Texila International Journal of Academic Research
ISSN: 2520-3088
DOI: 10.21522/TIJAR.2014.11.04.Art007

Impact of Electronic Banking Fraud on e-platforms. Study of Markets in Abeokuta South Local Government Area Ogun State Nigeria

Raphael Usifo Ibhayelia[1]
[1]*Department of Management, Texila American University, Guyana*

Abstract

Electronic banking products are choice alternative to cash payments, globally. However, local people to prefer cash payment in developing environments. The local markets in Abeokuta South Local government area are just like any other local market in developing economies where cash is the major means of payment. The study was carried out to see how fear of e-fraud affect buyers and sellers, in the choice of what payment method to use, in the area of study. With a sample of 50 respondents taken at random from each of the four main local markets, and analyzed with inferential statistics. The result revealed that the market people did not have the same level of fear for all the products. Result showed people felt safer with POS transactions as compared to other electronic platforms.

Keywords: *Cash Payments, Electronic Banking Fraud, Electronic Banking Product, Local Markets.*

Introduction

Electronic banking refers to the use of electronic bank-products such as mobile telephone - banking applications (and mobile communication devices), ATM cards, POS terminals and self-serve internet resources in performance of banking transactions. It includes virtual banking, internet banking, POS services and every other process that makes use of information technology to enable self-service among users. Doug, 2024 defines electronic banking as "the use of computers, phones, and other technologies to facilitate banking transactions rather than through human interaction. Electronic banking avails users ease of transactions, great speed in transactions, comfort of transactions and providing efficiency. Electronic banking products make life easier for users as people don't need to go the banking hall to physically carry out many types of transactions as they can effect such transactions, from the comfort of their homes and in any other place of their choice. The availability of electronic banking also serves as source of income, to banks and the other service providers. The suits of product may differ for each bank but, they are essentially aimed at the same goals.

However, despite the great benefits derivable from electronic banking system to users and the financial institutions providing the services, they are also vulnerable to security challenges resulting to loss of funds to fraudsters. [3] states that " electronic banking frauds have been issue of concern all over the world. It has left so many banks bankrupt, and caused many customers so much pain. Fraudsters are inventing newer techniques continually to elude detection and rub banks and customers of their possessions".

These attacks in the area of study, occur in various ways such as theft of identity, through hacking of peoples' accounts, stealing of personal information through phishing, implantation of Trojans, take-over of users' accounts, cloning of ATM cards and constant innovations by fraudsters. Even though threat

Received: 17.09.2024 ***Accepted: 15.10.2024*** ***Published on: 30.10.2024***
****Corresponding Author: raphaelusifo@yahoo.com***

of e-fraud is a global challenge, it is a major one in Nigeria generally and in the area of study in particular because the threat is compounded by the high level of illiteracy among users, seeming lack of security infrastructures and poor services by the banks in protecting the users. As a result, the electronic banking has not been fully accepted by majority of people in the area of study, not because they don't need it but due to their reservation about the vulnerability and frauds that are common with the products

Basic security feature of electronic banking products is that they are user-friendly and can be used directly and personally outside the direct intervention of the bankers, outside the banking halls. The users have personal responsibility to use the items without the immediate intervention from banks staff and users have a primary responsibility to protect themselves against attacks by securing their banking details, private. holders.

A common form of electronic banking fraud occurs through attack on accounts through acquisition of the telephone sim cards of their victims. Fraudsters often gain access to accounts of people by hacking the telephone lines of their victims and accessing the accounts that are linked to such numbers. This type of fraud known locally as 'fire fire' is done by using special codes to access the linked BVN and account details of the owners. With these details of the victims acquired, fraudsters steal funds and some fraudsters go further to use the personal details to obtain online loans and purchase items online. Electronic banking Frauds often also involve identity theft.

Relevance of the Research

The aim of this study is unravel the impact of fraud, on the usage of electronic banking products, in **Abeokuta**. The study is considered relevant because, it seeks to unravel electronic banking fraud and improve on the adoption of alternative payment systems in the area of study. It is also relevant because, it seeks to know how the choice of the traders in area of study, is affected by incidence of electronic fraud.

The study is unique because, there is no similar study that has been done on this topic (on the area of study) as much as the writer is aware of, that deals with this specific problem even though there are general studies and literature on electronic banking and frauds in electronic banking.

Problem Statement

Nigeria is in the process achieving a cashless economy but, people at the grassroots especially market people and petty traders are slow to adopt this method of payment. This does not appear to be necessarily because people hate changes but, it appears to be because of the challenges they are facing with the changes. Amongst these challenges is the threat of fraudulent attacks on electronic payment methods. "There are cases of bank customers that decline the use of electronic banking without any reason, but for the fear of not being hoodwinked" [9]. This creates the need to study the role that electronic banking frauds play in determining the behaviour of the people at the grassroot, in adopting electronic banking and offer solutions increasing the impact of the Cashless policy. It also creates the need to study and provide solutions to the fear.

Research Objectives

The general objective of this study is to discover how electronic banking fraud affects choice of market people and provide academic input to resolving the menace of electronic banking frauds in the area of study. It is also to serve as a point of reference, on the drive to achieve cashless economy in Abeokuta Ogun state of Nigeria.

The specific objectives are:

1. To determine how the incidence of electronic frauds affects decision

behaviour of individuals in the area of study, in respect of whether or not to use electronic banking facilities.
2. To proffer solution on how to improve on the usage of electronic banking products in the area of study.

Research Questions

1. What are the factors responsible for the choice of people / traders using electronic banking systems in the market?
2. Does the incidence of electronic banking fraud affect the usage of electronic banking products in the area of study?
3. What is the relationship between incidence of electronic banking frauds and people's usage of electric banking products in the local markets Abeokuta South Local government area of Ogun State Nigeria?

This paper relies on both primary and secondary data. The primary data is based on information gotten by the researcher from the samples from the area of study while the secondary data refers to the existing information already existing in the literature of other researchers, that are relevant to the issues here.

Literature Review

Types and Definition of Fraud

Fraud does not have a single universal definition. However, it may be defined as "a deliberate act (or failure to act) with the intention of obtaining an unauthorized benefit, either for oneself or for the institution, by using deception or false suggestions or suppression of truth or other unethical means, which are believed and relied upon by others" [5]. In describing the attributes of fraud, MacEwan University states that, "Fraud is crime, a knowing misrepresentation of the truth or concealment. The deliberate theft, misuse, or misapplication of an organization's assets or resources for personal gain" [6]. This kind of fraud includes any fraudulent act that the doer employs and electronic channel to perpetuate whether directly or indirectly. Fraud "is not an error that someone made or something that accidentally occurred" (MacEwan University) even though it might have been aided by a mistake from victim or another person.

Ref. [3] defined electronic banking frauds "as frauds associated with electronic banking perpetrated using ATM, POS, internet and mobile banking platforms. They further stated that, "electronic banking frauds are achieved through the following: "i) Impersonation: exposing secrete identities to a third party who impersonate and defraud the owner. ii) Phishing and spooling: giving response to futile text messages by revealing identities which are later used to defraud victims. iii) Hacking: using random code generating software developed specifically for frauds purpose to hack into any matching account and defraud victims. iv) Bankers: liaise with fraudsters by providing identities that are used to defraud banks and customers. v) Trojan horse: the interface with user login to divulge user's secret personal codes/identities which is in turn used to defraud victims" [3].

The scope of definition of electronic banking fraud is getting wider as ingenious fraudsters introduce new tricks different products by the day. The term generalizes includes any usage of mobile electronic device or process, to fulfil fraudulent intentions.

Common Frauds Involving Electronic Banking Products in Abeokuta

Debit and credit card are often the subject of attack by fraudster. The actual cards could be stolen from the account holders violently or tacitly and used to commit fraud. Also, when the actual cards are not available, the personal details of card holders is sufficient and could also be fraudulently obtained through usage of fraudulent/phony websites and used to defraud owners, These frauds could also occur as a result of exposure of card numbers and passwords to fraudsters, done by the bankers.

Fraudulent attacks on the funds of ATM card users have been a major dissatisfaction for the banking public in the area of study. Moreover, between 2007 and 2013, the major attack on bank customers in Nigeria was vide cloned ATM cards. Fraudsters were able to duplicate customers cards and withdraw money from their accounts.

There have been numerous newspaper reports on alarming electronic banking frauds, in Nigeria. For instance, Leadership newspaper, (2024) read that "data released by the Nigeria Inter Bank Settlement System (NIBSS) show that, while losses to fraud in the financial industry in the first quarter (of 2023) stands at N5.1billion, the figure has so far risen to N9.5 billion as at July 2023. This brings the total amount lost to fraud since 2019 to N50. 5 billion". N50bn was the equivalent of USD 78, 284, 014.40 at the mom prevailing exchange rate. Furthermore, the Premium times newspaper of 2nd March 2022 reported that "an investigator with the Economic and Financial Crimes Commission (EFCC) told a Lagos court how four bank officials cloned ATM cards and linked some accounts to them to steal N874 million belonging to Fidelity Bank and its customers in 2019 [10]. That was the equivalent of USD1,950,892.86 at the then exchange rate of N448 to one USD. A weakness that enables enabled this fraud (cloning of ATM cards) globally is that the cards operated with magnetic strips. However, following the directive of the Central Bank of Nigeria, this weakness has been corrected by usage of chips and pin.

Internet banking frauds: Following the availability of portable telephones (GSM) to the general masses in Nigeria and consequent availability of internet services, several people are now able to process transactions online and carry out transactions, instead of going physically to the bank. However, these electronic products are faced with fraudulent attacks on customers accounts on the internet.

The growth of cybercrime – particularly hacking, identity theft, phishing, Trojans, service denial attacks and account takeover– has created several challenges for financial institutions, especially regarding how they protect their assets and prevent their customers from becoming victims of cyber fraud. These criminal activities have remained prevalent due to certain features of cyber, such as the borderless nature of the internet and the continuous growth of the computer networks" [4].

The increase in temptation to carry out fraudulent attacks of electronic banking products is a result of the vulnerability, economic situation, lack of adequate control from stakeholders and gullibility of users.

Pattern of Electronic Banking Fraud

Fraudsters have been noted to often target new accounts and take advantage of the naiveness of the owners. Often when accounts are opened in commercial in Nigeria, banks and customers receive account notification of the account numbers and ATM cards, they receive phone calls from fraudsters callers who pose as staff of the bank requesting for details of the banking instruments. Such fraudulent callers are often fully armed with the names of the account holders, Bank Verification Numbers (BVN) and account numbers and what they ask for often are the ATM card details. When such details are released to them by the account owners, the fraudsters use them details to defraud the accounts by gaining access electronically to such accounts. Therefore, banks are consequently constantly educating customers not divulge banking information over the phone to persons. But the big question has been how such fraudsters obtain the information of the account holders in the custody of the banks if people close to the account opening process in the banks did not provide them. This shows that there is an unknown point leakage where information from Nigeran banks are getting to fraudsters.

Even the owners of old accounts also receive strange calls from purported staffs of banks requesting for personal details of the account.

Money transfer frauds: This occurs in cases where fraudsters plead with unsuspecting innocent people to accept transfers into their accounts with the excuse that their (fraudster's) ATM cards are faulty or lost. When such incoming transfers are allowed by the unsuspecting victims, they turn-out to be funds from kidnaping, fraud and other crimes. By transferring illicit funds to accounts of innocent people and receiving the equivalent in value or cash from them, fraudsters successfully avoid being part of the recorded audit trail of such funds and avoid being caught in police investigations. Fraudsters often attempt to employ the use of the account belonging to innocent persons to receive proceed of fraud, in order escapee being identified as the actors in crime scenes. Fraudsters have been seen to buy items and then ordering the transfer of fraudulent funds to the accounts of innocent sellers persons, in a form of receiving illicit funds. They (fraudsters) would receive goods while innocent sellers would receive illicit funds. There are also people who have used fake transaction alerts to defraud unsuspecting sellers as evidence of payments. They would generate fake text alerts generated from telephone applications representing payments to unsuspecting sellers in exchange for goods, from unsuspecting sellers.

Electronic fraud increased due to the drive to cashless economy. With transactions moving to electronic channels and greater number of people adopting electronic channels, the volume of transactions increased and multiple channels are now available. But the level of knowledge that will protect the users is not sufficient.

Fraudsters who access the banking details of victims could obtain loans in the accounts of the victims, could buy items online using their credit card and could steal in any form imaginable.

Theories of Fraud

The earliest theory of fraud is the White collar theory of fraud in 1944 by Edwin H. Sutherland. This theory refer to frauds committed by professionals without violence and for financial advantage. This theory speaks of fraud cases where the preparators are the staff of the financial institutions use their advantaged knowledge and position to steal. The theory known as Fraud Triangle theory was formulated by Donald R. Cressey. This was a study of White Collar crime theory. This theory assets that there are three foundations based on which fraud can or will occur. These basis are Opportunity, Rationalization and Financial pressure. There has been further development in the theories such as the Fraud Scale, Fraud Diamond, M. I. C. E. model, and A-B-C Analysis which all attempt to tell why, how and when fraud occurs and how to prevent it.

Figure 1. Fraud Triangle (Maniya, 2019)

Empirical Literature Review

Ref. [8] investigated the evolution of fraud theory and it's relevance to fraud prevention. on the village government in Indonesia. The research revealed and it was observed that strong internal controls in an organisation could prevent fraud from occurring. The study also established that review of fraud theories could prevent fraud from reoccurring.

Ref. [2] studied E-Fraud committed by staff of Nigerian banks to know why and how they occurred. Using as sample of 120 respondents from fraud investigators in commercial banks in Nigeria, the study undertook to know why e-frauds are committed by staffs of Nigerian banks. It was observed that pressures such financial, occupational presures, integrity issues, systems vulnerability were responsible for the high level of incidence of bankers' involvement in electronic of bankers to temptation to commit e-fraud.

Ref. [4] studied prevention of e-banking fraud and detection in Nigerian banks using mixed research methods. The study revealed that " the factors contributing to the increase in e-banking fraud in Nigeria include ineffective banking operations, internal control issues, lack of customer awareness, lack of staff training and education, inadequate infrastructure, presence of sophisticated technological tools in the hands of fraudsters, negligence of banks' customers concerning their e-banking account devices, lack of compliance with the banking rules and regulations, and ineffective legal procedure and law enforcement. In addition, the enforcement of rules and regulations in relation to the prosecution of financial fraudsters has been passive in Nigeria. Moreover, the findings also show that the activities of each stage of fraud management lifecycle theory are interdependent and have a collective and considerable influence on combating e-banking fraud." Fadayo , 2018.

Ref. [7] studied the impact of card fraud on Customers' Confidence in alternative banking channels using data from Central bank of Nigeria, Nigeria Deposit Insurance Corporation and Nigerian Electronic Fraud Forum. The studies revealed that while Nigeria has aligned with developed countries adopting the comfort of electronic banking, fraudsters have taken advantage and this has affected the confidence of users of electronic banking products in Nigeria, negatively. The results showed negative relationship between card frauds and customer confidence in alternative banking channels. The research concluded that card frauds affect customer confidence in alternative banking channels negatively leading to customers preferring in-branch transactions. The paper recommended improved collaborations between banks and CBN to tackle frauds and leverage on the Bank Verification Number platform to improve security of transactions on ABCs through biometric authentication.

Ref. [3] studied electronic banking fraud, fraud detection and control observed that the use of artificial neural network and geographic information system (GIS) to track criminal activities in hotspot areas is a solution to the threat of cybercrimes. This (a concept called he referred to as geocoding), utilizes a map created to show patterns and trends of crime. This method is a policing measure to curtail the threat of cybercrimes. [3] further noted that computer security can be used also to protect against electronic fraud by means of installing blocking software, V-chip, Browsers with ratings, Audit controls, Encryption, People controls, Fire walls, Access point cloaking. The study further analyses access control in terms of usage of access authorization, anti-virus software to debug viruses and malware, cryptography, Biometric authentication and Legislations and policies

Materials and Methods

Research Instrument

The research instrument used for this research, is a structured questionnaire designed by experts, specifically for the study.

Sampling Technique

A sample of 50 persons made up of sellers and buyers chosen at random, were selected from each market in the area of study. The questionnaires were hand delivered to the respondents by assistants of the researcher and the completed forms retrieved in the same way. This result shows the impact of electronic banking fraud on demand for electronic banking products, case study of markets in Abeokuta using the descriptive and inferential statistics. 50 respondents responded to the questionnaires

Research Method

The study was carried out as a correlational research. The correlational research method is used for situation when variables have association be positive or not which, is the purpose of this research that is, to study the association between the independent variable (fraud in electronic banking) and the dependent variable (choice of payment method).

The population of the study consists of the local markets in Abeokuta South Local government area in Ogun state of Nigeria. Four markets were selected out of the 8 recognizable markets in the area which includes the large gathering of closely associated shops and stores. A sample of 50 persons from market was targeted purposively, and issued structured questionnaire that was constructed by professional, for this research. The questionnaires were distributed and retrieved by the aids of the researcher and analyzed using simple percentages.

Results

Descriptive Analysis

Table 1. Gender Data of the Respondents

Location	Female		Male		Unknown		Mean
(Market)	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage	
Omida	31	62	18	36	1	2	16.67
Paseke	22	44	8	16	20	40	16.67
Kuto	16	32	33	66	1	2	16.67
Adatan	3	6	47	94		0	25.00

Source: Author's computation

Table 1 reveals that 62% of the respondents are female and 36% are male in Omida market. 44% of the respondents are female and 16% are male in Paseke market. 32% of the respondents are female and 66% are male in Kuto market and 6% of the respondents are female and 94% are male in Adatan market. The Statistics shows we have more of men in Adatan and high population of female in Omida in respond to this research.

Table 2. Age of the Respondents

Location	Less Than 20		21-30		31-40		41-50		51 & Above		Mean
(Market)	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	
Omida	5	10	6	12	13	26	15	30	11	22	10
Paseke	7	14	15	30	18	36	7	14		0	11.75
Kuto	5	10	8	16	9	18	11	22	14	28	9.4
Adatan	3	6	9	18	12	24	8	16	10	20	8.4

Source: Author's computation

Table 2 reveals that respondents with highest populations are above 21 years above.

Table 3. Respondents Education Background

Location	No Formal Edu.		Primary Edu.		Secondary Edu.		Tertiary Edu.		Post-Graduate		Mean
(Market)	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	
Omida	5	10	3	6	19	38	7	14	11	22	9
Paseke	1	2		0	18	36	18	36	11	22	12
Kuto	1	2	6	12	8	16	8	16	9	18	6.4
Adatan	3	6	5	10	9	18	9	18	3	6	5.8

Source: Author's computation

Table 3 reveals that most of the respondents have secondary, tertiary and post-graduate education in all the market sampled

Table 4. Respondents Connection to Market

Location	Trade/Shop Owner		Consumer		Others		Mean
(Market)	Freq	%	Freq	%	Freq	%	
Omida	37	74	8	16	4	8	16.33
Paseke	41	82		0	7	14	24
Kuto	36	72	4	8			20
Adatan	43	86		0			43

Source: Author's computation

Table 4 reveals that most of the respondents are trader and shop owners in all the market sampled

Table 5. Respondents Payment Methods in the Market

Means of Mobile Payment		Omida	Percentage	Paseke	Percentage	Kuto	Percentage	Adatan	Percentage	Mean
Pos	Yes	9	18	26	52	9	18	16	32	15
	No	36	72	14	28	30	60	32	64	28
Mobile Money	Yes	44	88	37	74	38	76	37	74	39
	No	6	12	6	12	5	10	7	14	6
Online Banking	Yes	35	70	31	62	32	64	19	38	29.25
	No	6	12	6	12	8	16	13	26	8.25

Source: Author's computation

Table 5 Reveals that most of the respondents use mobile banking and online banking in all the market sampled than POS

Table 6. Respondents on Frequency of Payment Methods in the Market

Type of Mobile Platform		Omida	Percentage	Paseke	Percentage	Kuto	Percentage	Adatan	Percentage	Mean
Pos	Daily	9	18	21	42	11	22	14	28	13.75
	Weekly		0	2	4	2	4		0	2
	Monthly		0		0		0		0	0

	Rarely		0	3	6	2	4	2	4	2.3
Mobile Money	Daily	37	74	36	72	28	56	30	60	32.75
	Weekly	1	2	3	6	1	2	5	10	2.5
	Monthly	1	2		0		0		0	1
	Rarely	5	10	3	6	9	18		0	5.67
Online Banking	Daily	30	60	24	48	17	34	6	12	19.25
	Weekly	1	2	2	4	2	4		0	1.67
	Monthly		0		0		0		0	0
	Rarely	3	6	4	8	8	16	6	12	5.25

Source: Author's computation

Table 6 reveals that most of the respondents perform frequency of payments of electronic banking daily.

Research Question 1: What are the Factors Responsible for the Choice of People/Traders using Electronic Banking Systems in the Market?

What factors encourage you to use POS terminals?

Table 7. Factors that Encourage the Use of POS Terminals

		Convenience of card payments	**%**	**Availability of POS terminals in the market**	**%**	**Acceptance by a majority of traders**	**%**	**Lower transaction fees compared to other digital methods**	**%**	**Mean**
Omida Market	VH	9	18	8	16	8	16		0	8.33
	H		0	1	2	1	2	1	2	1
	M		0		0		0	1	2	1
	L		0		0		0	2	4	2
	VL		0		0		0		0	0
Paseke Market	VH	14	28	14	28	10	20	4	8	10.5
	H	5	10	7	14	11	22	5	10	7
	M	4	8	4	8	4	8	4	8	4
	L		0		0	2	4	3	6	2.5
	VL	1	2		0	1	2	3	6	0
Kuto Market	VH	11	22	5	10	7	14	2	4	6.25
	H		0	2	4	4	8		0	3
	M	3	6	1	2	2	4	2	4	2
	L		0		0		0		0	0
	VL	3	6	1	2	1	2	3	6	2
Adatan Market	VH	8	16	5	10	6	12	1	2	5
	H	2	4	3	6	1	2	4	8	2.5
	M	3	6	3	6	2	4	1	2	2.25
	L	1	2		0		0	1	2	1
	VL		0		0	1	2		0	1

Source: Author's computation

Table 7 reveals that most of the respondents were motivate to use POS terminals in all the markets.

What are the reasons for using mobile money services?

Table 8. Reasons for Using Mobile Money Services

		Ease of use via mobile phones	**%**	**Lower transaction costs**	**%**	**Availability of mobile money agents**	**%**	**Ability to perform transactions remotely**	**%**	**Financial inclusion for those without bank accounts**	**%**	**Mean**
Omida Market	Vh	37	74	21	42	4	8	35	70		0	24.25
	H	6	12	9	18	9	18	6	12	3	6	6.6
	M	1	2	4	8	7	14	1	2	1	2	2.8
	L		0		0	3	6	1	2	4	8	2.67
	VL		0		0		0		0		0	0
Paseke Market	Vh	37	74	21	42	8	16	25	50	4	8	19
	H	4	8	6	12	2	4	4	8	4	8	4
	M	1	2	4	8	4	8	3	6	4	8	3.2
	L		0	1	2	5	10	2	4	3	6	2.75
	VL	1	2	1	2	2	4		0	4	8	2
Kuto Market	Vh	33	66	10	20	6	12	24	48		0	18.25
	H	1	2	4	8	4	8	8	16	2	4	3.8
	M	3	6	4	8	8	16	4	8	3	6	4.4
	L		0	1	2	3	6		0	1	2	1.67
	VL		0		0		0		0	1	2	1
Adatan Market	Vh	33	66	5	10	9	18	24	48	3	6	14.8
	H	5	10	12	24	3	6	7	14	3	6	6
	M	2	4	8	16	4	8	4	8	2	4	4
	L		0	1	2	1	2		0	1	2	1
	VL		0		0		0		0		0	0

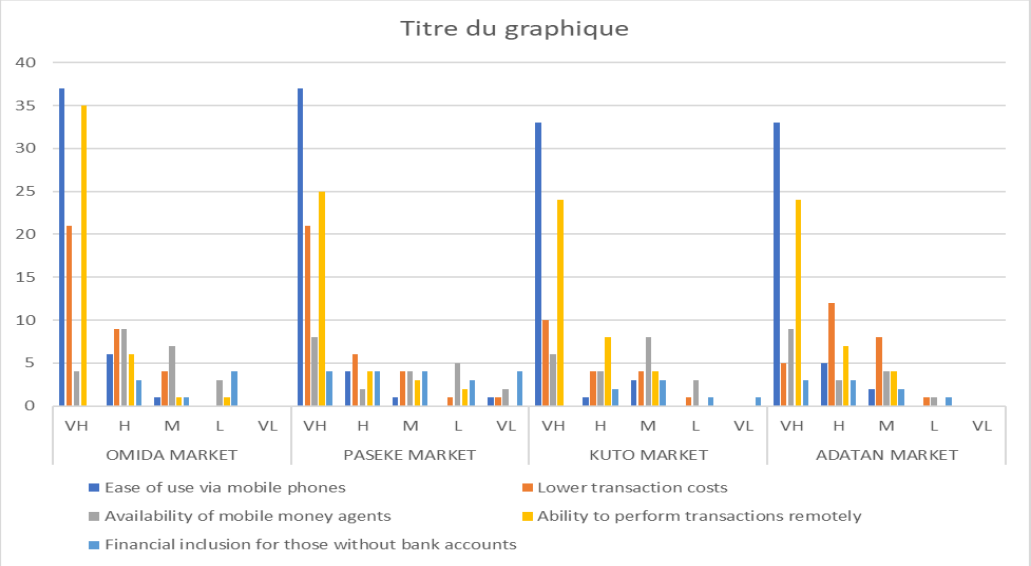

Figure 2. Chart Showing the Respondents Reasons for Using Mobile Money Services

Table 8 shows that most of the respondents were motivated to use mobile money services.

What factors drive the use of online banking?

Table 9. Factors that Drive the Use of Online Banking

		Accessibility From Anywhere With Internet	**%**	**Convenience of Online Transactions**	**%**	**Integration With Other Financial Services**	**%**	**Ease of Managing Multiple Accounts**	**%**	**Mean**
Omida Market	Vh	25	50	24	48	5	10	6	12	15
	H	7	14	5	10	5	10	3	6	5
	M	2	4		0	11	22	4	8	5.67
	L		0		0	5	10	5	10	5
	Vl		0		0		0		0	0
Paseke Market	Vh	22	44	12	24	7	14	12	24	13.25
	H	2	4	11	22	4	8	2	4	4.75
	M	3	6	1	2	5	10	2	4	2.75
	L		0		0	2	4	2	4	2
	Vl	3	6	2	4	3	6	2	4	2.5
Kuto Market	Vh	10	20	10	20	7	14	4	8	7.75
	H	8	16	6	12	4	8		0	6
	M	5	10	1	2	1	2	2	4	2.25
	L	1	2		0	3	6	4	8	2.67
	Vl		0		0		0		0	0
Adatan Market	Vh	6	12	3	6	1	2	2	4	3
	H	3	6	4	8	3	6	2	4	3
	M	2	4	1	2	1	2	2	4	1.5
	L		0		0	1	2	2	4	1.5
	Vl		0		0		0	2	4	2

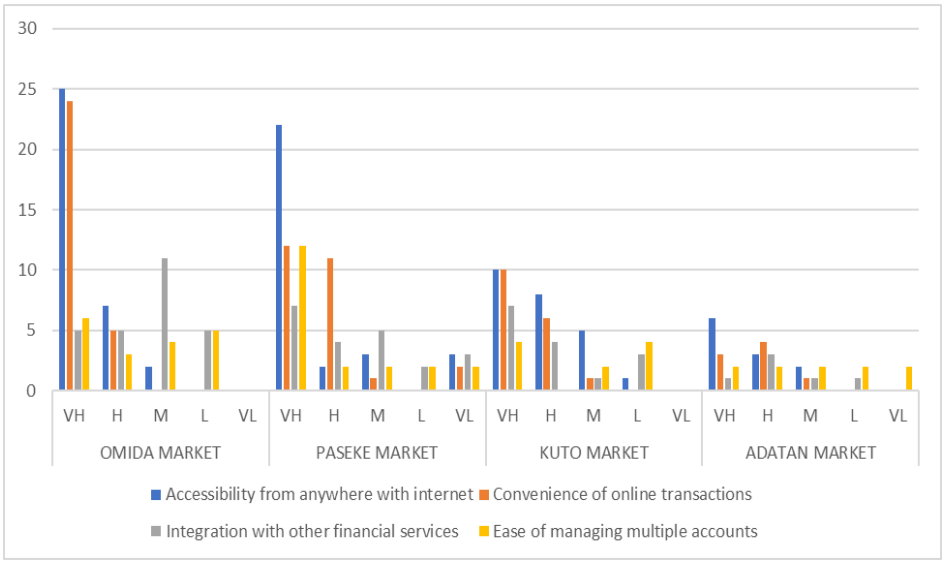

Figure 3. Chart Showing the Respondents Reasons for Using Mobile Money Services

Table 9 reveals that most of the respondents in Omida and Paseke markets were using mobile money service but few respondents were using mobile money services.

Research question 2. Effect of electronic banking fraud on the usage of electronic banking products

Table 10. Effect of Electronic Banking Fraud on Electronic Banking Products

		Availability of payment infrastructure (e.g., POS terminals, mobile networks)	**%**	**Financial literacy**	**%**	**Security concern**	**%**	**Perceived security on POS**	**%**	**Lack of access to digital payment systems**	**%**	**Mean**
Omida Market	Vh	26	52	21	42	6	12	1	2	12	24	13.2
	H	15	30	19	38	25	50		0	5	10	16
	M	3	6	5	10	13	26	4	8	13	26	7.6
	L		0		0		0		0	7	14	7
	VL		0		0		0		0		0	0
Paseke Market	Vh	24	48	19	38	17	34	7	14	3	6	14
	H	12	24	7	14	15	30	3	6	3	6	8
	M	4	8	5	10	1	2	2	4	3	6	3
	L	2	4	2	4	2	4	2	4	3	6	2.2
	VL		0		0		0	3	6	7	14	5
Kuto Market	Vh	21	42	16	32	14	28	3	6	16	32	14
	H	17	34	18	36	18	36	1	2	4	8	11.6
	M	4	8	2	4	6	12	1	2	3	6	3.2
	L		0	1	2		0	2	4		0	1.5
	VL		0		0		0	2	4	3	6	2.5
Adatan	Vh	17	34	16	32	15	30	1	2	9	18	11.6

Market	H	16	32	11	22	14	28		0	6	12	11.75
	M	2	4	7	14	5	10	3	6	1	2	3.6
	L	2	4		0		0	1	2		0	1.5
	VL	1	2	1	2	2	4	1	2		0	1.25

Table 10 shows that most of the respondents reacted on high effect of electronic banking fraud on electronic banking products.

Research question 3. Relationship between incidence of electronic banking frauds and people's usage of electronic banking products

Table 11. Relationship between Incidence of Electronic Banking Frauds and People's Usage of Electronic Banking Products

		Security Features on Online Mobile Banking	**%**	**Managing Multiple Accounts on Mobile App**	**%**	**Security Alertness**	**%**	**Alertness on the use of Pos**	**%**	**Mean**
Omida Market	VH	2	4	6	12	6	12	1	2	3.75
	H	15	30	3	6	25	50		0	14.33
	M	9	18	4	8	13	26	4	8	7.5
	L		0	5	10		0		0	5
	VL		0		0		0		0	0
Paseke Market	VH	10	20	12	24	17	34	7	14	11.5
	H	4	8	2	4	15	30	3	6	6
	M	4	8	2	4	1	2	2	4	2.25
	L	2	4	2	4	2	4	2	4	2
	VL	3	6	2	4		0	3	6	2.66
Kuto Market	VH	5	10	4	8	14	28	3	6	6.5
	H	4	8		0	18	36	1	2	7.67
	M	4	8	2	4	6	12	1	2	3.25
	L	1	2	4	8		0	2	4	2.33
	VL		0		0		0	2	4	2
Adatan Market	VH		0	2	4	15	30	1	2	6
	H	3	6	2	4	14	28		0	6.333333
	M	4	8	2	4	5	10	3	6	3.5
	L	1	2	2	4		0	1	2	1.333333
	VL		0	2	4	2	4	1	2	1.666667

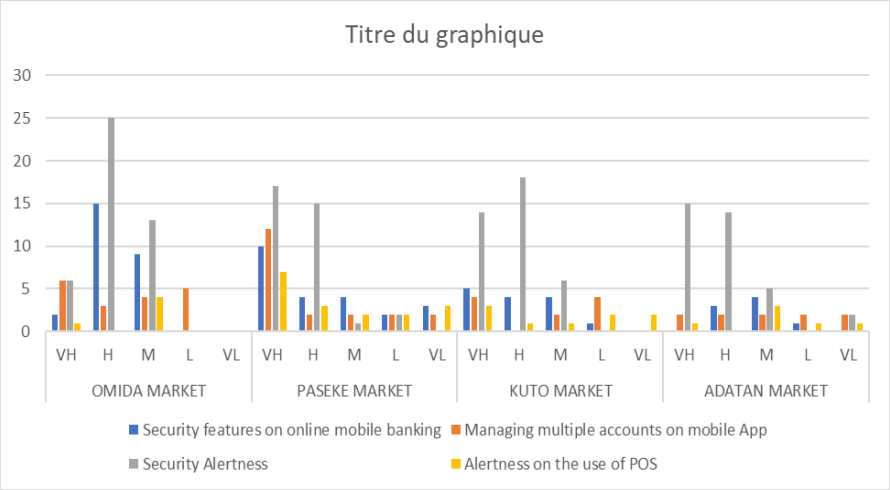

Figure 4. Chart Showing the Respondents on the Relationship between Incidence of Electronic Banking Frauds and People's Usage of Electronic Banking Products

Table 11 reveals that most of the respondents showed a high relationship between incidence of electronic banking frauds and usage of electronic banking products

Interpretation for the Inferential Statistics

Regression Model

Table 12. Table Showing a Regression Model

Model Summary[b]				
Models	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
POS	0.186	0.035	-0.448	6.913
ONLINE BANKING	0.956	0.915	0.872	2.98
MOBILE BANKING	0.941	0.885	0.827	0.885
a. Independent variable: effect of electronic banking fraud				
b. Dependent variable: pos, online banking, mobile banking				

R: This is the pearson correlation coefficient (r) which describes the strength and direction of linear relationship between two or more variables.

The R-value of 0.186, 0.956 and 0.941 for POS, online banking and mobile banking show that there is a strong correlation with effect of electronic banking fraud variable (Table 12).

R-Squared (R^2): The coefficient determination (R-Squared) is used to measure the goodness of fit or the explanatory power of a model. Technically, the R^2 gives the proportion or percentage of the total variation in the dependent variable that is explained by the independent variable (s).

R-Squared (R^2) value of 0.035 shows that about 3.5% have effect on the electronic banking fraud as a result of use of POS while 96.5% is captured by the error term. This shows that the model has a poor fit but 0.915 for online banking which is equivalent to 91.5% and 0.885 for mobile banking which is equivalent to 88.5% have effect on the electronic banking fraud shows that the models have a good fit (Table 12).

Effect and Relationship between Incidence of Electronic Banking Frauds and People's Usage of Electronic Banking Products using Correlation Method

Table 13. Table Showing the Pearson Correlation

Correlations					
		POS	**Mobile App**	**Online Banking**	**Effect of Electronic Fraud**
POS	Pearson Correlation	1	0.156	0.090	-0.186
	Sig. (2-tailed)		0.844	0.910	0.814
	N	4	4	4	4
Mobile App	Pearson Correlation	0.156	1	0.996**	0.941
	Sig. (2-tailed)	0.844		0.004	0.059
	N	4	4	4	4
Online Banking	Pearson Correlation	0.090	0.996**	1	0.956*
	Sig. (2-tailed)	0.910	0.004		0.044
	N	4	4	4	4
Effect Of Electronic Fraud	Pearson Correlation	-0.186	0.941	0.956*	1
	Sig. (2-tailed)	0.814	0.059	0.044	
	N	4	4	4	4
**Correlation is significant at the 0.01 level (2-tailed).					
*Correlation is significant at the 0.05 level (2-tailed).					

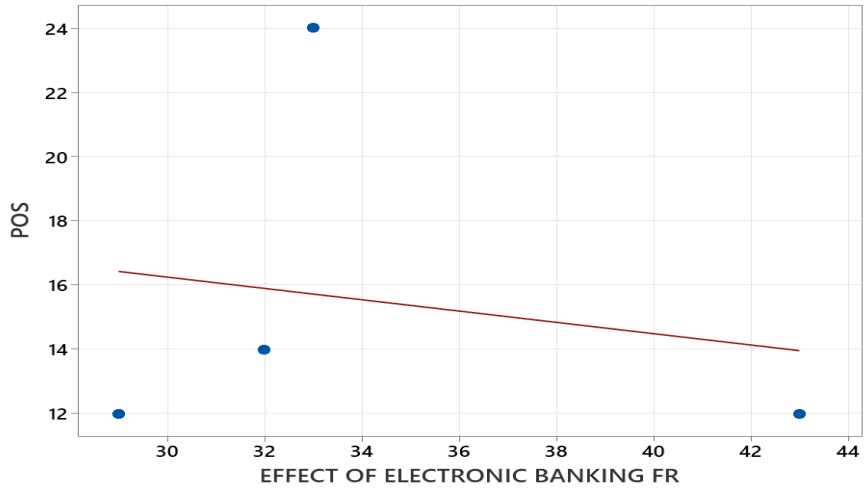

Figure 5. Correlation between Effect of Electronic Banking Fraud and POS in Markets of Abeokuta

1. The correlation between the usage of POS and the effect of electronic banking fraud is -0.186 which is a negative correlation in table 13. This means increase in the usage of POS leads to decrease in the effect of electronic banking fraud (0.814 value is greater than 0.05 significant level which show it is statistically insignificant as shown in figure 5.

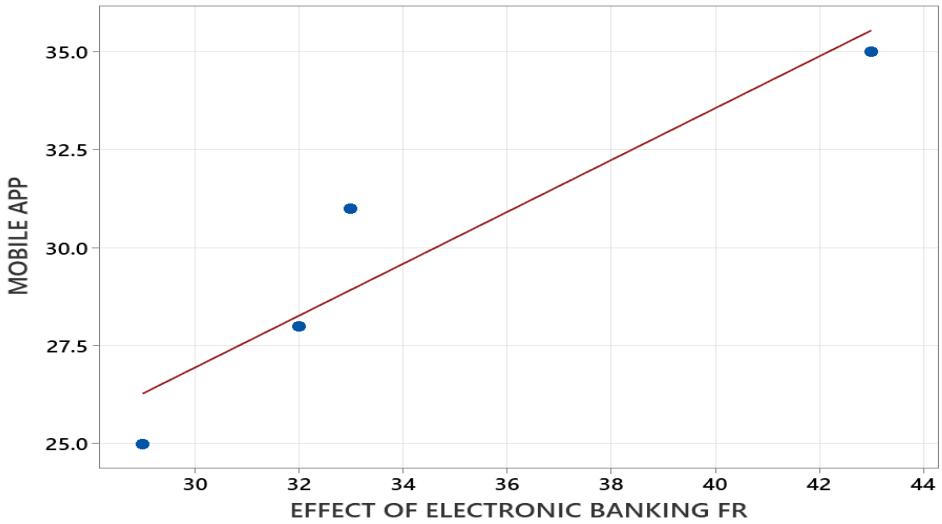

Figure 6. Correlation between Effect of Electronic Banking Fraud and Mobile App in Markets of Abeokuta

2. The correlation between the usage of mobile app and the effect of electronic banking fraud is 0.941 which is a positive correlation (table 13). This means increase in the usage of mobile app has strong effect of electronic banking fraud (0.059 value has an equal significant level (0.05) which show that this analysis is statistically significant as shown in figure 6.

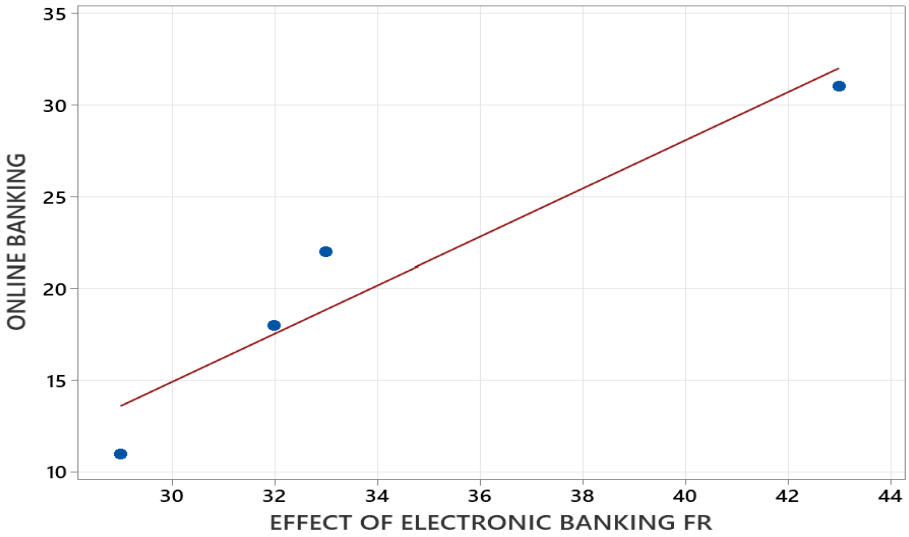

Figure 7. Correlation between Effect of Electronic Banking Fraud and Online Banking in Markets of Abeokuta

3. The correlation between the usage of online banking and the effect of electronic banking fraud is 0.956 which is a positive correlation in table 13, this means increase in the usage of online banking has strong effect of electronic banking fraud (0.044 value is less than 0.05 significant level) which show that this analysis is statistically significant shown in figure 7.

Discussion

Impact of the fear of electronic banking fraud on usage of electronic banking products of buyers and sellers in local market in Abeokuta South local government area, Ogun state Nigeria shows that most of the respondents use mobile banking and online banking in all the market sampled than POS. Based on the choice of people / traders using electronic banking systems in the market. The

findings revealed that 70% of the traders were motivate to use POS terminals in all the markets and 70% of the traders were motivated to use mobile money services. 55% of people in Omida and Paseke markets were using mobile money service but 45% were using mobile money services. 65% of the respondents agreed that there is high effect of electronic banking fraud on electronic banking products. 55% of the people showed that there is high relationship between incidence of electronic banking frauds and usage of electronic banking products. The inferential statistics showing relationship between incidence of electronic banking frauds and usage of electronic banking products reveals that there is negative correlation between the usage of POS and electronic banking fraud, there is positive correlation between the mobile App and electronic banking fraud, there is positive correlation between the usage of online banking and electronic banking fraud. In conclusion, market people did not have the same level of fear for all the products. Result showed people felt safer with POS transactions as compared to other electronic platforms.

Conclusion and Recommendation

The incident of fraud has a negative effect on the choice of electronic payment methods and there is therefore need for the vendors of the products, to carry out more sensitization on the local users to encourage their confidence in the products. Results suggests that users of electronic banking products in local markets could be vulnerable to attacks due to their personal weaknesses such as illiteracy and failure to conceal banking details. Fraudsters target unknowing victims and exploit their ignorance. The results suggest that usage of electronic products, is not affected equally by the threat of fraud. This could possibly influence a higher level of usage.

Conflict of Interest

There is no conflict of interest.

References

[1]. Adegboyega, J. E., Tomola, M. O., 2018, Card Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria. *European Scientific Journal June 2018 edition Vol.14, No.16 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431*, pp. 1857-7431.

[2]. Babatunde, M. O., Mary, K. S., Aderemi, D. A., 2020, *E-Fraud in Nigerian Banks: Why and How?* Retrieved from efraud in Nigeria: https://www.scirp.org/journal/paperinformation?paperid=102767

[3]. Eneji, S. E., Angib, M. U., Ibe, W. E., Ekwegh, K. C., 2019, A Study of Electronic Banking Fraud Fraud Detection and Control. *International Journal of Innovative Science and Research Technology*, pp. 709-711.

[4]. Fadayo, O. M., 2018, *An Examination of E-Banking Fraud Prevention and Detection in Nigerian Banks.* Retrieved from https://www.academia.edu/93245447/An_Examination_of_E_Banking_Fraud_Prevention_and_Detection_in_Nigerian_Banks

[5]. Indiana State Board of Accounts, 2024, *What is Fraud.* Retrieved from What is Fraud: https://www.in.gov/sboa/files/Fraud-and-Business-Ethics.pdf

[6]. MacEwan University, 2024, *What is fraud.* Retrieved from What is fraud: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.macewan.ca/c/documents/ias_fraudbulletin_1.pdf.

[7]. Maniyar, D., 2019, *Financial Statement Frauds & The Fraud Triangle.* Retrieved from Linked In: https://www.linkedin.com/pulse/financial-statement-frauds-fraud-triangle-dhaval-maniyar/.

[8]. Novita, P., 2016, Fraud theory evolution and its relevance to fraud prevention in the village government in Indonesia, *Asia Pacific Fraud*

Journal (apfj - association of certified fraud examiners, acfe).

[9]. Obadeyi, J., 2022, Electronic Banking Fraud and Commercial Banks' Performance: An Empirical Prove of Nigeria, *International Journal of Innovative Research in Accounting and Sustainability*, 89.

[10]. Punch Newspaper, 2017, Cartel running Nigeria's banking sector, CBN losing control – Senate. Récupéré sur Cartel running Nigeria's banking sector, CBN losing control – Senate: https://data.worldbank.org/indicator/FP.CPI.TOTL.ZG?locations=NG.