JOURNAL OF GLOBAL ACCOUNTING
10 (1) April, 2024.
ISSN (Online): 1597–7641; ISSN (Print): 1597-8273
https://journals.unizik.edu.ng/joga

BANKS AND WAR AGAINST FINANCIAL CRIME IN NIGERIA DIGITAL PAYMENT SYSTEM

Amara P. Ozoji, PhD[1] Beatrice O. Ezechukwu, PhD[2] Nwariaku S. Ihechiluru[3]

[1&3]*Department of Accountancy, University of Nigeria Enugu Campus, Enugu, State, Nigeria.*
[2]*Department of Accountancy, Federal Polytechnic, Oko. Anambra State, Nigeria.*

1. Email: amara.okoye@unn.edu.ng
2. Email: beatriceezechukwu@gmail.com
3. Email: nwariaku.ihechiluru@unn.edu.ng

Correspondence: *amara.okoye@unn.edu.ng*

Key words *Digital payment system, Financial Crime Fraud, Forgery, Security Measures, War.*

CITATION: Ozoji, A.P., Ezechukwu, B.O. & Ihechiluru, N.S. (2024). Banks and war against financial crime in Nigeria digital payment system, *Journal of Global Accounting*, 10(1), 191 – 208.

Available:https://journals.unizik.edu.ng/joga

ABSTRACT:

The study on banks and war against financial crime in Nigeria, primarily aimed at assessing the effectiveness of the banks' security measures in fighting financial crimes in Nigerian digital payment system. Bi-monthly data of the entire Deposit Money Banks operating in Nigeria as at 2012-2021 computed from the extracts from NDIC annual reports (2013, 2017, 2019 and 2021) and CBN Statistics Database (2012-2020) were used. Auto regression Distributed Lag (ARDL) model estimation was utilized for data analysis/test of hypotheses. Findings disclosed that banks' security measures are partially effective in the fight against frauds and forgery in Nigeria's digital banking system, as digital payment transactions (with the existing fraud prevention tools) through ATM and mobile phones have depressed the opportunity to commit fraud, while reverse is the case with POS transactions and internet banking. The study recommended among others that banks should install a good fraud linking software in all electronic payment channels with more focus on POS terminals and internet, which can aid the bank view relationships between transactions through identifiers like passwords, usernames, and others. This would help to disclose with relative certainty that a transaction may be fraudulent since the individual carrying out the transaction has previously carried out a confirmed fraudulent transaction, thereby facilitating fraud prevention..

1. INTRODUCTION

In Nigeria, banking sector is seen as a veritable goldmine for financial fraudsters due to the nature of its business. Banks deal in valuable financial information from various customers, multitudes of different currencies on daily basis and trade with different individuals and corporate organisations all over the world. Hence, they remained the most attractive sector for financial frauds, among all the sectors of the economy. Today, individuals, corporate

bodies and governments are losing huge sums of money and properties as a result of financial crimes. The digital economy solution for country's survival in the 21st century world of increasing advancement in information and technology (Okoye, 2018) which has triggered a journey of Nigeria towards a digitalized economy, where electronic transactions increasingly play a dominant role in the financial system, has worsened the ugly situation as these fraudsters became more sophisticated. According to NDIC (2021), the digital banking channel sources of fraud have accounted for the highest total fraud cases and actual loss of 88.74% and 69.10% respectively in the year, 2021. Ozoji et al. (2021) maintained that ATM, POS, mobile phone banking and internet banking are the main digital banking products of Nigerian banks since Nigeria witnessed the dawn of cash-less banking, resulting from the cashless policy introduction by the CBN in the year 2012.

Hence there exists a war on financial fraud across all the banks in Nigeria. Three major groups called Insiders, Outsiders and Outsiders/Insiders are waging a high-level insurgency that has inflicted millions of financial losses to the banks and the economy. Insiders involve the management of the bank at all levels who perpetrate management fraud and induced financial injuries to their victims, usually the investors and creditors; as well as the staff of the banks that are attracted to perpetrate employees or non-management frauds like cash thefts from the tills, forgery of customer's signature for illegal withdrawal of customer's money with the bank, opening and operating a fictitious account for illegal banking transactions and a host of others. While Outsiders are customers and other individuals that do not work with the bank but inflict financial injuries to the banks and the consumers through their illegal acts like advance fee fraud (419), cybercrime or computer fraud, cheque fraud, armed robbery and many others. Outsiders/Insiders involve insiders conniving with outsiders to brazenly attack the security installations in the banks. Olaoye et al (2014) as cited by Adekola (2017) maintained that Outsiders/Insiders frauds will only be successful when an insider is providing the necessary information and other logistics in secrete to the outsiders. The war on financial crimes among the three groups above has affected the banks severely as customers have lost confidence in banks.

In the fight against financial crimes in Nigerian banking system, Adelabu (2016) stated that the warfare of banking security has continued to change in response to the rapid developments in payment technology. The principal regulatory authorities of banks and other financial institution in Nigeria (CBN and NDIC) have over the years, issued several policies, circulars, rules and regulations in a bid to ensure the financial well-being of banks and their customers. Some of the regulations/circulars issued by CBN to the deposit money banks and other financial institutions are circular on the need to combat card fraud, introduction of 'Know

Your Customer' (KYC) principle and the use of National Identity Number (NIN) for the' Know Your Customer' (KYC) verification, need to install anti-skimming device on all ATM terminals, introduction of Bank's Verification Number (BVN) project and linking the BVN to customer's account on the core banking applications by banks, implementation of two factor authentication for internal banking processes, establishment of industry fraud desks in all deposit money banks, cybercrime (prohibition, prevention and others) Act, 2015 and 2018 risk-based cyber-security framework and guidelines for DMBs and Payment Service Providers (CBN Rule Book, 2019). Most of these regulations aid the banks in setting, reviewing and strengthen their internal control system, corporate governance and banking ethics, all in the bid of fighting frauds. NDIC Act of 2006, in its section 35 and 36 required all insured banks in Nigeria to furnish returns on frauds and forgeries or outright theft occurring in their organizations and also report on any staff dismissed, terminated or advised to retire on the grounds of fraud. This can assist the banks and the regulatory authority to monitor the trend of frauds in the banks and the system of the perpetrators' operation in other to determine the best way of curbing the financial crimes.

Amidst all the security measures above, yet there is still high rate of frauds/financial crimes in the banking sector, that many people have started questioning the effectiveness of the strategies employed by banks in the fight against financial frauds in Nigeria' digital environment. There exists paucity of empirical studies on the success rate of banks' security measures in the fight against financial frauds in Nigeria's digital payment system. The few earlier studies conducted on the subject during cashless era in Nigeria (Adesuyi et al. 2013; Eme et al., 2016;Adekola, 2017; Enofe et al., 2017; Chika et al., 2022; Ogwiji and Lasisi, 2022) used survey instrument of data collection, and their results disclosed mixed findings of positive and significant influence of the security measures on fraud prevention and control (Adekola, 2017; Enofe et al., 2017; Chika et al., 2022; Ogwiji and Lasisi, 2022) as well as the existence of inadequate security necessary to secure electronic transactions, customer's information and funds with the existing security implementation in the banks (Adesuyi et al., 2013; Eme et al., 2016). And this brings uncertainty in concluding whether the security measures of banks are effective in fighting frauds in Nigeria. Hence the need to use a more objective method of data collection that can reduce bias response when assessing the effectiveness of the security measures in fighting frauds in Nigerian banks. Therefore, this study made a difference in the methodology by using documentary method (secondary sources) of data collection to obtain data already in existence even before the research started, to determine the effectiveness of fraud prevention and control tool performance in fighting against financial crime in Nigerian's digital payment system.

JOURNAL OF GLOBAL ACCOUNTING
10 (1) April, 2024.
ISSN (Online): 1597–7641; ISSN (Print): 1597-8273
https://journals.unizik.edu.ng/joga

1.1 Objective of the Study

The broad objective of the study is to evaluate Nigerian banks' security measures through the examination of the digital payments transactions amidst the existing fraud preventive strategies in Nigeria's digital banking system, in order to determine the effectiveness of the fraud prevention tools in war against financial frauds in Nigeria. Specifically, the study aimed at determining the:

1. effect of the core digital payment transactions (ATM, POS, Mobile phone and internet) amidst banks' security measures (DPTBSM) on Fraud success rate (FSR) in Nigeria's deposit money banks (DMBs).

1.2 Hypothesis

H_O: The core digital payment transactions (ATM, POS, Mobile phone and Internet banking) amidst banks' security measures has no significant effect on the fraud success rate in Nigeria's DMBs.

2. LITERATURE REVIEW

2.1 Conceptual Review

2.1.1 Banking Transactions in Nigeria

In Nigeria, the business of banking was initially concerned with the acceptance of deposits on customers' accounts, payments for customers' withdrawals through cheques and pass books, as well as granting credit facilities to banks' customers, through the physical presence of the customers or their agent, client or creditor in the bank premises (Okoye, 2018). Advancement in information and technology witnessed in the 21st century world later re-directed the scenario to the idea that individuals and corporate bodies can also have access to savings, payments and other bank's products with the aid of electronic devices, without their physical presence in the bank. This resulted to the emergency of electronic banking in Nigeria, which was used as a platform to introduce cash-less banking in the country, with the introduction of cash-less policy by the CBN in 2012 (Ozoji et al., 2021). Since the introduction of cash-less policy, the digital banking transactions now dominated cash-based banking transactions in Nigeria. Digital banking transactions involve the use of digital or electronic devices like point of sale (POS) terminals, automated teller machine (ATM), mobile phone, internet and others to perform banking operations. CBN (2021) viewed electronic transactions (payment) to have been possible as a result of the existence of electronic money, which is a stored-value product in which a record of the value available to consumer for multipurpose use is stored on an electronic devise held by the consumer. The use of POS terminals, ATM, mobile phone,

internet and others to perform banking operations have continuously been on increase since the implementation of cash-less policy, and has risen the vulnerability of banks to frauds. Consequently, war on insecurity of banking transactions in Nigeria is witnessed in Nigeria among two major parties that are for the war (fraudsters) and against the war (banks).

2.1.2 War on Financial Crime in Nigerian Banks

Financial crime involves unlawful conversion of the ownership of one's property to another person's own personal use and benefit. However, financial crime in the banks could simply be seen as illegal conversion of the customers' transactions, money and information with the bank to another person's ownership and/or benefit. The major avenue of financial crime in Nigerian banks is banks' frauds. Fraud generally means an intentional act of deceit by someone to another, with the purpose of gaining an advantage from the deceived person whom the act would inflict legal injury. Bank fraud on the other hand involves an illegal means of obtaining banks or customers information, money and properties held in the banks by individuals or corporate bodies. Nwankwo (2013) as cited in Mawutor, et al. (2019) viewed damages in monetary value as the end product of frauds to businesses or countries. Ovuakporie (1994) opined that most of the common bank frauds are theft and embezzlement, defalcation, forgeries, unofficial borrowing, foreign exchange malpractices, impersonation, manipulation of vouchers, falsification of status report, money laundering, fake payments and computer fraud.

Three major groups called Insiders, Outsiders and Outsiders/Insiders are waging a high-level insurgency that has inflicted millions of financial losses to the banks and the country at large. Insiders involve the management of the bank at all levels who perpetrate management fraud and induced financial injuries to their victims, usually the investors and creditors; as well as the staff of the banks that are attracted to perpetrate employees or non-management frauds like cash thefts from the tills, forgery of customer's signature for illegal withdrawal of money from the customer's account with the bank, opening and operating a fictitious account for illegal banking transactions, used of forged cheque to withdraw money from the customer's account and a host of others. Olaoye, Dada and Adebayo (2014) as cited in Adekola (2017) added that financial statement is the medium for perpetration of management fraud. Employees may be tempted to commit fraud due to lack of good welfare package. While Outsiders are customers and other individuals that do not work with the bank but inflict financial injuries to the banks and the consumers through their illegal acts like advance fee fraud (419), cybercrime or computer fraud, cheque fraud, armed robbery, and many others. Outsiders/Insiders involve insiders conniving with outsiders to brazenly attack the security

installations in the banks. Olaoye et al (2014) as cited by Adekola (2017) maintained that Outsiders/Insiders frauds will only be successful when an insider is providing the necessary information and other logistics in secrete to the outsiders.

The war on financial frauds in Nigerian banks is more pronounced with the adoption and usage of IT-driven banking instruments. ATM fraud was recorded as the most attempted fraud incidents in 2016 with 491 incidents; while internet banking had the highest fraud value of 3.2 billion Naira in the same year (Nigeria Inter-Bank Settlement System Plc ‘’NIBSS’’ report, 2016 as cited by Awelewa, 2016). NDIC annual report of 2013 and 2019 disclosed increased cases of frauds and forgeries in Nigeria’s DMBs from 3,380 in 2012 to 52,754 in 2019 respectively. While NDIC (2018) attributed the rising fraud incidences to rise in sophistication of fraud related techniques like hacking and cybercrime, as well as hike in the use of information technology-related products. War on financial crime in the banks has negative implications as it has eroded customers’ confidence in the banking sector. This has severely affected the banks and the country, that there arose a concern as to whether the banks can fight against the three major groups stated herein.

2.1.3. Banks War against Financial Frauds in Nigerian Banks

CBN has over the years, issued several policies, circulars, rules and regulations to deposit money banks (DMBs) and other financial institution in a bid to fight financial crime in Nigerian banks. DMBs on their part have employed several security measures that can be classified into three major parts in fighting financial crime in the banks. These include compliance with the banks’ regulatory authorities’ regulations and policies, establishment of strong internal control system and maintenance of good corporate governance.

a. Compliance with the banks’ regulatory authorities’ regulations and policies: In Nigeria, the two major regulatory authorities of banks are the CBN and NDIC. Some of the regulations/circulars introduce by CBN to DMBs in fight against frauds in the banks include the need to combat card fraud firstly issued in 2010 and re-issued in 2011; introduction of ’ Know Your Customer’ (KYC) principle and the use of National Identity Number (NIN) for the’ Know Your Customer’ (KYC) verification issued in 2012; need to install anti-skimming device on all ATM terminals issued in 2014; introduction of Bank’s Verification Number (BVN) project, launched 2014 and linking the BVN to customer’s account on the core banking applications by banks, reviewed in 2015; regulatory framework for the use of unstructured supplementary service data (USSD) for financial services in Nigeria; implementation of two factor authentication for internal banking processes, 2015; establishment of industry fraud desks in all deposit

money banks issued in 2015; cybercrime(prohibition, prevention and others) Act, 2015 and 2018 risk-based cyber-security framework and guidelines for DMBs and Payment Service Providers (CBN Rule Book, 2019). Evident of DMBs' compliance to the CBN' s regulations above could be seen in the introduction of different USSD code by different DMBs as a solution that allows customers act swiftly to prevent fraudulent activities on their accounts, like *901*911# is the USSD code for access bank plc; proper capturing and validating of the BVN data of DMBs' customers as well as linking all operated accounts with the signatories' BVN. No wonder a customer cannot withdraw from his Nigeria's resident's bank account without BVN. Also, DMBs now established fraud desks and also make available email address and phone numbers to the customers for any fraud's complaints. Nlebem (2021) discloses access bank plc's contact centre's phone number and email as 01-2712005 and contactcenter@accessbankplc.com and frauddesk@accessbankplc.com for customers to report any suspicious activity on their accounts.

In compliance with section 35 and 36 of NDIC Act, 2006, DMBs among others render to the corporation, the total amount of incidences of attempted/reported fraud and forgery in their organisations and the actual amount loss to fraud and forgery in their banks. This could assist in ascertaining the fraud success rate in these banks in order to determine the effectiveness of already introduced security measures in the banks. It could also help to monitor the trend of frauds in the banks as well as the system of the perpetrators' operation in other to determine the best way of curbing the financial crimes.

b. Establishment of strong internal control system: Internal control system is the whole system of control, financial and otherwise established by the management in order to carry on the business of an enterprise in an order and efficient manner, ensuring adherence to management policies, safeguarding the assets and secure as far as possible the completeness and accuracy of records (ICAN, 2010 as cited in Enofe, Abilogun, Omoolorun and Elaiho, 2017). Ajala, Amuda and Arulogun (2013) opined that internal control system has significantly prevented and curbed frauds in Nigerian banks. While Enofe et al discovered strong internal control system as one of the items that positively and significantly influenced fraud prevention in banking industry.

c. Maintenance of good corporate governance: Corporate governance is the mechanism by which managers are selected, motivated and also made to be accountable for resources entrusted to them. Good corporate governance is a set of mechanisms designed to promote reliable and strong banking industry that will ensure the safety of depositors' funds, and also protect outside investors from expropriation by insiders (management).

Banks establish directorship, internal auditing and external auditing as the monitory mechanisms in ensuring good corporate governance. Hunkin (2002) opined that an effective board of corporate governance would provide a check and balances on management without being compromise to ensure fraud prevention. Hence, good corporate governance checks management fraud.

2.1.4 Fraud Success Rate (FSR) In Digital Payment System

FSR simply means the rate of success in banks' fraud. It is not all the fraudsters that manipulated the digital payment channels are successful. The level and volume of attempted frauds may rise while the success rate of fraud may decline due to the effectiveness of fraud prevention tools employed by banks to check frauds. The major challenge encountered by banks in allowing many fraudsters to game banking system successfully is the reputational risks. Hence there is need to measure the success rate of fraud prevention strategies and not just introduction of such strategies.

2.2 Theoretical Review

This study is based on fraud triangle theory. Fraud triangle theory maintained that an individual could only perpetrate fraud if the following three elements - pressure, opportunity and rationalization exit. The theory was developed by Donald Cressey in 1950's (Mawutor et al., 2019). Individuals are motivated to commit fraud when there is pressure from various sources like monetary needs, urge for modernisation and globalization. But the motivated prospective fraudster could not actualize the perpetration of the fraud if opportunity was not given. Hence it can be stated that opportunity is the most important element among the three conditions that must exist for fraud to be committed. Weak security measures could create opportunity for frauds.

The justifications given to the crime by the fraudster is called the rationalization. Part of the group called Outsiders may rationalized that the government and the banks have failed in assisting the masses to provide their basic needs, so stealing from the banks would not be bad. While insiders may rationalized that the bank poorly remunerate it's staff, so stealing from the bank is justified. Relating fraud triangle theory to this study, this work employed fraud success rate (FSR) as the variable used in measuring the opportunities given to the fraudsters who are being induced to attempt committing frauds by pressure and their rationale, to actually commit the frauds and cause financial loss to the victim. This is because it is not all the fraudsters that gamed the digital banking system that would be successful.

2.3 Empirical Review

The empirical review of related studies conducted in Nigeria on banks and war against financial crime in Nigeria is given below.

Adesuyi et al. (2013) Survey into ATM fraud and its security implementation in the banking environment, employing questionnaire method of data collection. Chi-Square test and one-way ANOVA were utilized in data analysis. No significant difference was found in the perception of the respondents (entrepreneurs, civil servants and students) on the positive impact of ATM on banking and on security challenges of ATM services. Current security implementation was concluded not to proffer the adequate security necessary to secure electronic transactions, customer's information and funds.

Enofe et al. (2017) carried out an empirical review on banks fraud and preventive measures in Nigeria. The study used survey method of data collection and ordinary least square regression model for data analysis. Findings show that strong internal control system, good corporate governance and compliance with banking ethics have positive and significant influence on fraud prevention in banking industry.

Chika et al (2022) examined the impact of cyber-security on fraud prevention in Nigerian commercial banks, using primary data through interview. Result showed cloud security and application security to have statistically increased fraud prevention in Nigeria.

Eme et al (2016) studied the effectiveness of the mechanisms of fraud prevention and detection in Nigeria by using questionnaire as the method of data collection, and student's t-test as analytical tool. The study found significant difference between the perceived effectiveness and actual usage of fraud prevention and detection mechanisms in Nigeria. Also the work revealed that the most effective mechanism like forensic accounting techniques remained the least used in fraud prevention and detection. These implied that the current tools for fraud's prevention and detection in the banks are not proactive in dealing with the fraud menace.

Adekola, (2017) studied impact of regulatory authorities in fraud control in Nigerian banks, using questionnaire method of data collection. The study disclosed that NDIC significantly and positively impacted fraud control in Nigerian banks while CBN prudential guidelines negatively impacted fraud control in Nigerian banks.

Ogwiji and Lasisi (2022) conducted a study on internal control system and fraud prevention of quoted financial services firms in Nigeria using questionnaire as the method of data

collection and SMART-PLS-3-SEM for analysis of data. The study found out that internal control system has a significant influence on fraud prevention

There exists paucity of empirical studies on the success rate of banks' security measures in the fight against financial frauds in Nigeria's digital payment system. The few earlier studies conducted on the subject during cashless era in Nigeria (Adesuyi et al. 2013;Eme et al., 2016;Adekola, 2017; Enofe et al., 2017; Chika et al., 2022; Ogwiji and Lasisi, 2022) used survey instrument of data collection, and their results disclosed mixed findings of positive and significant influence of the security measures on fraud prevention and control (Adekola, 2017; Enofe et al., 2017; Chika et al., 2022; Ogwiji and Lasisi, 2022) as well as the existence of inadequate security necessary to secure electronic transactions, customer's information and funds with the existing security implementation in the banks (Adesuyi et al., 2013; Eme et al., 2016). Consequently, uncertainty was created when concluding whether the security measures of banks are effective in fighting frauds in Nigeria. Hence the need to use a more objective method of data collection that can reduce bias response when assessing the effectiveness of the security measures in fighting frauds in Nigerian banks. Therefore, this study made a difference in the methodology by using documentary method (secondary sources) of data collection to obtain data already in existence even before the research started, to determine the effectiveness of fraud prevention and control tool performance infighting against financial crime in Nigerian's digital payment system.

3. MATERIAL AND METHOD

The study collated data secondarily. Ex-post facto research design was employed. Bi-monthly data of the entire Deposit Money Banks operating in Nigeria as at 2012-2021 computed from the extracts from NDIC annual reports (2013, 2017, 2019 and 2021) and CBN Statistics Database (2012-2020) were used. Specifically, the study utilized bi-monthly value of: total automated teller machine transactions (TATM) amidst banks' security measures, total point of sale (TPOS) terminals transactions amidst banks' security measures, total internet transactions (TWEB) amidst banks' security measures and total mobile phone banking transaction (TMPS) amidst banks' security measures (core digital payment transactions in Nigeria's cashless banking era), which were sourced from CBN Statistics Database (2012-2020), as proxies for independent variable, digital banking transactions amidst banks' security measures in Nigeria (DBTBSM). While bi-monthly value of total fraud success rate (FSR) in Nigeria's deposit money banks used as a measure of the dependent variable, financial crime

JOURNAL OF GLOBAL ACCOUNTING
10 (1) April, 2024.
ISSN (Online): 1597–7641; ISSN (Print): 1597-8273
https://journals.unizik.edu.ng/joga

prevention tools' performance in Nigerian banks, was sourced from NDIC annual reports (2013, 2017 and 2019). Auto regression Distributed Lag (ARDL) model estimation was utilized for data analysis/test of hypotheses with the aid of e-view 10.0. The choice of the analytical tool above was as a result of a co-integration test conducted to establish the existence of a long-run or short run relationship between the two categories of variables in the model, using Auto regression Distributed Lag (ARDL) bound testing techniques, which established the presence of a short-run relationship, necessitating the short-run model, ARDL as specified in equation 1 below, used for estimation of the study's hypothesis.

$$\Delta FSR_t = a_{oi} + \sum^{p}_{i=1} a_{1i}\Delta FSR\ t\text{-}i + \sum^{p}_{i=1} a_{2i}\Delta ATM_{t-i} + \sum^{p}_{i=1} a_{3i}\Delta POS_{t-i} + \sum^{p}_{i=1} a_{4i}\Delta MPS_{t-i} + \sum^{p}_{i=1} a_{5i}\Delta WEB_{t-i} + e_{it} \quad \text{eqn 1.}$$

Where:

e_{it} = the error terms, Δ signifies change, a_{oi} = constant terms and a_{1i} - a_{5i} = coefficients.

The models' estimations were also preceded by the Augmented Dickey-Fuller unit root test conducted to ensure non-spurious results since the study's models involved time series variables.

4. RESULT AND DISCUSSIONS

4.1 Data Analysis

A general description of the research variables is given by the descriptive statistical analysis. Table 4.1.1 below shows the statistics result of each variable:

Table 1: Descriptive Statistics

	FSR	TATM	TPOS	TMPS	TIB
Mean	20.11493	5833.113	2894.110	7578.348	6.250368
Median	23.02083	4981.278	1084.400	929.4500	5.052009
Maximum	38.92000	18199.70	24455.45	53208.27	13.20861
Std. Dev.	8.972082	3519.432	4846.998	14233.81	3.000609
Skewness	-0.577808	1.770807	2.813651	1.957805	1.452549
Kurtosis	2.502874	5.754204	10.52731	5.398009	3.655054
Jarque-Bera	14.30919	181.9967	798.6227	190.6205	80.18779
Observations	217	217	217	217	217

Source: Authors' Computation (2024) via E-view 10.0

Table 1 above revealed the measures of central tendencies and measures of dispersion of the variables. It displays the maximum, skewness, kurtosis, standard deviation, and mean.

JOURNAL OF GLOBAL ACCOUNTING
10 (1) April, 2024.
ISSN (Online): 1597–7641; ISSN (Print): 1597-8273
https://journals.unizik.edu.ng/joga

According to the table 1, the digital payment transactions (ATM, POS, Mobile phone and web) midst banks' security measures (DPTBSM) generally demonstrate changes in the success rate of performance of banks' security measures. The departure from this change indicated a significant dispersion from the DPTBSM's average mean. A positive value for kurtosis was shown by all variables. These disclosed a heavier tail called leptokurtic distribution as the degree of tailedness of all variables.

4.1.2 Correlation Matrix

Table 2: Pearson's correlation matrix among the variables

	FSR	TATM	TPOS	TMPS	TIB
FSR	1.000000				
TATM	-0.603810	1.000000			
TPOS	-0.476585	0.308796	1.000000		
TMPS	-0.650775	0.580338	0.927787	1.000000	
TIB	-0.697704	0.751137	0.853980	0.963585	1.000000

Source: Authors' Computation (2024) via E-view 10.0

Table 2 shows all the variables' degrees and directions of linear association. It can be inferred that positive and negative correlations exist among all the variables. The result showed that our variables are not highly correlated among themselves.

4.1.3 Unit Root Test

Table 3: Augmented Dickey-Fuller Unit Root Test

S/N	**Variables**	**ADF Stat**	**Critical Values**			**Integration Order**
			1%	**5%**	**10%**	
1	FSR	-2.582155 PV (0.0098)	-2.576***	-1.9423***	-1.6157***	1(0)
2	TATM	-4.001311 PV (0.0269)	-3.665***	-3.4309***	-3.1391***	1(0)
3	TPOS	-3.802318 PV (0.0049)	-2.847***	-1.9882***	1.6001***	1(1)
4	TMPS	-6.292057 PV(0.0492)	-4.483***	-4.4504***	-3.7015***	1(1)
5	TIB	-3.758723 PV(0.000)	-2.031***	-1.9423***	-1.6157***	1(0)

Source: Authors' Computation (2024) via E-view 10.0

JOURNAL OF GLOBAL ACCOUNTING
10 (1) April, 2024.
ISSN (Online): 1597–7641; ISSN (Print): 1597-8273
https://journals.unizik.edu.ng/joga

The stationary characteristics of the series are displayed in table 3, following the application of the augmented Dickey-Fuller (ADF) framework. The results, as displayed in table 3, show a combination of I(0) and I(1) variables which necessitated a co-integration test to be done.

4.1.4 Co-integration Test

Since the variables are in levels and first difference, performing a co-integration test is necessary to establish whether a long-run relationship exists. The Bound test proposed by Shine and Smith (2001) was appropriate to achieve this.

The hypothesis is stated as follows:

H_o: no co-integrating equation

H_1: H_o is not true

4.1.4.1 Decision Criteria for the Bound Test

If the calculated F-statistic is greater than the critical value for the upper bound 1(1), the H_o above is rejected at 10%, 5%, or 1% significance level. This implied the existence of a long-run relationship that would require a long-run model (Error Correction Model) to be estimated. But if the calculated F-statistic is lower than the critical values for the lower bounds 1(0), the H_o above is accepted at 10%, 5%, or 1% significance level. Therefore, there is no long-run relationship that existed among the variables in the equation. Hence, the short-run Auto regression Distributed Lag (ARDL) model should be estimated.

The result of the bound test conducted is shown in Table 4.

Table 4: Summary of Bound Test Result

Dependent Variable	**F-Statistics**	**Significant Level**	**Lower Bound Limit 1(0)**	**Upper Bound limit 1(1)**	**Co-integration**	**Decision**
FSR	**F_{FSR} =** 1.380372	10%	2.2	3.09	No	Estimate the ARDL (Short-run model)
		5%	2.56	3.49		
		2.5%	2.88	3.87		
		1%	3.29	4.37		

Source: Authors' Computation (2024) via E-view 10.0

JOURNAL OF GLOBAL ACCOUNTING
10 (1) April, 2024.
ISSN (Online): 1597–7641; ISSN (Print): 1597-8273
https://journals.unizik.edu.ng/joga

Table 4 disclosed the presence of a short-run relationship as the f-statistics is lower than the critical values at the lower bound limit 1(0). Therefore, the short-run model (ARDL) was employed.

For more accurate Autoregression Distributed Lag (ARDL) model estimation to be performed, there is need to obtain an appropriate lag length to be used. Table 5 shows the appropriate lag length for the hypothesis:

Table 5: Appropriate Lag Length for the hypothesis

Hypothesis	**Appropriate Lag**
Hypothesis One	2

Source: Authors' Computation (2024) via E-view 10.0

<

4.2 Test of Hypothesis

H_O: The core digital payment transactions (ATM, POS, Mobile phone and Internet banking) amidst banks' security measures has no significant effect on the fraud success rate in Nigeria's DMBs.

Table 6: Auto regression Distributed Lag (ARDL) model estimation

Dependent Variable: FSR

Variable	Coefficient	Std. Error	t-Statistic	Prob.*
FSR(-1)	1.943947	0.024163	80.45116	0.0000
FSR(-2)	-0.945537	0.024190	-39.08795	0.0000
TATM	-0.002723	0.000633	-4.299953	0.0000
TATM(-1)	0.005324	0.001272	4.183661	0.0000
TATM(-2)	-0.002620	0.000660	-3.971304	0.0001
TPOS	0.008717	0.000598	14.58057	0.0000
TPOS(-1)	-0.016839	0.001214	-13.87247	0.0000
TPOS(-2)	0.008105	0.000683	11.86280	0.0000
TMPS	-0.009567	0.000286	-33.46266	0.0000
TMPS(-1)	0.018445	0.000594	31.06597	0.0000
TMPS(-2)	-0.008878	0.000376	-23.59674	0.0000
TIB	47.60978	1.851222	25.71802	0.0000
TIB(-1)	-92.23547	3.819568	-24.14814	0.0000
TIB(-2)	44.66893	2.142344	20.85049	0.0000
C	-0.112202	0.181086	-0.619610	0.5362
R-squared	0.999952	Mean dependent var		20.06894

Adjusted R-squared	0.999948	S.D. dependent var	9.001113
S.E. of regression	0.064815	Akaike info criterion	-2.567343
Sum squared resid	0.840198	Schwarz criterion	-2.332183
Log likelihood	290.9894	Hannan-Quinn criter.	-2.472328
F-statistic	294784.9	Durbin-Watson stat	1.982676
Prob(F-statistic)	0.000000		

Source: Authors' Computation (2024) via E-view 10.0

The ARDL result as shown in Table 6 above disclosed that the exogenous variables are jointly responsible for a 99% variation in the endogenous variable with the R^2 of 99%, leaving an unexplained variation at 1%. This represents the goodness of fit of the regression. The TATM and TMPS individually showed negative significant effect on the FSR in Nigerian banks. While TPOS and TIB individually showed positive significant effect on the FSR in Nigerian banks.

Overall, the F-statistics (294784.9) with its p-value of 0.000000 revealed that the regression result is significant. Durbin Watson Statistics of 1.98 which is approximately 2, rules out all possible suspicion of first-order positive autocorrelation. The figures revealed point that this result is reliable for a meaningful analysis. Therefore, the null hypothesis is rejected and we concluded that there is a significant effect (negative and positive effect) of individual digital payment transactions (ATM, TMPS – negative; POS, Internet banking - positive) midst banks' security measures on fraud success rate in Nigeria's deposit money banks (DMBs). The findings from this work were discussed in relation to the study's specific objective.

Considering the objective on the effect of the core digital payment transactions (ATM, POS, Mobile phone and web) midst banks' security measures (DPTBSM), on Fraud success rate (FSR) in Nigeria's banks; the study revealed that The TATM and TMPS individually showed negative significant effect on FSR in Nigerian banks. While TPOS and TIB individually showed positive significant effect on the FSR in Nigerian banks. This implied that the opportunity to actually commit fraud was drastically curtailed with the security measures employed by Nigerian banks in respect of the ATM transactions and transactions through mobile payment system (TMPS). While many fraudsters are allowed to game the POS transactions and internet banking even with the existing fraud prevention tools in Nigeria's banks. The partial effectiveness of the banks' security measures in dealing with frauds menace in banks could be attributed to pressure from financial burden, management's desire for more investments and customers, lack of good welfare package for staff and government's failure in assisting the masses to provide their basic needs.

This result is in disagreement with the findings of Adesuyi et al. (2013) that disclosed the current security implementation not to proffer the adequate security necessary to secure electronic (ATM) transactions, customer's information and funds.

CONCLUSION AND RECOMMENDATIONS

In view of the empirical discoveries of this study, it is concluded that the security measures introduced by banks in fighting financial crimes in Nigerian banking sector has been partially effective as digital payment transactions through ATM and mobile phones have depressed the opportunity to commit fraud, while reverse is the case with POS transactions and internet banking. Consequently, this study recommended the following:

1. Provision of a good Fraud linking infrastructure by banks: Fraud prevention software that can aid the bank view relationships between transactions through identifiers like passwords, usernames, and others should be installed in all electronic payment channels with more focus on POS terminals and internet. This will help to disclose with relative certainty that a transaction may be fraudulent since the individual carrying out the transaction has previously carried out a confirmed fraudulent transaction, thereby facilitating fraud prevention.
2. Creation/ maintenance of good staff welfare package by Nigerian banks: Most of the working environments of banks staff could be referred to as deceptive favourable working environment where outsiders perceived that banks' staff have good welfare package due to their appearance in the banking hall without knowing that the staff are suffering and smiling. Many staff are under paid resulting from lack of upgrade of staff with additional qualification on the job, while majority of the banks do not grant their staff, sick leave unless the person is nearly dead. Correction of these ugly situations will aid reduction of insiders' fraud.
3. Employment generation by banks and government: This does not mean that government and banks should employ every job seeker, but should ensure effective implementation of their policies that supported entrepreneurial development. This will aid outsiders to meet their basic needs that could pressure them to commit fraud.
4. Additional customer awareness creation: Banks should update their customers on new strategies employed by fraudsters as they received reports on cases of frauds in the banks; and frequently reminding them not to disclose their personal bank's information to anyone. This will aid to keep them ahead of fraud schemes and prevent them from falling victims.

REFERENCES

Adelabu, A. A. (2016). A Changing Payments Eco System: The Security Challenge. Nigeria Electronic Fraud Forum Annual Report, CBN, Nigeria. Retrieved from www.cbn.gov.ng

Adesuyi, F., Adepoju, S. & David, R. (2013). A Survey of ATM Security Implementation within the Nigerian Banking Environment. *Journal of Internet Banking and Commerce,* 18(1), 01-16.

Adepetun, A. (2020**).** Nigerian Banks Spent N200b Preventing Cyber Attacks in 2019. Retrieved from https://guardian.ng/business-services/nigerian-banks-spent-n200b-preventing-cyber-attacks-in-2019/

Ajala, O. A., Amuda, T., & Arulogun, L. (2013). Evaluating Internal Control System as a Preventive Measure of Fraud in the Nigerian Banking Sector. *International Journal of Management Sciences and Business Research*, 2(9), 15 – 22.

Akinleye, G. T. & Adekola, D. R. (2017). Impact of Regulatory Authorities on fraud control in Nigerian banks. *Imperial Journal of Interdisciplinary Research*, 3(2), 1880-1885.

Awelewa, G. (2016). A changing payments landscape: the security challenge. The Nigeria Electronic Fraud Forum Annual Report. Retrieved from https://www.cbn.gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NeFF%202016%20Annual%20Report.pdf.

CBN (2019). CBN Rule Book: A Compendium of Policies and Regulations, 1. Retrieved from https://www.cbn.gov.ng/out/2020/fmd/cbn%20rule%20book%20volume%201.pdf

CBN (2021). Understanding Monetary Policy Series No. 6: The Nigerian Payments System. Retrieved from www.cbn.gov.ng

Chika, O. V., Eke, P., & Chukwumati, N. M. (2022). Impact of cyber-security on fraud prevention in Nigerian commercial banks. *JurnalAkuntansi, Keuangan, Dan manajemen*, 4(1), 15-27. DOI:10.35912/jakman.v4i/.1527

Eme, E. J., Inyang, I. O., & Udeme, J. (2016). Effectiveness of the mechanisms of fraud prevention and detection in Nigeria. *Advances in Social Sciences Research Journal*, 3(3), 206-217. DOI: 10.14738/assrj.331894.

Enofe, A. O., Abilogun, T. O., Omoolorun, A.J. & Elaiho, E. M. (2017). Banks Fraud and Preventive measures in Nigeria: An Empirical Review, *International Journal of Academic Research in Business and Social Sciences,* 7(7), 40-51. DOI: 10.6007/IJARBSS/v7-i7/3076

Hunkin, J. S. (2002). Ethics in business and everyday life. Canada: Gale Group.

.Mawutor, J. K. M., Enofe, A., Embele, K., Ndu, A. R. & Awodola, O. E. (2019). Fraud and Performance of Deposit Money Banks, *Accounting and Finance Research*, 8(2), 202-213.

NDIC (2013). Annual Report. Retrieved from www.ndic.gov.ng/wp/content/uploads/2013/07/link/parttwo/pdf

NDIC (2017). Annual Report. Retrieved from www.ndic.gov.ng/wp/content/uploads/2017/07/link/parttwo/pdf

NDIC (2018). Annual Report and Statement of Account. Retrieved from https://ndic.gov.ng/wpcontent/uploads/2019/09/NDIC-2018-ANNUAL-REPORT.pdf.

NDIC (2021). Annual Report. Retrieved from www.ndic.gov.ng/wp/content/uploads/2021/07/link/parttwo/pdf.

NDIC Act (2006). Federal Republic of Nigeria Official Gazette, 93(73), A427-454. Available at: ndicact.pdf

Nlebem, A. (2021). Access Bank's Security Measures Safeguard Customers from Fraud, Retrieved from https://businessday.ng/news/article/access-banks-security-measures-safeguard-customers-from-fraud/

Ogwiji, J. & Lasisi, I. O. (2022). Internal control system and fraud prevention of quoted financial services firms in Nigeria: A S mart PLS-SEM Approach, *European Journal of accounting, auditing and finance research*, 10(4). 1-13

Okoye, A. P. (2018). Effect of cashless banking on the unemployment rate in Nigeria, *Asian Journal of Economics, Business and Accounting*, 6(4). 1-18.

Ovuakporie, V. (1994). Bank Frauds: Causes and Preventions: An Empirical Analysis. Ibadan, Nigeria, ATT Books. Retrieved from search.worldcat.org

Ozoji, A. P., Iwara, O. E., Ezuwore-Obodoekwe, C. N., Inyada, S. J., Ezechukwu, B. O., Ayem-Fellarn, T. F., Ezuma, C. O., Ebisi, L. N. & Okoroiwu, L. K. (2021). Insecurity of cashless banking transactions: Evidence from Nigerian Banks, *Academy of Accounting and Financial Studies Journal*, 25(5). 1-23.