Article

JOURNAL OF MANAGEMENT SCIENCES
2025, Vol. 10(1), 178-191

ELECTRONIC BANKING AND BANK FRAUDS IN NIGERIA – IMPACT ANALYSIS

Sunday U. OKANTA[1], Kingsley C. MICHAEL[1], Catherine A. NNELI[2], and Ndubuisi N. UDEMEZUE[2]

[1]Department of Banking and Finance, Abia State University, Uturu, Nigeria
[2]Department of Banking and Finance, Alex Ekwueme Federal University, Ndufu-Alike, Ebonyi State, Nigeria

Abstract

This study aimed to examine the direction and degree of the impact of electronic banking on fraud in Nigerian banks. The technique of auto autoregressive distributed model was used on the variables of interest between 2010 and 2021. The results showed that electronic banking was not an important factor in explaining bank fraud in Nigeria's banking industry. The Automated Teller Machine (ATM), Point-of-Sale (POS), and mobile banking (MTR) transactions did not influence fraud in Nigerian banks. However, Web (internet) transactions were a negative influencer of fraud in Nigerian banks. This suggested that internet transactions accounted for some fraud occurrences. The researchers recommended that banks and the relevant regulators should reduce losses from fraud by using proactive and rapid response measures and policies, especially in the space of internet transactions. Efforts should be increased in skill training and development in advanced cybersecurity measures. Additionally, the gains already made in the areas of ATM, POS and MTR transactions should be sustained.

Keywords: Electronic Banking, Frauds, Banks, Nigeria, ARDL**.**

Introduction

Using electronic devices to conduct business is known as electronic banking. This is commonly referred to as "e-banking" in the banking sector. Today's markets and banking sector are shaped by electronic banking; it has changed banking operations, brought in new rivals and services, and extended the roles of financial institutions in the process. It has caused the payments system and bank deposits to undergo numerous important transformations. This is led by dynamic technological advancements in banking. This evolving scenario in e-banking defines the 21st-century banking industry's operating environment, which is competitive and complex. It is impossible to overstate the advantages that electronic banking has given to the banking sector. These benefits include timeliness and efficiency as well as growth and development in banking and other economic sector transactions. It is now a matter of great concern and importance for all banks to apply e-banking concepts, techniques, policies, and implementation strategies to banking services; in fact, it is a requirement for how banks plan and what products and services they offer in the banking business. It has persisted in altering the global structure of banks and their business ties and performances. No country is immune to fraud, although developing nations and their many states are more affected than others. Fraud is becoming more widespread.

In Nigeria, good intentions and selfless efforts have been betrayed by corrupt and fraudulent incidents that have been witnessed daily throughout the country (Okoye, 2016). Abaenewe, Ogbulu and Ndugbu (2013) claim that the introduction of electronic gadgets to help provide bank customers with high-quality and quick services marked the beginning of the revolution in Nigeria's banking sector. Customers no longer have to wait as long for banking transactions, thanks to the industry's increasing competition brought about by the advent of these electronic devices. The utilization of computers and other networking devices is what brings about this innovation. However, the banking industry is facing significant challenges as a result of the widespread use of electronic banking in bank services. One difficulty is risk exposure, which includes fraud and all of its associated activities. To mitigate this threat, banks have persisted in establishing their internal control frameworks and systems, as well as hiring reputable internal and external auditors. The expectation is that these measures will significantly curtail fraudulent activities within the banking sector. Nevertheless, in spite of these genuine tools, banks have been losing enormous sums of money as a result of employee and customer fraud. This notwithstanding, the usage of computers in the Nigerian banking sector still provides many benefits, despite the number of crimes that are perpetrated using them, such as increased efficiency and reduced transaction costs. Furthermore, banks and the government, via its different agencies, have persisted in implementing policies meant to prevent fraud in the financial sector. According to the NDIC (2016) report, there were over 943 fraud instances registered in the year 2016, with an actual loss of ₦903.60 million. A 2009 investigation by the CBN revealed that more than 13 out of the 24 banks in existence were experiencing liquidity issues as a result of insider abuse and fraudulent operations, particularly on the part of bank management. Additionally, approximately ₦1 billion was lost to online fraudsters. Our worry is that with the numerous proactive measures to checkmate electronic banking related fraud, the industry is still plagued with enormous frauds. We want to dissect the components of electronic banking to find the specific indicators and proffer suggestions. In our work, quarterly data were used in place of the typical annual statistics seen in the majority of the evaluated literature. Thorough pre and post diagnostics analysis were conducted to ensure credible results This is a departure from the literature the researcher reviewed.

Scholars like Kanu and Okoroafor (2013), Aruomoaghe and Ikyume (2013), Owolabi (2010), Uche and Agbo (2013), Ikpefan (2006), and Odi (2013) have all conducted studies on the effects of fraud on Nigerian banks. Some approached it from the perspective of the real amounts involved in credit mobilization while the majority did so from the standpoint of the number and types of staff involved. The main goal of this study was to assess how electronic banking instruments affected the prevalence of banking fraud in Nigeria's banking industry. The study specifically determines the electronic banking channels that have reduced or increased financial fraud in Nigeria over time. Hence, It attempts to address the following queries: the effect of ATM, POS, MTR and web (WTR) transactions on bank frauds in Nigeria. This investigation was conducted between 2010 and 2021. This time frame was selected because it aligned with the introduction and integration of e-banking into the Nigerian banking sector. The study is expected to broaden the body of information that policymakers can draw upon to combat fraud in the Nigerian banking industry. This can provide important insights into the extent of the effects and variations across the various e-banking channels, as well as the degree to which each one is susceptible to fraud based on volume and naira values. These comparative effects will help policymakers and banks make more informed plans. The study is divided into the following sections: the introduction is in Section 1, a review of related works follows in Section 2, the methodology in 3, the analysis of data is in Section 4, and then the conclusions.

REVIEW OF RELATED WORKS

CONCEPTUAL VIEWS: Online Banking

The definition of electronic banking varies widely. According to Steven (2002), it is the process of providing bank clients with a variety of value-added goods and services via electronic and communication networks, regardless of their location, schedule, or time zone. Deposit taking, lending, account administration, financial advising, electronic bill payment, and electronic money are a few examples of these goods and services. Electronic banking is described by the Basel Committee on Banking Supervision as the delivery of big-value electronic payments, other electronic wholesale banking services, and retail and small-value banking products and services through electronic channels. When conducting banking operations, such as money transfers, bill payments, checking and savings account balance checks, mortgage payments, and the purchase of financial instruments and certificates of deposit, e-banking makes use of the internet as the delivery channel (Mohammed, Siba & Sreekmar, 2009). According to Abubakar (2014), there are four types of electronic banking: telephone-based banking, Internet-based banking, TV-based banking, and personal computer banking. The majority of financial transactions may be conveniently completed at the customer's convenience using electronic banking. The client has round-the-clock access to their money, including the ability to move it between accounts, pay bills, and make purchases (Siam, 2006).

Channels of Online Banking:

Automated Teller Machine (ATM): Automated Teller Machines (ATMs) are now a key gauge of banks' ICT spending. Banks around the world have embraced and continue to adopt Automated Teller Machines (ATMs). They provide banks and their depositors with significant advantages. According to Olatokun and Igbinedion (2009), the machines have the ability to allow depositors to withdraw cash at more convenient times and locations than during regular banking hours. These advantages are increased when banks share their ATMs, granting depositors from other banks access to their accounts via a bank's ATM. Since ATMs can handle more transactions per unit of time than tellers can, banks are now the primary ATM deployers. This is because a single transaction made at an ATM may be less expensive than a transaction made with a teller. According to Jegede (2014), there are a number of other names that can be used interchangeably with Automated Teller Machines, such as Automatic Banking Machine (or Automated Banking Machine in the United States), Automated Transaction Machine (especially in the United Kingdom), Cash line Machine (named after the Royal Bank of Scotland), and All Time Money in India.

Point of Sale (POS): This is the next-generation remote service device that can electronically add a third party to the communication channel between a financial institution and its customers. POS manages credit authorization, cash deposit and withdrawal, cash payment, and check verification. This improves electronic fund transfer at the point of sale, making it possible to deduct the cost of a purchase from an outlet like a grocery store or gas station right away, debiting the customer's account.

Mobile Banking (MB): Mobile banking technology is one of the electronic distribution methods used by banks. Researchers are interested in mobile banking because it is growing in popularity in today's banking environment. According to Adewoye (2013), mobile banking refers to financial transactions that are carried out by utilizing a mobile device to access a bank's website and monitor account balances, make transfers between accounts, or pay bills. The way banks operate has altered as a result of mobile banking. New banking services that attempt to reduce transaction costs and reach more bank clients have been introduced as a result of this. All banks operating in Nigeria now consider the deployment of electronic banking services to be of utmost relevance and concern. It is also a must for maintaining local and international competitiveness (Akingbola, 2006). E-banking has helped banks perform better in terms of growing their market share, offering a wider range of goods, offering customizable options, and responding more quickly to customer

requests. E-banking has the potential to impact banks' revenue streams and operations. The usage of electronic banking is now regarded as the most crucial component of the environment for electronic commerce. Some banks are currently adopting the global system for mobile communication (G.S.M.) as a means of doing some of their business since its introduction. Additionally, the owner can purchase any bank e-product or service by using this to access additional transaction links (Okey, 2005).

Fraud

According to Adewumi (1986), fraud is the deliberate, premeditated activity of an individual or group of individuals with the goal of distorting the truth or a reality in order to benefit financially from it. It requires the use of trickery and deceit, as well as occasionally very clever cleverness and expertise. Typically, the activity takes the form of outright theft, forgery, document falsification, and authorized signatures. According to Idowu (2009), fraud comprises embezzlement, theft, or any attempt to steal or unlawfully obtain, misuse, or harm a bank's asset. It also includes the intentional misrepresentation, concealment, or omission of the truth for the purpose of deception or manipulation to the financial detriment of an individual or an organization (such as a bank). A corporation or economy that commits fraud suffers consequences, most frequently in the form of monetary losses. According to Ojeaga, Ikpefan, and Odejimi (2014), fraud is pervasive in both developed and developing nations, and it differs depending on the location in terms of its scope, origins, and manifestations as well as how it affects development and administrative performance. Fraud typically entails: falsifying or changing documents, such as accounting records; theft or misappropriation of property; removing or hiding a transaction's impact from records or documentation; recording of transactions free of drugs; 5. deliberate misuse of accounting regulations and deliberate fabrication of the entity's transactional state of affairs. Depending on how it is seen, fraud is just an act of dishonesty and deception that includes stealing goods from its rightful owner without that person's knowledge, approval, or consent, or purposefully or carelessly misrepresenting facts.

Electronic fraud: The term "e-fraud" refers to a broad range of illegal activities that involve the use of information technology infrastructure. These activities include illegal or unauthorized access, illegal interception of computer data transmitted to and from a computer system through technical means, data interference resulting in unauthorized destruction, deterioration, alteration, or suppression of computer data, and systems interference causing interference with the input, transmission, misuse of devices, and forgery (ID theft) of data (Paul, 1999). There are several crimes that use electronic fraud as a goal, including: hacking into computer networks or systems, compromise of programs and operating systems, theft of information or data and theft of intellectual property, including software for computers. Others are theft of promotional data, blackmail based on data obtained from digital files, including financial, medical, and personal histories.

Causes of Bank Fraud: Poor management is one of the main institutional causes of fraud, according to Nwaze (2006). This appears in the shape of insufficient oversight. Once more, an immoral external environment surrounding the bank encourages dishonest behavior both within and outside of the bank (Idowu, 2009). As Bello (2005) clarified, "when a country's legislation does not allow for private prosecution of incidents of fraud and in situations where fraud is not looked into by the authorities, it is utterly impossible to bring such a matter before a court of law.

Furthermore, poor research always results in poor prosecution, ultimately leading to the offender's discharge and acquittal on moral grounds. Because of this, con artists in Nigerian society are aware that they can always have their way with the police. Donli (2006) noted that the absence of safeguards for bank regulators and the meddling of the government have raised the amount of fraud in Nigeria's leading corporations, particularly the banking sector. The current structure of the Nigerian judicial system makes it difficult to dissuade frauds

committed in the banking industry. The system's administration is the problem. Currently, the courts are crowded, which means it can take months or even years for a case involving bank fraud to be eliminated. Prompt punishment or no prosecution usually doesn't dissuade potential offenders. There is typically a possibility of evading justice because of our legal system's "protection" and protocols. This has kept encouraging dishonest behavior.

Nigerian E-Banking: Development

From the days of ledger cards and other manual filling systems to the computer age, banking has come a long way. Society General Bank (Nigeria) Limited was the first bank in Nigeria to introduce computers to the country's banking sector in the 1970s. Few computerized banks used the Local Area Network (LAN) in their branches until the middle of the 1990s. The more advanced banks then connected their branches inside cities to create the Wide Area Network (WAN), while a few used leased lines to create intercity connectivity (Salawu and Salawu, 2007). Later, the situation changed. In addition to adopting computerization, banks also advanced from processing checks and making deposits to performing very basic retail operations like cash withdrawals and withdrawals. This was due to intense competition brought on by an unprecedented rise in the number of banks and branches as well as advancements in information technology. In response to growing market pressure and customer demands for more convenient and better service, banking operations needed to be innovative and modernized. As a result, using the internet and electronic banking has become essential. Sanusi (2002), referenced by Dogarawa (2005), states that the CBN approved All States Trust Bank's deployment of a closed system electronic purse known as ESCA in 1996, marking the beginning of the introduction of e-banking (e-payment) goods in Nigeria. This was followed in February 1997 by Diamond Bank's launch of a comparable product dubbed "Paycard." With Smartcard Nigeria PLC's approval in February 1998—a corporation founded by a group of 19 banks to create and oversee value cards issued by the member banks—the card-based e-money products gained access to an open platform. In November 1999, the CBN approved the introduction of the "Smartpay" Scheme, which was organized by Gemcard Nigeria Limited and involved over 20 banks (Dogarawa, 2005). Since then, the number of banks taking part in each of the two initiatives has increased. Additionally, while on a restricted basis, the CBN approved several banks to offer online banking via the internet, telephone banking, and international money transfer products (Dogarawa 2005). It is also necessary to discuss how certain banks developed automated teller machines (ATMs) to improve their service delivery and make it easier for customers to use cards. Almost every bank in Nigeria has a website these days. Additionally, automated is the ordering process for certified checks payable to third parties or bank drafts.

THEORITICAL REVIEW

Our work is hinges on Sutherland’s (1949) "white-collar crime." Hypothesis. He defines white-collar crime as a crime carried out by a reputable individual who holds a high position at their place of employment. White-collar criminals are shrewd, cunning, well-educated, and opportunistic people who think they can take advantage of situations to get money. Furthermore, there are people who meet the requirements to work in positions that allow them to have unrestricted access to enormous sums of money. Thus, in order to prevent future instances of this kind of fraud, the services of a qualified and experienced investigator, such as a forensic aforementioned accountant, are necessary due to the position and/or talents of those who committed the atrocities (Alao, 2016).

EMPIRICAL REVIEW

Ololade, Salawu & Adekanmi (2020) investigated the causes and mechanisms of electronic banking fraud in Nigerian banks using a survey research approach, and the findings indicated that economic difficulties and disruptive technologies were the cause of job losses. This resulted in employees disengaging from their jobs without being compensated,

which may have given rise to employee fear of committing electronic banking fraud. Olaleye and Fashina (2019) looked at the consequences and controls of electronic banking fraud in Nigeria. The study used secondary sources of data using a case study research style. The study found a strong correlation between Nigerian e-banking practices and the rate at which transaction security is increasing, which has helped banks successfully provide high-quality services.

The frequency of electronic banking fraud in the Nigerian banking sector was examined by Amaefule and Onu (2019) employing survey research, primary questionnaires, and secondary data sources. The study's recommendations called for focusing on the most effective ways to reduce the issue of electronic banking fraud by reevaluating and fortifying current security measures that guarantee end users' safety. Ibanichuka and Oko (2019) looked into the financial performance of Nigerian commercial banks that were quoted as well as electronic fraud. Secondary data and an ex post facto research design were used in the study, which ran from 2013 to 2017. In a panel data context, simple descriptive analysis, multivariate regression, and Pearson Product Moment Correlation were used to analyze the obtained data. The findings indicated a weak and unfavorable correlation between financial performance metrics and electronic fraud channels. Adeoti (2011) looked into the scope of Nigerian ATM fraud. The study looks into ATM frauds in Nigerian banks using both primary and secondary data. The data was analyzed and the hypothesis was tested using the chi-square statistical approach. The article comes to the conclusion that bank employees and clients must work together to apprehend those who commit ATM fraud in banks.

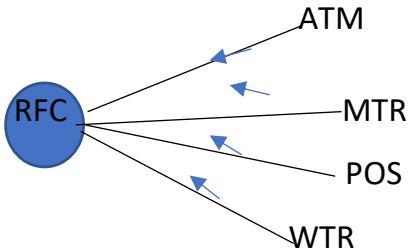
Bhasin (2016) investigated how technology could be used to stop bank fraud. A survey using questionnaires was carried out among 345 bank workers in 2013–14 to find out how they felt about bank frauds and assess the variables affecting their level of compliance. This study offers an open discussion of the mindsets, tactics, and tools that professionals will require to stop bank fraud. Due to the constantly sharpening double-edged sword of technology, fraud protection in the present era is not achievable with a single silver bullet. Globally, the application of real-time behavior models powered by neural networks has revolutionized the field of fraud management. Banks will experience a decrease in fraud losses if they can better prevent fraud by utilizing technology and analytics advancements. Because financial frauds and white-collar crimes are increasing at a rapid pace, forensic accounting has gained attention recently. Ehimen and Bola (2010) looked into cybercrime and the pertinent laws that Nigeria has to fight it. According to the report, using the internet to facilitate criminal activity can involve a variety of activities, including banking fraud, business espionage, and accessing and destroying data from computer networks belonging to important businesses. They discovered that less than 10-4% of Nigeria's 140 million citizens are engaged in cybercrime nationwide. Their investigation thus came to the conclusion that everyone in society must work together to combat cybercrime, not just the police, who currently lack the experts in their investigative units to deal with this type of crime.

Dzomira (2014) examined the types of electronic fraud that are committed in the banking sector as well as the difficulties encountered in reducing the risk. It was based on descriptive research that used content analysis to examine the phenomena of cyberfraud. The chosen informants from 22 banks were given questionnaires and interviews in order to collect the data. Techniques for judgmental sampling and convenience were applied. It was discovered that the majority of the electronic fraud types mentioned are committed by those working in the financial sector. To protect technical systems from cyberattacks, it is advised that the subject of cyber security be addressed with the involvement of all stakeholders. The goal of Duah & Kwabena's (2015) research was to determine the scope of fraudulent cyber activity and how it affected Ghana's electronic business development. An analysis of secondary data was conducted using the generic inductive approach. The findings

showed that cyber fraud is quickly spreading throughout Ghana and that both consumers and companies suffer direct financial losses as a result.

Dzomira (2017) examines the public alerts sent by South African banking institutions to the public about internet banking fraud. The routine activity theory, a criminology theory, served as the focal point of the investigation. In order to provide a thorough understanding of internet banking fraud alertness in the banking industry, a qualitative content analysis was employed as the research technique for the interpretation of the text data from each bank's website through the methodical classification process of coding and identifying themes or patterns. Thirteen of the sixteen South African retail banks with foreign and local management made up the sample size. The results show that banks are not giving the general public enough internet fraud vigilance information on their websites, even if the majority of banks do give such information to log-in users and there is question about how such information is used. According to this study, there is a need to improve internet fraud alertness data and provide internet banking users with adequate knowledge about the many kinds of online banking fraud that are committed by online fraudsters before they log in to complete transactions. Ogbulu, Uruakpa, and Umezinwa (2014) looked into the connection between Nigerian DMB performance and bank fraud. Multiple regression analysis, unit root tests, cointegration, error correction mechanisms, and Granger causality tests were all used in the study's approach. Various NDIC Annual Report issues included secondary data on indications of bank fraud and DMB earnings before taxes (EBT) for the years 1991–2012. The study's main conclusions show a significant negative correlation between bank performance and bank fraud. Moreover, there is a unidirectional Granger causation relationship between Earnings before Tax and Expected Loss on Bank Fraud (ELF) and Value of Bank Fraud (VFC), respectively.

Figure1: Model



RFC is a function of ATM, MTR, POS, and WTR, as shown in Figure 1; that is, RFC=f (ATM, MTR, POS, and WTR). It details the kind and/or extent of e-banking products that have an annual impact on the incidence of frauds in Nigerian depository institutions. The aforementioned models can be rewritten as follows linearly:

Data and Methods

Auto auto-distributed lag model was used in the study to determine the extent of the association between bank fraud and e-banking. In this study, the secondary source was consulted. The secondary sources that are utilized are publications by CBN statistical books. The data time series spans the years 2010 through 2021. The indicators of Automated Teller Machine (ATM), Mobile Banking (MTR), Point of Sale (POS), and Web Transaction (WTR) are independent variables. The value of reported fraud cases (RFC) is a dependent variable. The researchers first define the variables and discuss how they fit into the models before specifying the model.

$$RFC=b_0 + b_1ATM + b_2MTR + b_3POS + b_4WTR + u_t \quad \text{...Equation 1}$$

Where:

RFC = Value of Fraud Cases Reported
ATM =Transactions through ATMs
MTR =Mobile transactions.
POS = Point of sale transactions
WTR stands for web transactions.
μ=unaccounted-for variable

The parameter estimates of ATM, MBT, POS, and WTR, respectively, in the RFC are b_1, b_2, b_3, and b_4. b_0 is an estimate of constant parameters. With a logarithmic transformation, the aforementioned model appears as:

Log (RFC) = b_0 + b_1Log(ATM) + b_2Log(MTR) + b_3Log(POS) + b_4Log(WTR)... Eqn 2

Log is the natural logarithm of the variable sequences and represents a relative change in value.

Multiple regression analysis was performed on the models that were given.

Auto regressive distributed lag model

$$\Delta\Delta\gamma_t == - \sum_{i=1}^{p-1} \gamma_1 * \Delta\gamma_{t-1} + \sum_{t=1}^{k} \sum_{i=0}^{qj-1} \Delta x j, t - i \quad \beta j, \quad i*-\Phi\varepsilon c_{t-1} + \epsilon_t$$

Eq. 3

ARDL approach to cointegration is preferable to other conventional cointegration approaches (Peseran, Shin and Smith, 2001). One of the reasons is that ARDL is applicable irrespective of whether the variables are purely I(0) or I(1) or combination of the two. Another reason is that it is more robust and good for a small sample size. This is because it expands the model and brings out contemporaneous and lagged variables of the model.

A Priori" Economic Expectations

The present study's expected 'a priori' relationship between the dependent and independent variables adheres to the economic theory principle that states that, within the growth paradigm of e-fraud, the parameter estimates of e-banking indicators should be negligible and negative.

ANALYSIS AND RESULTS

Variables Statistics

An overview of the statistics that characterize the distributional features of all the data is provided in Table 4.2 below. The variables' standard deviations were 3.42, 505.08, 171.05, 3.37, and 0.87 for RFC, ATM, POS, WTR, and MTR, in that order. ATM had the highest standard deviation, while MTR had the lowest. All variables, with the exception of RFC, showed platykurtic distributions when the Kurtosis value was less than 3. A leptokurtic distribution is suggested when the RFC is bigger than 3. All of the variables' skewness coefficients indicated a positive skewed distribution. While the p-value of Jarque Bera at RFC is significant at 5%, providing strong evidence of an atypical distribution, the p-values at ATM, POS, WTR, and MTR are insignificant at 5%, indicating a normal distribution. Table 4.2: RFC, ATM, POS, WTR, and MTR Descriptive Statistics

	RFC	ATM	POS	WTR	MTR
Mean	4.307750	614.6644	197.6794	34.40500	201.0179
Median	3.335000	479.6650	139.9750	27.83000	137.7650
Maximum	20.08500	1832.550	481.7400	73.48000	503.3200
Minimum	1.112000	62.59000	1.870000	3.370000	0.870000
Std. Dev.	3.424987	505.0838	171.0538	23.47139	181.4085
Skewness	2.625119	0.701837	0.198158	0.232600	0.346279
Kurtosis	11.22125	2.306469	1.333741	1.488754	1.553514
Jarque-Bera	190.3081	4.902575	5.866968	5.000548	5.143917
Probability	0.000000	0.086183	0.053211	0.082062	0.076386
Sum	206.7720	29503.89	9488.610	1651.440	9648.860
Sum Sq. Dev.	551.3351	11990153	1375191.	25892.58	1546725.
Observations	48	48	48	48	48

E-View results of the researcher's work

The investigator proceeded to examine the variables' stationarity. This process is used in time series analysis to determine the best method for model estimation. As seen here, the researcher employed the Augmented Dickey Fuller (ADF) unit root test.

Unit Root and Stationarity Test

The stationary test for both level and first difference data is displayed in Table 4.3 below. The findings indicate that although RFC is stationary at the level, ATM, POS, WTR, and MTR are distinct once to be stationary or integrated at order one. The ARDL model that was chosen is justified by the variables' varying orders of integration.

The ADF Unit Test Table 4.3

Variables	MaxLag	Level	1st Difference	Critical Value		Remarks
		ADF Statistics	ADF Statistics	5%	10%	
RFC	9	-8.293306 (0.0000)	-	-2.925169	-2.600658	@1(0)
ATM	9	-	-5.200210 (0.0001)	-2.926622	-2.601424	@1(1)
POS	9	-	-8.111922 (0.0000)	-2.926622	-2.601424	@1(1)
WTR	8	-	-8.177264 (0.0000)	-2.928142	-2.602225	@1(1)
MTR	8	-	-7.832096 (0.0000)	-2.926622	-2.601424	@1(1)

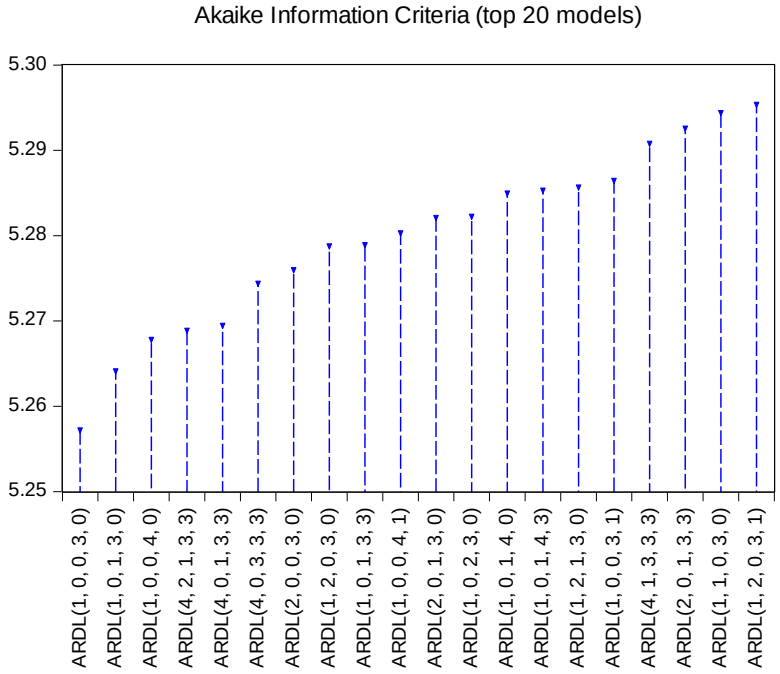
Results from E-view 10.

The model selection process was then carried out by the researcher using the Akaike Information Criterion (AIC), as seen in Figure 4.2 below.

MODEL CHOICE

The ARDL model selection is based on the Akaike Information Criterion (AIC) as shown in Figure 4.2 below. Models are chosen based on information criteria that reduce their values. Figure 4.2 below shows that an ARDL (1, 0, 0, 3, 0) is the optimal model based on AIC. This suggests that the optimal model to describe the researchers' data is one that adds a lagged value of the dependent variable as an extra regressor.

Figure 4.2: AIC-based model selection



E-view the researcher's input's output

Estimation of the Model and Outcomes

Next, using the ARDL framework, the researcher estimated the correlation between bank fraud in Nigeria and e-banking. According to Table 4.4 below, 0.43 decrease in the previous one year of RFC significantly (p-value of 0.0049) affected one unit growth in reported frauds in Nigerian banks. The 0.001-unit growth in ATM insignificantly influenced 1 unit growth in current reported frauds in banks. A 0.005-unit decrease in POS transactions insignificantly impacted on 1-unit growth in current incidence of frauds in banks. Only 0.382 units growth in WTR at lag 3 significantly affected a growth in current reported frauds in Nigerian banks at 5% significant level. With a significant p-value of 0.0082 and an autonomous component or constant (C) of 6.184, it appears that the e-banking variables are not the most important ones in explaining bank frauds in Nigeria's banking industry. The adjusted R-square of 0.24, shows that the explanatory variables jointly accounted for only 24% of the total variation in RFC. The estimated model is very significant, as indicated by the likelihood of the F-Statistic of 0.017. The Durbin-Watson Statistics (Dw) of 2.099, though positive and indicates the absence of autocorrelation in the series, is irrelevant in ARDL model containing lag values. The researchers moved further to test for serial autocorrelation and other conditions by conducting diagnostics tests. With confidence, the researcher states that the model was able to explain the association between e-banking variables and bank fraud in Nigeria to a moderate extent.

Table 4: Estimated Results of ARDL

Dependent Variable: RFC				
Variable	Coefficient	Std. Error	t-Statistic	Prob.*
RFC(-1)	-0.434069	0.144878	-2.996114	0.0049
ATM	0.000757	0.001257	0.601884	0.5510
POS	-0.004914	0.012739	-0.385754	0.7019
WTR	-0.179916	0.120715	-1.490424	0.1448
WTR(-1)	-0.004708	0.131050	-0.035922	0.9715
WTR(-2)	-0.031781	0.131534	-0.241614	0.8105
WTR(-3)	0.382403	0.119790	3.192270	0.0029
MTR	-0.018736	0.018544	-1.010363	0.3191
C	6.184201	2.209289	2.799181	0.0082
R-squared	0.378885	Adjusted R-squared		0.240860
F-statistic	2.745040	Prob(F-statistic)		0.017862
Durbin-Watson stat	2.099918			

EFFECTS OF SIZE OR MAGNITUDE

Our findings demonstrate that, in comparison, ATM has a positive size effect (0.001) on current incidence of frauds in banks than WTR (negative size effect of -0.180). This suggests that ATM transactions account for the majority of fraud cases that are currently reported than the current WTR (which is the opposite). However, in the previous three years, WTR significantly accounted for about 38% more than ATM. This means that in the current period, reported ATM frauds are growing in size, though insignificant, while reported WTR frauds are insignificantly decreasing in size and magnitude. The magnitude of reported frauds emanating from POS is insignificant compared to ATM, MTR and WTR. This is a credit on the users and managers of POS technology in Nigeria. Fraud instances originating from point of sale and mobile banking channels have little, negative effects, or none at all. This has contributed to the rapid growth of POS as a business in Nigeria.

ARDL Bound Test

Test of long-term relationships between e-banking variables and bank fraud is the output of E-view 10 (see table 4.5), which is the ARDL Bound cointegration test. The F-Statistics, derived from the bound test, is 16.68713, exceeding all critical values at 1(0) and 1(1) bounds at 1% to 10%. Within the parameters of

the analysis, we reject the null hypothesis that there is no association at all and instead propose that there is a long-term relationship between bank fraud and e-banking in Nigeria.

ARDL Bound Cointegration Test Table 4.5

F-Bounds Test		Null Hypothesis: No levels relationship		
Test Statistic	Value	Signif.	I(0)	I(1)
F-statistic	16.68713	10%	2.2	3.09
K	4	5%	2.56	3.49
		2.5%	2.88	3.87
		1%	3.29	4.37

E-view 10

Table 4.6: Long-term Form and Cointegrating

Cointegrating Form				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	6.184201	2.209289	2.799181	0.0082
FCM(-1)*	-1.434069	0.144878	-9.898496	0.0000
ATM**	0.000757	0.001257	0.601884	0.5510
POS**	-0.004914	0.012739	-0.385754	0.7019
WTR(-1)	0.165998	0.170176	0.975451	0.3358
MTR**	-0.018736	0.018544	-1.010363	0.3191
D(WTR)	-0.179916	0.120715	-1.490424	0.1448
D(WTR(-1))	-0.350622	0.120764	-2.903360	0.0063
D(WTR(-2))	-0.382403	0.119790	-3.192270	0.0029
Long run Form				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
ATM	0.000528	0.000879	0.600417	0.5520
POS	-0.003427	0.008866	-0.386530	0.7014
WTR	0.115753	0.119128	0.971672	0.3377
MTR	-0.013065	0.013008	-1.004344	0.3219
C	4.312344	1.432767	3.009802	0.0048
-1.434ECM = RFC - (0.0005*ATM-0.0034*POS +0.1158*WTR-0.0131*MTR +4.3123)				

E-view 10

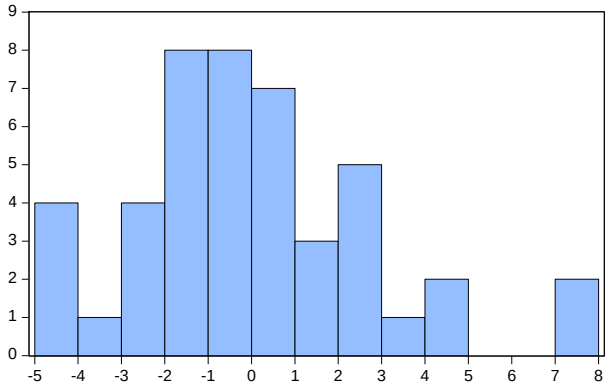
The error correction equation, CointEq(-1), has an anticipated negative sign of -1.434069 and a p-value of 0.0000, as can be seen in the results in Table 4.6, which shows that the model is statistically significant. Additionally, it is evident that 143% of the equilibrium's flaws can be fixed in the following period and that the rate of adjustment is 143%.

Residual Diagnostics

Test for Normality

With a P-value of 0.072686 and a Jarque-Bera Statistic of 5.243226, it is evident from Fig. 4.3 below that the distribution is clearly normal and not significant.

Table 9: Distribution of Normalcy



E-view output

Serial Correlation Test

The table below reveals that Breusch-Godfrey Serial Correlation LM Tests F-Statistic has P-value of 0.7390, which shows non-rejection of the null hypothesis, confirming no serial correlation.

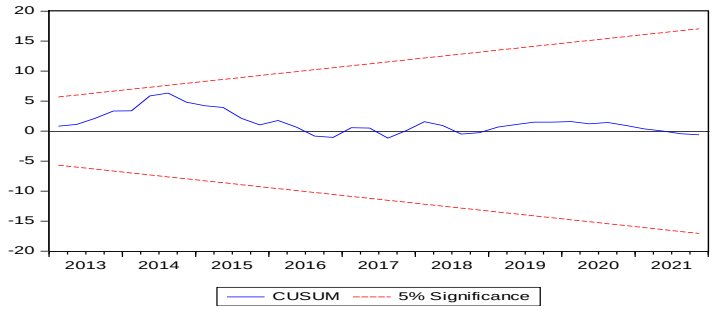
Table 8: Serial Correlation Test

Breusch-Godfrey Serial Correlation LM Test:			
F-statistic	0.305130	Prob. F(2,34)	0.7390
Obs*R-squared	0.793455	Prob. Chi-Square(2)	0.6725

E-view result

Figure 3: The CUSUM (Cumulative Sum Control) Test's Recursive Estimates
Figure 3 below illustrates Recursive Estimates of the CUSUM. It reveals that the blue line lies between the two red lines that represent the bounds of the 5% significance level. This verified the stability of the model.

Figure 3: CUSUM TEST



Effects of size or magnitude

Our findings demonstrate that, in comparison to WTR, ATMs have a beneficial but smaller impact on fraud. This suggests that online transactions account for the majority of fraud cases that are reported, with automated teller machines coming in second. Online transactions have a large but favorable impact on the frequency of fraud in Nigerian banks. Fraud instances originating from point of sale and mobile banking channels have little negative effects, or none at all.

Discussion of the results

According to our data, there is a positive but noteworthy correlation between WEB transactions and documented fraud cases in Nigerian banks. It appears that the number of reported frauds in Nigerian banks has increased in tandem with the growth of WEB transactions. The findings of this study contradict those of studies by Solomon (2016), Jegede (2014), Akpan (2016), Abeenewe, Ogulu and Ndugbu (2013), and Akpan (2016), which contend that ATM use and WTR help banks prevent money loss. However, the current analysis shows that the banking industry has seen more financial losses due to frauds as a result of their expanded use. This is hardly surprising given that fraud in Nigeria has been increasing, particularly due to pin theft, ATM card theft, and ATM detail cloning. Due to the dishonest actions of "Yahoo Boys," who increasingly take advantage of newlyweds, the rate of internet fraud has increased dramatically in recent years. The study demonstrates that the value of reported fraud incidents has a negative and negligible association with mobile banking activities. This shows that the decline in industry-reported scams may have been caused by the increased use of mobile banking. This indicates that as Nigerians utilize mobile banking channels more frequently, fewer frauds are being reported. This is not surprising, since mobile transactions require a user's pin and phone number; a scam of this kind can only happen if the owner of the pin is carelessly copied by fraudsters. Mobile banking uses registered SIM cards that are kept inside cell phones and are constantly handy, as opposed to ATM transactions, which call for clients to visit ATMs and use cards. According to studies by Okon and Amaegberi (2018) and Morfu (2016), mobile banking is still one of the safest e-banking options available and could be profitable for Nigerian banks in the future. The policy's consequence is that banks ought to push their clientele to use mobile banking for more transactions. The value of reported instances shows a negative and negligible correlation with Point of Sales (POS). This implies that despite a rise in POS channels, fewer fraud cases are reported. Despite the fact that POS systems are still largely utilized by restaurants and supermarkets in Nigeria, job seekers have recently avoided using them in order to either build their own jobs or serve their bosses. It is now a useful instrument in Nigeria's fight against fraud. Therefore, one could argue that while point of sale terminals are a practical e-banking solution, neither banks nor customers can use them to stop the growing number of fraud cases that are being reported in Nigeria.

Conclusion

This study attempts to examine the direction and degree of the impact of electronic banking on fraud in Nigerian banks between 2010 and 2021. We used the auto regressive distributed model (ARDLM) and also ran preliminary analysis, including diagnostic checks to achieve robust and reliable results. Electronic banking is disaggregated into automated teller machine, point of sale, internet banking and mobile banking transactions. The results showed that electronic banking was not an important factor in explaining bank fraud in Nigeria's banking industry. The Automated Teller Machine (ATM), Point-of-Sale (POS), mobile banking (MTR) transactions did not influence fraud in Nigerian banks. However, Web (internet) transactions was a negative influencer of fraud in Nigerian banks. This suggested that internet transactions accounted for some fraud occurrences. The researchers recommended that banks and the relevant regulators should reduce losses from fraud by using proactive and rapid response measures and policies, especially in the space of internet transactions. Efforts should be increased in skill training and developments in advanced cyber security measures. Additionally, the gains already made in the areas of ATM, POS and MTR transactions should be sustained.

References

Abaenewe, Z. C., Ogbulu, O. M. & Ndugbu, M. O. (2013). Electronic banking and bank performance in Nigeria, *West African Journal of Industrial and Academic Research*, 6 (1): 170-186

Abubakar, A. (2014), Effect of electronic banking on growth of deposit money banks in Nigeria, *European Journal of Business Management*, 6(33):79-89.

Adeoti, J.A. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *Journal of Social Sciences*, 27(1): 53-58.

Adewumi W. (1986): Fraud in Banks – An Overview. Landmark Publication Ltd. Lagos.

Adeyemo, A. K, (2012). Nigerian bank frauds: their nature, underlying reasons, consequences, and likely solutions, *Journal of Social Sciences in the Mediterranean Region*, 3 (2): 279.

Akingbola, A. A. (2006). Electronic payment systems and telebanking services in Nigeria, *Journal of Internet Banking and Commerce* 11(3): 13–28.

Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). European Journal of Accounting, Auditing and Finance Research, 4(8), 1-19.

Albrecht, W. S., Albrecht, C., & Albrecht, C. C . (2008). Current Trends in Fraud and its Detec tion. *Information Security Journal: A Global P erspective*, 17(1).

Albrecht, W.S. & Romney, M.B. (1986). Red-flagging management fraud: A validation, *Advances in Accounting*, 3, 323-333.

Archibong, E.E., 1992. *The Bank Inspector*. Lib: New born Publishers.

Aruomoaghe, J. A. & Ikyume, J. C. (2013). Accounting for fraud in Nigeria: The banking sector in focus, *International Journal of Research in Management*, 3(6), 59-73.

Ayo, C. K., Adewoye J. O., & Oni A. A. (2010). The State of e-Banking Implementation in Nigeria:A Post-Consolidation Review. *Journal of Emerging Trends in Economics and Management Sciences (JETEMS)*, 1 (1), 37-45

Bello, D. A. (2005) „The Impact of E-banking on Customer Satisfaction in Nigeria“,Munich Personal RePEc Archive, MPRA Paper No. 23200, pp. 1-13

Bhasin, M.L. (2016). The Role of Technology in Combatting Bank Frauds: Perspectives and Prospects, *Ecoforum*, *5(2)*, 200–212.

Donli, J. G. (2002). The situation and prospects of Nigeria's banking sector. 11(6) NDIC Quarterly: 1-16. Ehimen, O. R., and Bola, A. (2010), Cybercrime in Nigeria. *Business Intelligence Journal*, 3(1), 93–98

Idowu, A. (2009). An Assessment of Fraud and its Management in Nigeria Commercial Banks, *European Journal of Social Sciences*, 10, (4), 628-640

Ikpefan, O. A. (2006). Growth of bank fraud and the impact on the Nigerian banking industry, *Asian Journal of Business Management*, 12(7), 1-25

Jegede, C.A. (2014). Effects of Automated Teller Machine on the Performance of Nigerian Banks. *American Journal of Applied Mathematics and Statistics*, 2(1), 40-46.

Kanu, S. I. & Okorafor, E. O. (2013). The nature, extent and economic impact of fraud on bank deposits in Nigeria, *Interdisplinary Journal of Contemporary Research in Business*, 4(9), 253- 265

KPMG (2008). The 2009 Integrity and Fraud Survey. The 21001NSS fraud study 082409.pdf can be seen at http://www.kpmg.com/aci/docs/insights. Accessed April 26, 2016.

Mohammed, S. K. & Siba, S. M. & Sreekumar (2009). Service quality evaluation in internet banking: an empirical study in India, *International Journal of Indian Culture and Business Management*, *Inderscience Enterprises Ltd*, 2(1), 30-46.

Nwaze, C. (2006). Bank Fraud Exposed with Cases and Preventive Measures. Lagos: Control and Surveillance Associates Ltd.

Odi, N. (2013). Implication of fraud on commercial banks performance in Nigeria, International *Journal of Business and Management*, 8(15), 144-150

Ojeaga, P. Ikpefan, O. & Odejimi, D. (2014). Do High Customer Bank Deposits Incite Management Fraud? Examining Causes of Management Fraud in the Nigerian Banking Sector. *Journal of Educational and Social Research* MCSER Publishing, Rome-Italy. 4 (6), 331-341.

Okey, N. (2005). Electronic commerce, company practices, and payment assessment. taken from https://www.ejise.com/issue/download.htm1%3 .

Okoye, E.I. (2016). Anatomy of Fraud and Corruption in Nigeria: A Search for the Pandora Box and Panacea. 32nd Inaugural Lecture of Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. , Available at SSRN: https://ssrn.com/abstract=3055017

Okoye, E. I. and Gbegi, D.O. (2013). An Evaluation of the Effect of Fraud and Related Financial Crimes on the Nigerian Economy, *Kuwait Chapter of Arabian Journal of Business and Management Review*. *2(7), 81-91*

Okoye, E.I. and Akamobi, N.L. (2009). The function of forensic accounting in fraud analysis and legal assistance. *The Nigerian Academic Forum*, November 39–44, J 7 (J)

Olanipekun, W.D., Brimah, A.N & Ajagbe, S.T. (2013). Role of electronic banking in enhancing human resource performance and customer satisfaction: Evidence from Guaranty Trust Bank Plc, Nigeria, *IJSRM*, 3(4), 36-4.

Olatokun, W. M. & Igbinedion, L. J. (2009). The Automatic Teller Machines in Nigeria: An Application of Theory of Diffusion of Innovation. In: Cohen, E., Ed., Growing Information, Part 1, *Information Science*, 373-393.

Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020) E-Fraud in Nigerian Banks: Why and How?. *Journal of Financial Risk Management*, **9**, 211-228.

Owolabi, S.A. (2010). Fraud and fraudulent practices in Nigerian banking industry, *An International Multi-Disciplinary Journal*, Ethiopia 4(3b), 240-256.

Salawu, R. O. and Salawu, M. K. (2007). The Emergence of Internet Banking in Nigeria: An Appraisal. *Information Technology Journal, 6, 490-496*

Salawu, R. O. (2019). Fraud Detection and Prevention: The Role of the Reporting Company and the External Auditors. In Candido Da Rocha Memorial Lecture during the 8th Convocation Ceremonies for the Award of Postgraduate, First and Honorary Degrees of Osun State University (pp. 1-55). Osogbo: UNIOSUN Printing Press.

Siam, A. Z. (2006). Role of the Electronic Banking Services on the Profits of Jordanian Banks. *American Journal of Applied Sciences*, 3, 1999-2004.

Soludo, C. C. (May 2005). a keynote speech given during the National Payments System Committee (NPSC) launch in the Central Bank of Nigeria's Abuja headquarters. https://www.centralbanking.com/central-banking/news/1411733/nigeria-plans-payment-reforms

Sutherland, E. H. (1949). White Collar Crime. New York: Dryden Press.

Taylor P. (1999) *Hackers: Crime in the Digital Sublime*. Brunner-Routledge, 1st edition, 200 pages.

Uchenna, C. & Agbo, J. C. (2013). The effect of fraud and fraudulent activities on Nigerian banks' performance, *British Journal of Arts and Social Sciences*. 15(1), 12-28.

Ugwu, E. (2008). CBN, banks to tackle ATMs' hitches. Retrieved April 25, 2013, from http://www.guardiannewsngr.com.

Wang, Y.-S., Wang, Y. M., Lin, H. H. & Tang, T. I. (2003). Determinants of User Acceptance of Internet Banking: An Empirical Study, *International Journal of Service Industry Management*, 14(5), 501–519.

Wolfe, D., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal*, 74(12), 38-42

Worku, G., Tafa, M.A., and Tilahun, A. (2016). Customers of Dashen and Wogagen banks in Gondar City are the focus of this study on the effect of electronic banking on customer satisfaction in Ethiopia's banking sector. *Journal of Financial and Business Affairs*, 5 (2), 1–18.