International Journal of
Advanced Research in Statistics, Management and Finance
p-ISSN: 2315-8409 | e-ISSN: 2354-1644
IJARSMF
January, 2021
Vol. 8, No. 1

Impact of Cybercrime on Selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT)

[1]Fadairo-Cokers Olumide Adegboyega &
[2]Ibrahim Gerarh Umaru
[1&2]Institute of Governance and Development Studies,
Nasarawa State University, Keffi

Article DOI:
10.48028/iiprds/ijarsmf.v8.i1.12

Keywords:
Cybercrimes, Deposit Money Banks, Automated Teller Machine (ATM), Online

Corresponding Author:
Fadairo-Cokers Olumide Adegboyega

Abstract

Banking activities have become more complex with the introduction of Information and Communication Technology (ICT), which has changed the mode of bank crimes and fraudulent practices. Therefore, this study is to examine the impact of cybercrimes on selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT). The study used structured questionnaires and the population of the study is the staff and management of the selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT). The sample size of the study was determined using population mean or average values with assumed Z corresponding value of 1 percent level of significance to be 2.58 and 0.56 as population standard deviation for a true value of the population mean. The study used the mean of descriptive analysis and Statistical Package for Social Science (SPSS) for the estimation of the mean values of the banking activities indicators which are Automated Teller Machine (ATM) usage by bank customers and online banking transactions by bank customers. the study revealed that cybercrimes have a negative impact on online banking transactions and Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT). The study also found that there is a high level of banking cybercrime activities in the (FCT), banks online protocols against banking cybercrime activities in (FCT) is adequate, fight against banking cybercrimes in the FCT by the related agencies is below expectation, poor financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes and the awareness creation on banking cybercrimes by all the related agencies are adequate. Therefore, the study recommended that there should be more awareness creation on banking cybercrimes by all the related agencies to reduce the rate of online banking transactions and Automated Teller Machine (ATM) cybercrimes in the Federal Capital Territory (FCT).

Background to the Study

Banking activities have become more complex with the introduction of Information and Communication Technology (ICT), which has changed the mode of bank crimes and fraudulent practices. Berney (2008) discovered that customers highly depend on the internet for their banking activities, which has led to an increase in the activities of online banking transactions. Gates and Jacob (2009) and Malphrus (2009) opined that the internet and online banking provides cybercrime with great opportunities to attack bank customers who are not physically present on the internet to confirm their online banking transactions.

According to Greene (2009), the real economic costs are about 150 percent of the actual fraud loss. In Nigeria, despite the banking regulation and regulations by the apex bank, the Central Bank of Nigeria (CBN), the supervisory role and activities of the Nigeria Deposit Insurance Corporation (NDIC) in the financial cyberspace, and the continuous role of the Chartered Institute of Bankers of Nigeria (CIBN), there is still deep concern about cybercrime and other unethical activities in the banking sector. Report from the NDIC (2008) on the examinations and special investigations activities showed that banks were still faced with issues of cybercrime, inaccurate financial reporting, weak board, and management oversight; poor book-keeping practices; declining asset quality, nonperforming insider-related credits, and attendant large provisioning requirements; non-compliance with banking laws, inadequate debt recovery; significant exposure to the capital market through share and margin loans and rules and regulations.

Okpara (2009) revealed that one of the factors that impacted the most on the banking system's performance in Nigeria was fraudulent practices. Since the fraudulence in banks has become an ever-existing problem. According to Akinyomi (2012), the two main sources of cybercrime in Nigeria are the Internet and Automated Teller Machines (ATMs). It is evident from their study that, the internet constitutes the larger channel through which cybercrimes were perpetrated in banks in 2016. On this backdrop, Gartner (2019) predicted that worldwide spending on information security will significantly grow to $124 billion in 2019. And still, spending according to some security researchers estimate that cybercrime costs will quadruple from their figure in 2015 to about $2.1 trillion by end-2019, and outpace expenditure on cyber-security by over 16 times. The vulnerability of this electronic market to criminal activities has therefore been a growing concern. Nigeria's internet penetration since the 21st century had been on the increase. Internet users as a percentage of the population increased significantly from 3.5% in 2005 to 47.4% in 2014 (WDI, 2016). Similarly, teledensity has been forecasted to continuously increase overtime in Nigeria (Asemota, et al, 2015). The proliferation of the internet in Nigeria has indeed come with an unintended consequence, as a haven for criminals. Cybercrime has remained a challenging issue despite increasing awareness and attention to addressing the menace in Nigeria and across the globe. For instance, Cybercrime accounted for about 43% of total monetary loss due to fraud in 2016. As observed by AbdulRaheem, Isiaka, and Muhammed (2012), the degree and incidence of cybercrime in the Nigerian banking industry have been on the increase with obvious implications on bank performance such that it has a negative social impact on the banking sector. At the moment, fraud in the banking industry, as well as its social impact, has been a topical issue not only to the shareholders, and regulatory authorities but also those that have an interest in the industry's performance. Also, Ikpefan (2006), it stems from the fact that cybercrime constitutes a threat to the continued corporate existence of an organization. The growth of bank cybercrimes over the years has constituted a problem. Therefore, this study seeks to examine the impact of cybercrimes on selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT).

Literature Review

Conceptual Review

The definition of cybercrime as a concept has been a major issue with different scholars. However, this study reviewed some definitions by some selected scholars. Cybercrime is seen as computer crime, computer-related crime, digital crime, information technology crime (Maat, 2004) and cybercrime could reasonably include a wide difference in criminal activities. In the 10th conference on Prevention of Crime and Treatment of Offenders, a conference dedicated to the activities on crimes related to computer networks which were carried out by United Nations Congress, cybercrime activity was subdivided into two definitions. Firstly, Cybercrime in a narrow sense of definition is an illegal activity directed by the process of electronic operations that are targeted towards the security of computer systems and the data processed by them. Secondly, cybercrime in a broader sense of definition is an illegal activity done utilizing, or about, a computer system, which includes crimes as illegal possession and offering or distributing information using a computer system (United Nations, 2005).

In another conference by the Council of Europe's Convention which was on cybercrime issues and in this conference, cybercrime was defined as the different kinds of criminal activities including offenses against computer data and systems, computer-related offenses, content offenses, and copyright offences (McQuade, 2006). Also, the conference consists of four main cybercrime activities. First, cybercrime activities relating to the confidentiality, availability, and integrity of computer data and systems which are illegal access, illegal interception, data or system interference, and illegal devices. Second is computer-related offences like computer-related forgery and computer-related fraud. The third is the content-related offences (e.g. child pornography). And, the fourth is the cybercrime activities relating to infringements of copyright and other related rights. A similar definition is the one of Thomas and Loader (2000), who defined cybercrime as those "computer-motivated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".

The Canadian Police College defined cybercrime as a criminal activity involving a computer system as the processor channel of the crime, or the tool used to commit a material component of the offence (Statistics Canada, 2002). Maat (2004), proposed a definition for cybercrime which encompasses all illegal activities where the computer, computer systems, an information network or data is the target of the crime and those known illegal activities or crime that are actively committed through or with the aid of the computer, computer systems, an information network or data. It is significant to note that there is no consistent and statutory definition for cybercrime.

Empirical Review

There are several empirical studies on cybercrime, banking systems, and related literature, but for this study, selected studies on cybercrime and banking system were reviewed; among them is the work of Akinfala (2005) researched job involvement/ experience factors and fraudulent behaviors among serving and convicted bank staff. The study found that job involvement has three factors: motivation, identification, and a feeling of pride that people achieve in their jobs. Nwude (2006) carried out a bank fraud using the methodology of interaction with bank staff of various cadres with a structured questionnaire to identify the fraud forms and characteristics in the banking industry. The study reveals that some staff involved in fraud due to greediness and arrogance.

Adewunmi (2007), in his study on bank crime, identify social and economic lapse in the economy which are the unquestioning attitude of society towards the sources of wealth, misplacement of societal values, the rising economy and citizens expectations from bank staff and the subsequent and the demand for the staff to live up to such expectation, have remained some of the contributory factors for cybercrime. In another study, Otusanya (2008) carried out a study on the role of Bank CEOs in the perpetration of corporate executive frauds in the Nigerian Banking sector. The study found that recent banking crises in Nigeria have exposed bank executives' corruption and fraudulent practices using institutional anomie theory called the American dream theory, and the study revealed that the urge for monetary success has come to dominate society and therefore increase the rate of financial cybercrime.

Idowu (2009) researched the means of minimizing the incidence of fraud in the Nigerian banking industry. The study found that so many factors contributed to the incidence of frauds in banks; amongst them is inadequate working conditions, poor management of policies and procedures, staff feeling frustrated as a result of poor remunerations, and bank staff staying longer on a particular job. In another study carried out by Wole and Couisa (2009) investigated the attributes of the theory of diffusion of innovation empirically. This study used automated teller machines (ATMs) as the target innovation in the banking system. The study revealed that attitudinal dispositions significantly influence ATM's use in any bank, thereby affecting the bank's performance.

In a researched done by Adepoju and Alhassan (2010) believed that bank customers have come to depend on and trust the use of special devices in banking transactions especially, the use of Automatic teller machine (ATM) to meet their banking needs conveniently. Also, there has been a proliferation of ATM frauds in the country. Managing the risks associated with ATM fraud and diminishing its impact is an important issue facing banks as cybercrime techniques have become more advanced with increased occurrences. Akindele (2010) examined the "challenges of Automated Teller Machine (ATM) usage and bank fraud occurrence in Nigeria banking system." The research revealed that the lack of adequate training, communication gap, and poor leadership skills were the greatest causes of banks' fraud. He advised that adequate internal control mechanisms be put in place and that workers' satisfaction, comfort, and other benefits be adequately cared for.

In another study in Nigeria, Onuorah and Ebimobowei (2011) investigated the fraudulent activities and forensic accounting in Nigeria. The research revealed a need for banks in Nigeria to adopt more proactive measures such as forensic accounting procedures in the bank system. The study of Abdulrasheed, Babaitu, and Yinusa (2012) examined the impact of fraud on Nigeria's bank performance. The study results show a significant relationship between banks' profit and the total amount of funds involved in fraud. Also, a study done by Kanu and Okorafor (2013) researched the nature, extent, and economic impact of fraud on bank deposits in Nigeria using descriptive and inference statistics. The study examined a positive significant relationship between bank deposit and fraud in the Nigerian banking industry.

Iyodo, Agbaji, and Abu (2016) examined the consequences of bank fraud on the Nigerian economy's growth. The scope of the study is from 1995 to 2014. The study used secondary data in its analysis. Regression analysis and SPPS application software are being used for data analysis. The study reveals that bank fraud has negative and significant consequences on the growth of the Nigerian economy. Banks' ability to improve economic growth and development in any society is the duty of the extent to which financial activities are carried out with confidence, trust, and least risk. These undoubtedly require a safe and sound banking practice, which many of the banks in Nigeria today have despised to their peril. The study recommends that banks in Nigeria need to improve on their supervision, careful when recruiting employees. Wonderful results alone are not enough, but fear of God and employees' integrity should be considered. The research concluded that the fight for the uncovering, preclusion, and retribution of fraud perpetrators must be tackled to reduce the temptation to commit fraud and increase the chances of detection. While a positive work environment will improve to achieve the former, the latter can be achieved by a sound internal control system.

Theoretical Framework

The study adopted the theory of Technology-Enabled Crime as a theoretical framework and the key nature of the theory is that it consists of several categories of criminological theories to help society better understand why crimes co-evolved with computer and telecommunications technologies to become among the most complex and difficult forms of crime to prevent, investigate and control. McQuade (1998) reveals that understanding and maintaining relatively complex crime is initially quite difficult, and there an unending competition between the perpetrators of criminal activities and law enforcement agencies or bodies for technological gains. As the perpetrators of criminal activities do something new and innovative, law enforcement must catch up to avert, control, deter, and prevent new forms of crime.

McQuade (2006) argues that technology-enabled crime theory consists of the following activities. First, crimes committed directly against computers and computer systems. Second, are activities that fall under this category are often referred to as high tech crime, computer crimes, or cybercrimes. The third is the use of technology to commit or facilitate the commission of traditional crimes. Forth is the crimes such as fraud, scams, and harassment can be facilitated using technology which brings unique challenges to old crimes. The theory provides a framework for understanding all forms of criminality and especially those that are evolving with computing and telecommunications technology inventions and innovations. The theory is pertinent for understanding contemporary threats posed by emerging forms of cybercrime, transnational crime, and terrorism networks that defy traditional methods of criminal justice and security measures for preventing and controlling crime (Chamlin & Cochtan, 2007). The theory is also relevant to this study because it provides us insight into the understanding of the new tools and techniques used by cybercriminals; that is, a shift from the simple crime committed using simple tools to the complex crime committed using complex tools. It also helps in understanding the new forms of deviance, social abuse, or crime committed through the innovative use of technology.

Methodology

Population and Sample Size of the Study

The population of the study is the staff and management of the selected deposit money banks in Federal Capital Territory (FCT). However, because the total number of the population of staff and management of the selected banks were unknown, the study used the mean sampling technique to determine the sample size of the study. Thus, the population mean or average values can be obtained by:

$$n = \frac{Z^2\sigma^2}{e^2}$$

Where Z = the Z-statistic (or value) corresponding to the desired confidence level σ = a pre-determined value of the population standard Deviation e = the maximum acceptable margin of error. Therefore, the study assumed Z corresponding value of 1 percent level of significance to be 2.58 and 0.56 as population standard deviation for a true value of the population mean for the staff and management of selected banks in FCT, Abuja will be within 10 percent of the sample mean (Osuala, 2007). The sample size was calculated as:

$$n = \frac{Z^2\sigma^2}{e^2} = \frac{2.58^2 0.56^2}{0.1^2} = 209$$

Therefore, the sample size of this study is 209. However, the random sampling technique was used to select the banks and the respondents in the selected banks. Table 1 shows the list of selected banks in the FCT with international authorization (Central Bank of Nigeria, 2018).

Table 1: The Selected Deposit Money Banks (DMBs) in Federal Capital Territory (FCT)

S/N	Banks	Respondents	S/N	Banks	Respondents
1	Access Bank Plc	23	6	Guaranty Trust Bank Plc	23
2	Diamond Bank Plc	23	7	Union Bank of Nigeria Plc	23
3	Fidelity Bank Plc	23	8	United Bank of Africa	24
4	First City Monument Bank Plc	23	9	Zenith Bank Plc	24
5	First Bank Nigeria LTD	23	**Total**		**209**

Source: Authors Compilation, 2020

Validation of Research Instrument

The instrument is said to be valid when it measures what it is intended to be measured (Creswell, 2012). To ensure the face and content validity of the items on the instrument measuring the different variables in the study, the questionnaire will be submitted to two experts in educational research and statistics and one expert in test and measurement, to ascertain whether the items measured what they purported to measure. These experts in conjunction with my supervisor certified the instrument as being valid to measure what it set out to measure at least in content and face validity. During this process, their comments and corrections led to changes being affected on the items in the questionnaire in terms of appropriateness and precision of words, sentences, and expressions. Flaws and errors in terms of phraseology, tautology, grammar, and organization of the instrument were identified and the necessary corrections were affected.

Method of Data Analysis

The study used the mean of descriptive analysis. Thus, responses of each subject were coded on the computer coding sheet, and thereafter, entered and processed, using the Statistical Package for Social Science (SPSS), mean and simple percentages were used for analysis and interpretation of the results. The frequency distributions of the various response categories were calculated. To obtain the item and section mean ratings, frequencies were weighed in the following manner: strongly agreed - 4 points, agreed - 3 points, disagreed -2 points, and strongly disagreed -1 point. The mean ratings of the various responses were calculated and were used to answer the research questions. The mean of 1, 2, 3, and 4 is 2.50 for this study; a mean rating of 2.51 or above was regarded as significant while a mean rating less than 2.50 was regarded as insignificant in explaining the changes in the variables under study. The study used the Statistical Package for Social Science (SPSS) for the estimation of the mean values of the banking activities indicators which are Automated Teller Machine (ATM) usage by bank customers and online banking transactions by bank customers.

Data Presentation and Analysis

The results of the data collected are analyzed below based on each research question, out of the 209 questionnaires distributed, 203 questionnaires were well completed and valid for analysis for this study.

Table 2: Frequencies and percentages of sex, position, and year of experience of respondents

Sex distribution of respondents	**Frequency**	**Percentage %**
Male	97	48
Female	106	52
Total	**203**	**100**
Job Position of respondents	**Frequency**	**Percentage %**
Senior Management	24	12
Junior Management	89	44
Senior Officer	47	23
Junior Officer	43	21
Total	**203**	**100**
Years of Experience of respondents	**Frequency**	**Percentage**
1-10	30	15
11-20	65	32
21-30	85	42
31-above	23	11
Total	**203**	**100**

Source: Administered Questionnaire, 2020.

Table 2 shows the percentages of sex, position, and year of experience of respondents. Table 2 shows that 48 percent of the total respondents are males, while 52 percent of the total respondents are females. This implies that there are more female respondents than male respondents. Also, Table 2 shows that 12 percent of the total respondents are senior management staff of the selected banks, 44 percent of the total respondents are junior management staff, 23 percent of the total respondents are senior officers, while 21 percent of the total respondents are the junior staff. Furthermore, Table 2, shows that 15 percent of the total respondents are between 1-10 years of experience, 32 percent of the total respondents are between 11-20 years of working experience, 42 percent of the total respondents are between 21-30 years of working, 11 percent of the total respondents are between 31-above years of working experience. The results show clearly that a larger percent of the respondents is experienced in the banking industry.

Table 3: Frequencies and percentages of issues of cybercrimes and banking activities in FCT

The level of banking cybercrime activities in the FCT .?	**Frequency**	**Percentage**
High	110	54
Moderate	69	34
Low	24	12
Total	**203**	**100**
Banks online protocols against banking cybercrime activities in the FCT is…?	**Frequency**	**Percentage**
Adequate	130	64
Inadequate	73	36
Total	**203**	**100**
The fight against banking cybercrimes in the FCT by the related agencies is .?	**Frequency**	**Percentage**
Below expectation	98	46
Up to expectation	77	38
Not certain	28	16
Total	**203**	**100**
Poor financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes….?	**Frequency**	**percentage**
Agreed	158	78
Disagreed	45	22
Total	**203**	**100**
The awareness creation o f banking cybercrimes by all the related agencies is.?	**Frequency**	**Percentage**
Adequate	098	64
Inadequate	163	36
Total	**203**	**100**

Source: Administered Questionnaire, 2020

Table 3 shows percentages of issues of cybercrimes and banking activities in FCT, 54 percent of the total respondents agreed that there is a high level of banking cybercrime activities in the Federal Capital Territory (FCT), also, 34 percent of the total respondents agreed that there is a moderate level of banking cybercrime activities in the Federal Capital Territory (FCT). While 12 percent of the total respondents agreed that there is a low level of banking cybercrime activities in the Federal Capital Territory (FCT).

Table 3 shows that 64 percent of the total respondents believed that banks online protocols against banking cybercrime activities in the Federal Capital Territory (FCT) are adequate, while 63 percent of the total respondents believed that banks online protocols against banking cybercrime activities in the Federal Capital Territory (FCT) are inadequate. Table 3, 46 percent of the total respondents believed that the fight against banking cybercrimes in the FCT by the related agencies is below expectation, 38 percent of the total respondents believed that the fight against banking cybercrimes in the FCT by the related agencies is up to expectation, while 16 percent of the total respondents are not certain of the fight against banking cybercrimes in the FCT by the related agencies.

Also, Table 3 shows that 78 percent of the total respondents agreed that poor financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes Federal Capital Territory (FCT) while 22 percent of the total respondents disagreed that the poor financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes Federal Capital Territory (FCT). Finally, Table 3 shows that 64 percent of the total respondents believed that the awareness creation on banking cybercrimes by all the related agencies is adequate and 36 percent of the total respondents believed that the awareness creation on banking cybercrimes by all the related agencies is inadequate.

Table 4: The impact of cybercrimes on Automated Teller Machine (ATM) usage by bank customers

Cybercrimes have a negative impact on Automated Teller Machine (ATM)usage by bank customers	**Frequency**	**Percentage %**
Strongly agreed	95	47
Agreed	51	25
Disagreed	30	15
Strongly disagreed	27	13
Total	**203**	**100**

Source: Administered Questionnaire, 2020.

Table 4 shows that 47 percent of the total respondents strongly agreed that cybercrimes have a negative impact on Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT), 25 percent of the total respondents agreed that cybercrimes have a negative impact on Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT), 15 percent of the total respondents disagreed to the fact that cybercrimes have negative impact on Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT) and 7 percent of the total respondents strongly disagreed to the fact that cybercrimes have a negative impact on Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT).

Table 5: Descriptive Statistics results on the impact of cybercrimes on Automated Teller Machine (ATM) usage by bank customers.

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
ATMUBC	203	1.00	4.00	3.0542	1.07262

Note: *The mean of 1, 2, 3 , and 4 is 2.50 for this study; a mean rating of 2.51 or above was regarded as a positive impact while a mean rating of 2.50 and less was regarded as no impact in explaining the changes in the variables under study.*

In Table 5, the mean statistic is 3.05; this implies that cybercrimes have a negative impact on Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT). Since the calculated mean statistic is greater than 2.50, the alternative hypothesis i.e. H_1 is accepted meaning that cybercrimes have a negative impact on

Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT), and $H_0$is rejected meaning that cybercrimes have a negative impact on Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT).

Table 6: The impact of cybercrimes on online banking transactions by bank customers

Cybercrimes have a negative impact on online banking transactions by bank customers	Frequency	Percentage %
Strongly agreed	77	38
Agreed	73	36
Disagreed	28	14
Strongly disagreed	24	12
Total	**203**	**100**

Source: Administered Questionnaire, 2020.

Table 6 shows that 38 percent of the total respondents strongly agreed that cybercrimes have a negative impact on online banking transactions by bank customers in Federal Capital Territory (FCT), 36 percent of the total respondents agreed that cybercrimes have a negative impact on online banking transactions by bank customers in Federal Capital Territory (FCT), 14 percent of the total respondents disagreed to the fact that cybercrimes have a negative impact on online banking transactions by bank customers in Federal Capital Territory (FCT) and 12 percent of the total respondents strongly disagreed to the fact that cybercrimes have no negative impact on online banking transactions by bank customers in Federal Capital Territory (FCT).

Table 7: Descriptive Statistics results in the impact of cybercrimes on online banking transactions by bank customers (OBTBC)

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
OBTBC	203	1.00	4.00	2.9951	1.00739
Note: *The mean of 1, 2, 3 , and 4 is 2.50 for this study; a mean rating of 2.51 or above was regarded as a positive impact while a mean rating of 2.50 and less was regarded as no impact in explaining the changes in the variables under study.*					

Table 7 revealed that the calculated mean statistic is 2.995 which means that cybercrimes have a negative impact on online banking transactions by bank customers in Federal Capital Territory (FCT). Since the calculated mean is greater than 2.50, the alternative i.e. H_1 is accepted meaning that cybercrimes have a negative impact on online banking transactions by bank customers in Federal Capital Territory (FCT), and while the H_0 is rejected meaning that cybercrimes have no negative impact on online banking transactions by bank customers in Federal Capital Territory (FCT).

Conclusion and Recommendations

In conclusion, the study revealed that cybercrimes have a negative impact on online banking transactions and Automated Teller Machine (ATM) usage by bank customers in Federal Capital Territory (FCT). The study also found that there is a high level of banking cybercrime activities in the Federal Capital Territory (FCT), banks online protocols against banking cybercrime activities in the Federal Capital Territory (FCT) is adequate, fight against banking cybercrimes in the FCT by the related agencies is below expectation, poor financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes Federal Capital Territory (FCT) and the awareness creation on banking cybercrimes by all the related agencies are adequate. Therefore, the study recommended the following:

i. There should be more awareness creation on banking cybercrimes by all the related agencies to reduce the rate of online banking transactions and Automated Teller Machine (ATM) cybercrimes in the Federal Capital Territory (FCT).

ii. Various banks should revisit the online protocols against banking cybercrime activities in the Federal Capital Tertiary (FCT) to reduce the rate of online banking transactions and Automated Teller Machine (ATM) cybercrimes in the Federal Capital Territory (FCT).

References

Abdulrasheed, S., Babaitu, D., & Yinusa, G. (2012). Fraud and its implications for bank performance in Nigeria, *International Journal of Asian Social Science*, *2* (4), 35-45.

Adepoju, A. & Alhassan, G. (2010). Challenges of automated teller machine (ATM) usage and fraud occurrence in Nigeria: A case study of selected banks in Minna metropolis, *Journal of Internet Banking and Commerce (JIBC)*, *15*(2), 2-10.

Adewumi, S. (2007). *An ideal ATM implementation in an unsecured environment*, Jos: University of Jos Press, 89-102.

Akinyomi, O.J. (2012). Examination of fraud in the Nigerian banking sector and it's prevention, *Asian Journal of Management Research*, 3 (1), 1-20.

Akindele, R. I. (2011). Fraud as a negative catalyst in the Nigerian banking industry, *Journal of Emerging Trends in Economic and Management Sciences*. 2 (5).

Akinfala, G. (2005). Precipitating factors in fraud and criminal motivation, *International Journal of Bank Marketing*, *10* (3), 232-250.

Central Bank of Nigeria (2018). *List of deposit money banks and financial holding companies operating in Nigeria as of September 30th, 2018,* Accessible: www.cbn.gov.ng, Retrieved December 10th, 2020.

Chamlin, M. B.; Cochtan, J. (2007). An evaluation of the assumptions that underlie institutional anomie theory, *Theoretical Criminology* 11 (1), 39-61.

https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

Idowu, A. (2009). An assessment of frauds and it's management in Nigerian commercial banks, *European Journal of Social Sciences*, 10 (4), 1-20.

Iyodo, B. Y, Agbaji, J. S & Abu, A. S. (2016). Consequences of bank frauds on the growth of the Nigerian economy, *Global Journal of Commerce and Management Perspective*, 5 (4), 19-28.

Kanu, S. I. & Okorafor, E. O.(2013). The nature, extent, and Economic impact of fraud on Bank deposits in Nigeria, *Interdisciplinary Journal of Contemporary Research in Business*, 4 (9), 1-20.

Maat, S. (2004). *Cybercrime: A comparative law analysis (Doctoral thesis*), University of South Africa, Pretoria, South Africa p.239

McQuade, S. (1998). *Towards a theory of technology-enabled crime*, Unpublished manuscript. George Mason University, Fairfax, Virginia.

McQuade, S. (2006). *Understanding and managing cybercrime,* Boston: Allyn & Bacon.

Nwude, C. (2006) Quality and internal control challenges in contemporary Nigeria banking, *Zenith Economic Quarterly, Zenith Bank Plc*, *3* (2), 23-28.

Onuorah, S. & Ebimobowei, D. (2011). Fraudulent activities and forensic accounting services of banks in Port Harcourt, Nigeria, *Asian Journal of Business Management*, *4* (2), 232-251.

Osuala, E. C. (2007). *Introduction to research methodology* (*3rd ed*.), Onitsha: African – First Publishers Ltd.

Otusanya, J. O. (2008). *An investigation of corporate executive fraud by CEOs in the Nigerian banking industry,* A seminar paper presented at the Department of Accounting, Faculty of Business Administration, University of Lagos.

Statistics Canada (2002). Canadian Community Health Survey Cycle 1.2: Mental Health and Well-being. 2002.

Thomas, D. & Loader B (2000). Cybercrime: law enforcement, security, and surveillance in the information age. Routledge, *London, J. Soc. Policy*, 30 (1), 300.

United Nations (2005). *UN recommendations on fighting cybercrime*, http://www.crime-research.org/news/13.05.2005/1225/ 25th November 2013**.**