0.215448	1.000000

Authors' Computation 2023 (Using E-views)

The correlation test result on table 3 above shows the correlation of the dependent variable (the financial performance of the banks) and the independent variables (the financial fraud channels). The relationship appeared negative across board, and the strength of the correlation differed. The strength of the correlation indicated 40.21%, 10.26%, 38.69%, 66.91%, and 16.23% respectively for automated teller machine electronic fraud (AEF), mobile phone USSD channel, online web banking channel and point of sale channel respectively. This implies that electronic fraud have (inverse) relationship or is negatively correlated with the financial performance of the deposit money banks.

4.4 Effect of Fraud on the Financial Performance of Banks in Nigeria

The broad objective of this study is to investigate the effect of fraud on the financial performance of banks in Nigeria. To achieve this, the researcher employed the panel regression technique to estimate the coefficients of the model variables. The panel estimation was in three phases (the pooled regression phase, the fixed effect regression phase and the random effect regression

4.4.1 Panel Regression Analysis

Table 4: Summary of pooled, fixed effect and random effect regression results

Series	Pooled regression (1)	Fixed effect regression (2)	Random effect regression (3)
C	-	15.16052 [0.0000]*	15.82932 [0.0000]*
AEF	0.828779 [0.0000]*	1.008542 [0.0000]*	-3.015834 [0.0003]*
MPEF	-0.779099 [0.0000]*	-0.030825 [0.6620]	-0.295478 [0.0179]*
OBEF	68.66113 [0.0000]*	-1.882445 [0.4792]	-8.010412 [0.0417]*
PEF	2.530107 [0.0041]	4.861008 [0.0098]*	-1.380107 [0.3041]
OBSERVATION	198	198	198
R-SQURAED	0.469390	0.970958	0.635417
F-VALUE	-	405.6586 [0.000000]	14.409930 [0.00027]*

Source: Authors' computation 2023 (E-views)

** indicates 5% level of significance

On table 4, the study considered the pooled panel regression. Observing this result, the study pools all 198 observations together and ran the regression model, neglecting the cross section and time series properties of the data. It was found that the R-squared value for the pooled regression model is 0.469390 indicating that about 46.94% of the total variation in the financial performance of the selected banks (TAS) is explained by the explanatory variables (the financial fraud variables: online web banking channel fraud, point of sale banking channel fraud, automated teller machine channel fraud, and the mobile phone USSD banking channel fraud). More so, all the channels of financial fraud indicated to be significant in influencing the performance of the banks. This is confirmed by the P-values [AEF: 0.0000, MPEF: 0.0000, OBEF: 0.0000 and PEF: 0.0041]. Also the coefficients were positive except the mobile phone USSD banking channel fraud. The major problem with pooled regression model is that it does

not distinguish between the various firms that are in the sample. In other words, by combining different firms through pooling, the heterogeneity or individuality that may exist among the selected firms is not considered.

In order to allow for heterogeneity or individuality among the firms by allowing each of the Banks to have its own intercept value; the fixed effect model (FEM) was applied. This became necessary because it is time invariant indicating that although the intercept may change across the individual banks, it however does not change over time. From the fixed effect result (table 4 above), the coefficient of determination (R-squared) value of 0.970958 indicates that approximately 97% of the total variation in the performance of the banks is explained by the financial fraud variables. While only the mobile phone USSD (MPEF) banking channel fraud and the online web banking channel fraud showed to be negative in influencing the banks' performance; the automated teller machine channel fraud, and the point of sale channel fraud were positive. However, only the automated teller machine electronic fraud (AEF) and point of sale turn up significant.

Panel series can show unobserved properties. The pooled panel regression and the fixed effect regression do not take care of such. The random effect regression model was applied in order to account for the unobserved effects in fixed effect model.The random effect regression results indicated that all the financial fraud variables were significant except the point of sale channel. However, all the financial fraud channels were indicated to be negative. The negative coefficients are a further indication that fraud through these channels has negative influence on the performance of the banks. The random effect model showed that (63.54%) of the total variations in the financial performance of the selected banks under study are accounted for, by the explanatory variables (financial fraud through the various electronic channels). This is evidenced from the R-squared value of 0.635417. The output values indicate that all the financial fraud variables (as modeled) significantly and jointly influence financial performance (the total assets) as confirmed by the P-values [AEF = 0.0003, MPEF = 0.0179, OBEF = 0.0417 and PEF = 0.3041].

4.5 Hausman Test of Model Selection

To affirm direction and properly inform policy statements arising from the study, there is need to decide between the fixed effect model and the random effect model, the Hausman test solves this. The Hausman test selects the model most appropriate for estimation; it is performed under null hypothesis that the random effects model is the most appropriate. In the alternative, the fixed-effects model is appropriate. The selection of either fixed effect model or random effect model is based on the statistical significance of the P-value.

Table 5: Correlated Random Effects - Hausman Test
Equation: Untitled
Test cross-section and period random effects

Test Summary	Chi-Sq. Statistic	Chi-Sq. d.f.	Prob.
Cross-section random	4.073810	5	0.5388
Period random	2.680991	5	0.7490
Cross-section and period random	4.700015	5	0.4536

Source: Authors' Computation 2023 (Using E-views)

Following the result in table 5, the Hausman test statistics p-value for the cross-section random, period random, and the cross-section and period random are [0.5388, 0.7490 and 0.4536] respectively. This is greater than the 5% (0.05) chosen level of significance. Consequently, the null hypothesis cannot be rejected. Therefore, it was concluded that cross-section random effect model is desirable for prediction. The random effect panel regression result presented in table 5 above, revealed that the fraud through the automated teller machine (AEF) has significant negative impact on the financial performance of the deposit money banks in Nigeria. This result is in conformity with the apriori expectation that financial fraud is a negative determinant of performance of banks. The panel regression result also revealed that fraud through the mobile phone channel (MPEF), and fraud through the online banking channel (OBEF) had significant negative effect on the financial performance of the banks studied.

5. Summary, Conclusion and Recommendation

The first specific objective of the study was to investigate the effect of amount lost to fraud through automated teller machine (LOGATM) on the financial performance of deposit money banks. From the results obtained, the estimated coefficient value for financial fraud through

(ATM) is -3.015834, with p-value of 0.0003. This implied that fraud through the automated teller machine channel has significant negative effect on return on assetsof selected sample banks in Nigeria. In comparison with other empirical findings, this result agrees with Ashiru, Balogun and Paseda (2023) which investigated the impact of mobile, internet, and automated teller machines (ATMs) on banks' financial performance. Bank fraud is a major issue that can cause serious financial losses for individuals, businesses, and financial institutions (Elumaro & Obamuyi, 2018).

In the second objective of the study, the researcher evaluated the effect of mount Lost to Fraud through Online Banking on Financial Performance of Selected Deposit Money Banks in Nigeria. From the results we obtained, the estimated coefficient value for online web banking fraud (LOGOWF) is -8.010412, with a p-value of 0.0417. It was indicated that there is significant positive effect of online banking fraud on return on assetsof the sampled banks. For empirical comparisons, the study disagreed with the findings of Rufus , Olubunmi, Modupe and Abimbola (2022) which examined the impact of cyber security and financial innovation of selected deposit money banks in Nigeria. Scholars have opined that electronic banking have positive correlation with bank performance, recent have also provided evidence that electronic banking is negatively correlated with the financial performance of banks due to electronic fraud.

In the third objective of the present study, the researcher determined the effect of amount lost to fraud through the point of sale (LOGPOS) is -1.380107 with a p-value of 0.3041. By implication, fraud through the point of sale channel has insignificant negative effect on return on assetsof the selected banks. Point of Sales Fraud The POS e-banking channel enables customers to pay clients, also known as merchants, for products and services received on the merchants' property (Okechi & Kepeghom, 2017). Customers with cards, such as ATM cards, can conduct financial transactions outside of the bank's premises using a portable device called a POS terminal (Grazioli & Jarvenpaa, 2017). Customers can use the POS services to make cashless purchases of products and services into the merchant's account while transacting with merchants. A credit card or a debit card can be used by the customer to complete other tasks including checking their account balance and printing small bank statements (Khan 2017). Customers and businesses who favour cashless transactions primarily use this route.

The fourth objective of the study investigated the effect of fraud through mobile phone USSD channel on the performance of selected deposit money banks in Nigeria. From the results obtained, the estimated coefficient value for mobile USSD fraud (LOGMPU) is -0.295478, with p-value of 0.0179. This imply that there is significant negative effect of mobile phone related fruadon return on assets of the selected deposit money banks in Nigeria. Asogba, Ariyibi & Soyemi (2023) also offer consistency with this study. These are banking services provided by banks via mobile phone technology to its consumers. At the time of opening the account in the bank, Personal Identification Numbers (PINs) are issued and are required from clients for authentication. An e-fraud perpetrator may be able to gain access to this sensitive account information through the theft of the Personal Identification Number (PIN) (Hoffmann & Birnbrich, (2017).

Thus, every channel of electronic commerce (the ATM, POS, Mobile phone USSD and Online web transactions) is vulnerable to electronic fraud. Electronic fraud, according to Agboola, (2017), has caused banks' liquidity to plunge and their performance to deteriorate. The rate at which electronic fraud is growing is disturbing, and the options for reducing it aren't promising. This has resulted in a significant decline in the productivity and performance of Nigeria's deposit money institutions. Hence, based on the results, this study concluded that electronic fraud had significant negative effect on the sample deposit money banks in Nigeria for the period studied. The study thereby recommended that there is an urgent need for effective monitoring of bank fraud which will allow for the growth of Nigeria deposit banks performance. This is necessary especially this period that the world is going cashless and e payment instrument are used for cashless banking system. And failure to do that, will affect customer’s confidence in the industry. It is also recommended that the Bank fraud shall be reduce through effective supervision and regulation of banks by the monetary authorities so that financial industry will contribute to the economy.

References

Akinyomi, O. J. (2012). Examination of Fraud in the Nigerian Banking Sector and Its Prevention. *Asian Journal of Management Research, (3) 184-192*.

Albrecht, C., Albrecht, C. C., Wareham, J., & Fox, P. (2008). The Role of Power and Negotiation in Online Fraud. *Journal of Digital Forensics, Security and Law, (1), 29-48.*

Button, M., Lewis, C., & Tapley, J. (2014). Not a Victimless Crime: The Impact of Fraud on Individual Victims and their Families. *Security Journal, (27), 36-54.*

Cressey, D. (1953). Other People's Money: A Study in the Social Psychology of Embezzlement. Glencoe, IL: Free Press

Elumaro, A. J., & Obamuyi, T. M. (2018). Cards Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria. *European Scientific Journal, 14, 40-60*

Fernandes, L. (2013). Fraud in Electronic Payment Transactions: Threats and Countermeasures. *Asia Pacific Journal of Marketing and Management Review, 2, 23-32.*

Grazioli, S., & Jarvenpaa, S. L. (2003a). Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence. *International Journal of Electronic Commerce, 7, 93-118.*

Grazioli, S., & Jarvenpaa, S. L. (2003b). Deceived: Under Target Online. Communications of the ACU, 46, 196-205.

Hoffmann, A. O., & Birnbrich, C. (2012). The Impact of Fraud Prevention on Bank-Customer Relationships: An Empirical Investigation in Retail Banking. *International Journal of Bank Marketing, 30, 390-407*.

Ibor, B. (2016). An Investigation of Human Resources Nexus to Frauds in the Nigerian Banking Sector. *International Journal of Scientific and Research Publications, 6,*