MPRI-JFRBD | INTERNATIONAL JOURNAL OF FINANCIAL RESEARCH & BUSINESS DEV. VOL. 1 NO. 1 JUN-2022

EFFECT OF CYBERCRIME PRACTICES ON CONFIDENCE OF CUSTOMERS IN ONLINE TRANSACTIONS IN MAIDUGURI METROPOLIS

***DR MOMOH, M.; **ASHIGAR, F. A.; & ***MUSTAPHA, H.**

**Department of Business Admnistration, University of Maiduguri **Faculty of Management Sciences, University of Maiduguri ***CPDDS, University of Maiduguri*

KEYWORDS:
Cybercrime, Online transactions, Financial services, Customers, Confidence.

Abstract

This research investigate the effect of cybercrime on depositor's confidence in electronic transactions within Maiduguri Metropolis. The competitive environment in the financial system has compel the utilization of alternative delivery channels. The most recently delivery channel is the electronic fund transfer system. As good as these may seems, this innovative transaction system has created a new breed of criminality called 'cybercrime'. Therefore, the study evaluates the relationship between cybercrime practices and customers' confidence; and, assess the effect of cybercrime on customers' confidence on online transactions platforms in the study area. The study utilised multistate sampling techniques, which includes purposive and random sampling with interview guide to elicited data from 278 customers alike with fair knowledge of online transactions in the study area. The study reveals high cases of cybercrime practice such as e-financial fraud through online transaction, internet scams, identity theft, Salami attack, phishing, etc. in the area under review. It also found that cybercrime significantly affect

EDITOR-IN-CHIEF
Prof. Ravinder Rena [South Africa]

customers' confidence on the electronic transaction system within the study population. It recommends that the management of the financial service providers should routinely offers sensitization training to their customers and take adequate measure against the practice of cybercrime, such as transfer of funds through the ACH network and banking risk mitigation to enhance customers' confidence.

Introduction

Online transaction refers to electronic financial system, which provide easy access to funding activities and provides effective service delivery. The activities culminating electronic money transfers, online blocking of account functions, retrieving account balance and account history, amongst others. Fields (2018) argues that the financial services that were once randomly accessible to limited customers now become a pathway for financial inclusion for household with speedy, reliable and secure transactions. Indeed, online transactions has gradually become an indispensable part of modern life of both bank officials and customers alike. It help provides sure ways to effectively meet-up the challenges of modern competitive business environment, particularly the financial services. The use of this technological innovations greatly enhance quality of financial services the world over. The innovation ought to enhance effective financial service delivery and boost customers' satisfaction and confidence in the real sense, but largely susceptible to high waves of criminality. Put differently, online transactions enhances satisfaction in a way, and breed grounds for online-crimes tagged 'cybercrimes'. Cybercrime generally refer to fraudulent activities via the online business transactions. The forms of cybercrime practices include identity theft, confiscating online bank account details such as account numbers and passwords, credit/debit card fraud and varied repudiation acts amongst others. Such crimes affect the banking industry greatly as well as customers' confidence on the online transaction system.

As plausible as this innovative offerings, empirical investigation of impact on customers' perception is sacrosanct. A wide literature search reveal

varied documentations of cybercrime practices and its impact on service delivery across the globe. The criminal practices aspect of the innovation has created customers apprehension on the safeguards of their funds via the online transaction system. On a personal note, some citizens prefer investment in landed properties than liquid assets for fear of cyber fraudsters. Experience also has it that for years, cases of hackers and yahoo-yahoo boys are common scenarios. The yahoo-boy for instance, will create anonymous bank officials via phone calls, demanding for necessary customers details such as ATM card number, BVN number and/or the likes. Once such vital account information facts are supplied, the victim within a blink of an eye has his/her account emptied. Hilariously, the financial service providers are deficient in tracking the fraudsters nor adequately avert such fraudulent practices. Similarly, on personal experience, online fund transfers were successfully transacted on the debit side without corresponding credit alerts onto the recipients' accounts. Sometimes it take long time to get that money reversed which frustrate customers' satisfaction. Another motivation for this research is borne on the fact that, within Maiduguri Metropolis, I am aware that many customers are sceptical of online transactions mode and most specifically electronic payments and/or fund transfers.

Therefore, the extent of this negative operatives in finance industry and by extension, the entire economic system in Nigeria is worthy of empirical investigation. To address this research problem, therefore, the study evaluates the effect of cybercrime practices on customers' confidence in e-transactions within Maiduguri Metropolis. Specifically, it investigates the extent of cybercrime practices in the area; and, examines the effect of cybercrime on customers' confidence within the study population. The study hypothesized that:

i. Ho1: There is no significantly recorded cases of cybercrime practices in the area.
ii. Ho2: Cybercrime practices has no significant effect on customers' confidence in the area.

EDITOR-IN-CHIEF
Prof. Ravinder Rena [South Africa]

Conceptual Literature

Meaning and Scope of Cybercrime

The tern cybercrime refers to any criminal activities that involves the use of electronic facilities to perpetuate crimes or any act of criminality. Worku, Tilahun and Tafa (2016) observes that the high interconnectivity to the global networks have created this breed of criminality. Hamid, Razak, Bakar and Abdullah (2016) opines that the advancements in information technology has facilitate more accessibility services and promote public access to information. The easy access to information has equally increase the chances of cyber criminality. Therefore, cybercrime is the prodigious dark side of ICT revolution. More so, IRMA (2019) argues that cybercrime involve fundamental breeches of customers' privacy in forms of assaults information in digital-depositories via online transaction based crimes such as fraud tagged the 'yahoo-yahoo boys in Nigeria, digital piracy, money laundering and counterfeiting. According to Fianyi (2016), cybercrimes varied activities include identity theft, confiscating customers' account information, debit/credit card frauds, amongst other nefarious acts via Automated Teller Machines (ATM), Mobile Banking Applications and Unstructured Supplementary Service Data (USSD) platforms.

Today, many aspects of cybercrime occurs in the banking industry such as credit/debit card fraud, identity theft, Salami attack, phishing, etc. (Fields, 2018). The salami attack, which involve small-scale skimming of many accounts that saw a paradigm shift in the banking industry and greatly affects customers' confidence in online transactions. Cybercrime according to Raghavan and Parthiban (2014), are categorised into four major classes i.e. cyber deceptions, cyber – pornography, cyber –violence, and cyber – trespass. Hussain (2016) identifies cybercrime approaches to include 'Data Crime', 'Network Crime', 'Access Crime' and other types of online crimes. Delpy (2018) identifies different attacks witnessed in online transactions, which include ATM fraud, cyber money laundering and debit/credit card fraud. Generally, the rationale of all cyber frauds are targeted monetary theft by hacking into victims' account credentials like passwords, pins, OTP

code, Tokens, etc. and once done, the stolen amounts are immediately transfer into a 'mule accounts'.

Wada and Odulaja (2012) cited 'cyber terrorism', whereby online criminals lunch attack on government or corporate organisations hacking onto sensitive digital information, committing act of cyber-extortion demanding ransom tagged 'ransomware'. Similarly, Yedaly and Wright (2016) tipped 'identity theft' as online criminality in which someone pretends to be somebody else and retrieve vital information therefrom for his or her advantage. This include hacking login details to gain access to ATM and BVN codes. Indeed, cyber-thieves such as the yahoo-yahoo boys types cybercrime in Nigeria have web-links modules, which requests users to fill in their vital account information to them defraud the victims. Fianyi (2016) cited a case on 9 May 2013, where an international group of cyber-thieves stole more than $45million (US dollars) via ATMs within hours of cybercrime operations. Yedaly and Wright (2016) adds 'spam' as another form of cybercrime where victims receive unsolicited bulk messages indiscriminately targeting victims who tag on-the-screen agreements without reading the 'fine prints' of such agreements. Again, Yedaly and Wright (2016) cited cases of 'malware' dealing with electronic viruses, worms and Trojans, which wreak havoc on victims' digital information. This form of cyber criminality facilitates 'Salami fraud', whereby perpetrators carefully skim small-scale sums from the balances of a large number of victims' accounts in order to bypass internal controls and detection.

Cybercrime and Customers Confidence

Information management literature has been unanimous on effects of cybercrimes on customers' satisfaction and confidence. According to Fields (2018), in the 4th Industrial revolution, a wide range of technologies impinge on financial services for customers' satisfaction and confidence. Indeed, the innovative banking system places lot of emphasis on effective service-delivery for customers' satisfaction and provoking massive online transactions as cost effective technique (Kabir, Dovash, Nafee & Saha, 2019). On this note, Worku, et al (2016) submit that online transaction

services improve financial transactions efficiency and effectiveness as well as faster and most convenient manner. Raghavan and Parthiban (2014) argue that online transactions reduce bank-halls activities, lessen cash-handling effects, reduced operating-cost and enhances service delivery for customers' satisfaction. Raghavan and Parthiban (2014) add that ICT revolution has made human life lives simpler in different industries and finance in particular, but it has also brought unintended consequences in form of cybercrimes, which activities like 'ATM frauds', 'Phishing', 'identity theft', 'Denial of Service', amongst others (Tunmibi & Falayi, 2013).

However, Longe and Chiemeke (2008) worried over the high rate of criminality this banking innovations have created and seriously affecting customers' confidence in the online transaction platforms.

That is, available literature is not ignorant of the effects cybercrime have on depositors' confidence in online transaction system in Nigeria. Evidential cases of fraudulent withdraws from customer's account with huge amount of money without customers' knowing by sampling interjecting the alert system. Ohwovoriole (2019) acclaims that the sum of ₦127billion is loss annually by customers through cybercrime. With the availability of sophisticated firewalls and high electronically secured networks, one wonders how customers account are easily hacked and the banks do not have any system to track the hackers. Similarly, Wada and Odulaja (2012) aptly engrossed the Reuter's media briefs from Cameroon, where the British Prime minister claims, cybercrime costs the British economy some 27 billion pounds a year; whilst, the Economic and Financial Crimes Commission (EFCC) reports ranks Nigeria as third among the top ten sources of cybercrime in the world. Indeed, after the USA with 65 percent and the UK with 9.9 percent, Nigeria is the 3rd hub with 8 percent of cyber criminality in the world.

The growth of online transactions in the last 2 decades has also created huge opportunities for perpetrators of cybercrimes. Within this period, records of funds embezzlement via wire-transfers and account takeovers is on the increase. Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks,

and by compromising online banking payment systems. Identity takeover can also affect online banking, as new accounts are taken-over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions. The risen practices of cybercrime and its effects on the victims and the economy require the formulation of appropriate policy to squarely address it. To this end, IRMA (2019) suggest a rhetorical framework for evaluating surveillance and privacy practices

Theoretical Underpins

This study review theories relative to the subject matter and found consistency with '***Routine Activity Theory***' (RAT) and '***Space Transition Theory***' (STT). The duo theories help explain the situations that facilitate the occurrences and practices of cybercrime in the global world. The proponents of RAT argue that for cybercrime to thrive there must be viable targets, week security networks, and motives to commit crime. ***Whilst the*** Proponents of STT argue that behavioural tendencies of the users in the cyberspace depicts compliance and noncompliance the criminality. Therefore, careful assessment of the prevailing situations largely determine whether a crime takes place.

Methodology

The study investigates the effect of cybercrime on depositor's confidence in online transactions in Nigeria with specific reference to Maiduguri Metropolitan area of Borno State. The study population comprises of estimated 1000 customers with fair online experience in the study area. The study used multistate sampling techniques to elicited data for this analysis. First, it used purposive sampling to select the study area and estimation theory/Taro Yamane Formula to determine the population and sample size respectively.

More so, Random sampling was used for the administration of the 286 questionnaires with the help of 5 research assistance a period of 2weeks. Therefore, the population estimated at 1000 of online financial services customers and the sample is given: n = $\frac{1000}{1+1000(0.05)2}$

EDITOR-IN-CHIEF
Prof. Ravinder Rena [South Africa]

n =**286.** The questionnaire was with five-points Likert scale namely; strongly (SA), Agreed (A), Undecided (U), strongly Disagree (SD) and Disagreed (D) and were administered with interview guide. The resultant data was analysed using cross tabulation, Simple regression Model given as: y = **a+bx**
Where:
a = y intercept
b is associated with X the coefficient of net regression
y = Customers' confidence
x = Cybercrime

Results and Discussions

In the course of the field exercise, 286 copies of the study questionnaires were administered to the respondents and 278 were retrieved and found valid for this analysis. The resultant data were subjected to statistical examination using cross tabulation and regression coefficients.

Test of Hypothesis (H₀1): There is no significant relationship between Cybercrime Practices and Customers' Confidence in the study area.

Table 1: Cross-tabulation for and ***Regression Coefficient Statistics***

Cybercrime Practice (X)	*Customers' Perception (Y)*	*X2*	*Y2*	*XY*
174	60	30276	3600	10440
208	84	43264	7056	17472
165	13	27225	169	2145
139	405	19321	164025	56295
193	828	37249	685584	159804
∑X=879	∑Y=1390	∑X2=157335	∑Y2=860434	∑XY=246156

Source: Field Survey, 2021.

$$\bar{\mathbf{x}} = \frac{\mathbf{879}}{\mathbf{5}} = 175.8$$

$$\bar{y} = \frac{1390}{5} = 278$$

EDITOR-IN-CHIEF
Prof. Ravinder Rena [South Africa]

$$b = \frac{\sum xy - n\sum x\sum y}{\sum x2 - nx2}$$

$$= \frac{24615 - 5(879)(1390)}{157335 - 5(157335)}$$

$$= \frac{24615 - 6109050}{157335 - 786675}$$

$$= \frac{-6084435}{-629340}$$

b = 9.7

$y = a + bx_i$

278 = a + 9,7 (175.8)

278= a +1705

a = 1705-278

a = 1427

Regression Coefficient

$$r = \sqrt{\frac{a\sum y + b\sum xy - ny2}{\sum y - ny2}} = \sqrt{\frac{1427(1390) + 9.7(246156) - 5(1932100)}{1390 - 5(1932100)}}$$

$$r = \sqrt{\frac{1983530 + 2387713.2 - 9660500}{1390 - 9660500}} = \sqrt{\frac{-5289256.8}{-9659110}}$$

$$r = \sqrt{0}.547592562875875 = \mathbf{0.74}$$

Decision Rule

The Regression coefficient statistics (r) is 0.74, which infers existence of high correlation between cybercrime and Customers' satisfaction. On this note, therefore, the research rejects the null hypothesis on pure statistical grounds.

Test of Hypothesis (*H_o*2): Cybercrime Practices has no significant effects on Customers' Confidence in the study area.

Cybercrime Practices (X)	*Customers Confidence (Y)*	*X2*	*Y2*	*XY*
192	56	36864	3136	3420
183	86	33489	7396	2992

EDITOR-IN-CHIEF
Prof. Ravinder Rena [South Africa]

183	16	33489	256	832
191	373	36481	139129	6721
116	859	13456	737881	17009
ΣX=865	ΣY=1390	ΣX2=120290	ΣY2=887798	ΣXY=200305

Table 2: Cross-tabulation for and Regression Coefficient Statistics

Source: Field Survey, 2021.

$$\bar{x} = \frac{865}{5} = 173$$

$$\bar{y} = \frac{1390}{5} = 278$$

$$b = \frac{\sum xy - n\sum x\sum y}{\sum x2 - nx2} = \frac{200305 - 5(865)(1390)}{120290 - 5(120290)} = \frac{200305 - 6011750}{120290 - 601450} = \frac{-5811445}{-481160}$$

b = 12

$y = a + bx_i = 278 = a + 12\ (173) = 2076\text{-}278$

a = 1798

Regression Coefficient

$$r = \sqrt{\frac{a\sum y + b\sum xy - ny2}{\sum y - ny2}} = \sqrt{\frac{1798(865) + 12(1390) - 5(1932100)}{865 - 5(1932100)}}$$

$$r = \sqrt{\frac{1555270 + 16680 - 9660500}{865 - 9660500}} \quad r = \sqrt{\frac{-8088550}{-9659635}} = \sqrt{0}.837355655777883$$

$$\mathbf{r = 0.92}$$

Decision Rule

The Regression coefficient statistics (r) is 0.92, which infers that cybercrime has significant effects on Customers' confidence in the study area. On this note, therefore, the research rejects the null hypothesis (Ho2) purely on statistical grounds.

Conclusions

The study investigates effect of cybercrime on depositors' confidence on electronic banking system in Nigeria. The findings of this study reveal that there is high records of Cybercrime practices in online transactions within the study population with a beta coefficient of 0.74. This finding is consistent with the report of Delpy (2018) who found that 'fear of cybercrime has a measurable soft-cost; and Bakare (2015) who 'evident that some customers are still conservative towards' online transactions.

Similarly, the regression analysis shows very high effect of cybercrime on customers' confidence in the area with a beta coefficient of 0. 92. Impliedly, online transactions service losses reputation to cyber criminality resulting in customers' corresponding loss of confidence in the system. The findings inconsistent with the report of Amaduche, Adesanya, and Adediji (2020: 85), who argue that "e-banking is secured-enough to ensure adequate patronage by customers".

Recommendations

Based on the findings, the following recommendations were made:

i. The bank management should take adequate measure against the practice of cybercrime, such as transfer of funds through the ACH network and banking risk mitigation to enhance customers' confidence.
ii. Customers should be wary of unsolicited supply of their confidential information such as password, personal details, token, credit or debit card details to anonymous officer(s).
iii. The implementation of higher-level security architecture that combine Captcha techniques with stepwise password requires is paramount to curb cybercrime practices in the financial system. Captcha is online security measure, which means the 'Complete Automated Test to Put Computer and Human Apart'.
iv. There is the need for continuous customers' education to create awareness on the knowledge of various authentication system for online transaction in the financial system. The knowledge of such s security architecture includes but not limited to 'Denial of Service (DOS) attack' to safeguard dealing with online fraudsters.

References

Amaduche, S., Adesanya, B. M. & Adediji, A.M. (2020). The impact of electronic banking on the operations and performance of deposit money banks in Nigeria. *International Journal of Operational Research in Management, Social Sciences & Education (IJORMSSE), e-ISSN: 2536-653X, Volume 6 Number 1. https://www.research-gate.net/publication/342883011*

Bakare, S. (2015). Varying Impacts of Electronic Banking on the Banking Industry. *Journal of Internet Banking and Commerce, vol. 20, no. 2 http://www.icommercecentral.com*

Delpy, D. (2018). *Understanding the costs of cybercrime: A report of key findings from the costs of cybercrime working Group.* OGL, ISBN: 978-1-78655-392-8. nationalarchives.gov.uk/doc/open-government-license/version/3

Fianyi, I. D. (2016). Curbing cyber-crime and enhancing e-commerce security with digital forensics. *International Journal of Computer Science Issues (IJCSI), Volume 12, Issue 6, ISSN (Online): 1694-0784. www.IJCSI.org*

Fields, Z. (2018). *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution.* e-book, ISSN: 9781522547648. IGI Global, USA.

Fredrick (2014) Preventing phishing attacks using one time password and user machine identification. *International Journal of Computer Applications, 68*(3), 7-11.

Hamid, A.A., Razak, F.Z.A., Bakar, A.A. & Abdullah, W.S.W. (2016).The effects of perceived usefulness and perceived ease of use on continuance intention to use e-government. Elsevier B.V. Procedia Economics and Finance 35, 644 – 649, doi: 10.1016/S2212-5671(16)00079-4

Hussain, R. (2016). Cyber-crimes and e-banking: An empirical study. Institute of business administration (IBA), Karachi, Pakistan.

Information Resources Management Association (IRMA, 2019). Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and applications. *ISSN: 9781522588986. IGI Global, USA.*

Kabir, M.R., Dovash, R.H., Nafee, S. E. & Saha, S. (2019). Impact of Online Banking Adoption on Bank's Profitability: Evidence from Bangladesh. *European Journal of Business & Management Research (EJBMR) Vol. 4 No. 3. ISSN: 2507-1076 (Online) DOI: 10.24018/EJBMR*

Longe, O. B. & Chiemeke, S. (2008). Cyber crime and criminality in Nigeria - What roles are internet access points in playing? *https://www.researchgate.net/ publication/ 294461326*

Ohwovoriole, O. (2019).Nigeria Losses About ₦127bn to Cybercrime Annually. National Information Technology Development Agency (NITDA); Thisday June 19, 2019 4:16 am; https://www.thisdaylive.com/index.php/2019/06/19

Raghavan, A.R. & Parthiban, L. (2014). *The effect of cybercrime on a Bank's finances.* International Journal of current research and academic review, ISSN: 2347-3215 Volume-2 Number 2 pp.173-178 www.ijcrar.com

Tunmibi, S. & Falayi, E. (2013). IT Security and E- Banking in Nigeria. Research Gate, DOI: 10.15580/GJIICS.2013.3.071613734.https://www.researchgate.net/publication/255969365

Wada, F. & Odulaja, G.O. (2012). Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. African Journal of Computing & ICT Vol 5. No. 1. pp 69-82. ISSN 2006-1781

Worku, G., Tilahun, A. & Tafa, M.A. (2016). The Impact of Electronic Banking on Customers' Satisfaction in Ethiopian Banking Industry (The Case of Customers of Dashen and Wogagen Banks in Gondar City). *Journal of Business & Financial Affairs Vol. 5 No.2 DOI: 10.4172/2167-0234.1000174*

Yedaly, M. & Wright, B. (2016). *Cybercrime and cyber security.* Symantec Worldwide: http://www.symantec.com/ND