www.iaajournals.org
ISSN: 2636-7246

Effect of Cybercrime on Nigeria's Online Banking System

Nicholas Attamah
Department of Economics Enugu State University of Science and Technology (ESUT) Enugu, Nigeria.
E-mail: numanick@esut.edu.ng

ABSTRACT

Cybercrime refers to those criminal acts such as identity theft and bank frauds facilitated through the use of the internet. This paper examined the effect of cybercrime on Nigeria's commercial banking system. The paper adopted the library research method as secondary data sourced from articles, journals, periodicals and publications were used. Anchored on the risks society theory, the paper argued that the evolution of Information and Communication Technology has brought about unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and other related cyber crimes. Accordingly, the paper observed that widespread cybercrime has negative impact on online banking system as it results in huge financial losses, threatens profitability, and tarnishes the image of the country on a global scale, which often dissuades foreign investors from investing in the country. Based on this, the paper recommended among others, the need for an Anti-Scan Centre in the geopolitical zones in Nigeria, in alliance with other international anti scam centers, so as to obstruct fund transfer and every other medium used by cybercriminals to perpetrate crime; adding that investors and customers should endeavour to adopt simple security tips such as having updated and original anti-virus software to avoid disclosing personal information to third parties.

Keywords: Cybercrime, Nigeria, Economy, Online Banking, ICT.

INTRODUCTION

Today, we live in an interconnected online world, where most of our daily communications and commercial activities now take place using the Internet [1]. Several people have come to rely on the sheer size technological power and high speed of the internet to seek out large volumes of information, and to communicate with nearly anyone, across the globe [2]. According to the Internet World Statistics report, as at 2000 to 2010, the internet has expanded at an average rate of 444.8% on a global level, and currently an estimated 1.96 billion people are on the internet [3]. In Nigeria, most individuals possess mobile phones with internet access and are registered on social media platforms such as Facebook, twitter, whatsApp, yahoo mail, Google mail and so on. [3], posit that the advent of mobile telephones has caused Nigerian Internet penetration levels to increase from less than 5% in 2002 – 2003, to over 30% by the end of 2012 with the growth poised to continually accelerate. These internet based platforms have provided an array of opportunities for individuals to communicate and network with people of diverse cultures, and also aided local business to grow by providing regional and international markets [4].

However, irrespective of these gains associated with the internet revolution, [5] posits that the rapid growth of digital technology have brought about unimaginable risks both nationally and internationally [6]. Today, many traditional crimes are now being aided or abetted through the use of computers and networks, and wrongdoings previously never imagined has surfaced because of the incredible capacities of the information system. [7] argued that the information technology revolution associated with the internet has brought about two edge functions: one is that, it has contributed positive values to the

world; on the other hand, it has produced a new wave of crime to the world [8].

One sector that is particularly affected by internet crime is online banking. Online banking basically implies an interchange of money, relatively done online or electronically, from one account to another account with the aid of the internet [9]. The introduction of internet banking system is of high significance to the banking system in Nigeria because it has enabled banks to surmount borders, adopt tactical outlook, and come up with several innovations. It has brought about services like online transfer, payment, mobile banking, automated teller machine, electronic fund transfer, point of sale, and electronic cheque, among others [10]. Online banking has also stretched banking hours beyond office hours.

A number of studies on online banking have been carried out in Nigeria. [11] cited in [12], for instance, carried out a study on adoption of online banking where major obstacles included insecurity and inadequate operational facilities, as well as telecommunications facilities and electricity supply. Also, another study showed that online banking is still at the beginning stage in Nigeria, with most banks providing little Internet transactional services. Nevertheless, other studies revealed that there has been a continuous shift from cash as business deals are now being automated [13]. Though online banking has the ability to increase customer loyalty and give banks a competitive advantage as far as market share is concerned, the challenges of insecurity, ineffectiveness of telecommunications services, unstable power supply, cyber crime comprising economic fraudsters, internet frauds and scams, still remain. Online banking security has become a major concern for banks and their customers, as it involves managing the risks around banks that are accessible by means of a subjective computer, or laptop. Although, ICT tools such as user identification, transaction access code (TAC), password electronic token, SMS (short message services) alert, internet bank transfer, and bill payment, comprise the mainstream preventive procedures used to combat cybercrime in the banking sector; the use of these tools has not in any way lessened the rate of online banking crimes [14]. Thus, ongoing research on the impact of cyber crime on online banking is inconclusive, especially in developing economies like Nigeria, and serves as an open ground for more research.

Overview of Online Banking in Nigeria

There is no official definition of online banking however, it involves a service that allows customers to use some form of computer to access account-specific information and possibly conduct transactions from a remote location like home or workplace [15]. Also, online banking affords customers the convenience of carrying out regular banking transactions from the comfort and security of any location from which they wish to transact [16]. The internet is the global presence that connects many computers (banking sectors) and users of the internet, for the benefit of sharing vital information among themselves. Internet technology is one principal medium that has simplified customers satisfaction, but came with security challenges which constitute a major problem for both banks and customers in Nigeria. Almost all banking system now uses a centralized banking application to run its daily operations from the head office, under the supervision and monitoring of the apex bank Central Bank of Nigeria (CBN) across it branches. Banking is now made easy as customers can now carry out transactions using mobile banking application, codes and other after sales services [17].

Shifting to the centralized control of financial management, share of information and customer services in Nigerian banking system has increased the number of computer crime and prospective offenders, making it difficult to trace, detect and prevent these crimes. Cybercrime has not only affected the financial institution in Nigeria, it has also

discouraged foreign investors [18] from investing in Nigeria. Commercial banks in Nigeria lost over NGN 15 billion (US$39 million) in 2018 to cyber-crime and electronic fraud, followed by the loss of customers deposit, recorded to the sum of NGN 1.9 billion on a yearly basis (Ogbonnaya, 2020). As a way of tackling this menace, banks employ the services of cyber experts to help manage their cyber security challenges, build intense firewalls, implement strong authentication control, train bank staff on security measures and improve physical security within the banking facilities. The government has also taken corrective measure by setting up the National cyber security initiative (NCI) in 2013 and Nigeria cybercrime working group (NCWG), which unfortunately could not keep up with the rate of growth cybercrime [19].

The Concept of Cyber Crime

According to [20], cybercrime refers to offences committed against an individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, by using modern telecommunication networks such as internet (chat rooms, e-mails, notice board and groups) and mobile phones. On the other hand, [21] defines cybercrime as crimes committed on the internet or unlawful acts using the computer as either a tool (e.g. fraud, forgery, identity theft, phishing scams, spams, junk e-mails, pornography, online gambling, intellectual property crime, cyber defamation, cyber stalking etcetera) or a targeted victim (e.g. unauthorized access to computers networks, electronic information theft, denial of service attacks, malware, malicious codes, e-mail bombing, data didling, salami attacks, logic bombs, web jacking, internet time theft, Trojan attacks etcetera). Kamini's definition implies that all cybercrimes involve both the computer and the individuals as victims; it depends on which of the two is the main target.

Types of Cyber Crime

The types of cyber crimes that have economic impact either directly or indirectly on the financial system include the following:

Credit Card or ATM Fraud: Credit card or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction or when withdrawing money using ATM card. The hackers can abuse this card by impersonating the credit card holder.

Hacking: In this case, hackers are usually engaged in brainstorming sessions, trying to break security codes for e- commerce, funds point cards and e-marketing product sites.

Spoofing: This refers to a situation in which a person's computer on a network is made to act like another computer, usually one with exceptional access rights, so as to gain access to the other systems on the network.

Phishing: Phishing refers to cloning product and e-commerce web pages in order to dupe unsuspecting users. This is a technologically advanced scam that often uses spontaneous mails to trick people into disclosing their financial and/or personal data. According to [20], phishing is simply a high- tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites [22]. [23], reports that about two million users gave information to spoofed websites resulting in direct losses of $1.2 billion for U.S. banks and card issuers in 2003. Phishing affects every aspect of the internet and is a huge priority for electronic mail service providers; hence, a holistic approach involving collaboration between technology innovation, industry,

government, and user education will help tackle this menace.

Fake Copy-Cat Web Sites: A new trend in on-line fraud is the appearance of fake 'copy-cat' web sites that take advantage of end users that are unfamiliar with the Internet or who do not know the valid web address of the company that they wish to visit. The customer, believing that they are entering credit details in order to purchase goods from the intended company, innocently enters details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud [24].

Electronic Spam Mails: These are unsolicited bulk e-mail to multiple recipients. They can be commercial, political, or religious. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media like instant messaging spam, web search engines, and blogs. A good example is 419 mails or the Nigerian advance fee frauds which was estimated to have cost unsuspecting clientele over five billion dollars in 1996 [25]. The effects of such scams have immense effects with confirmed losses of millions of dollars annually [26].

Theoretical framework

This paper adopted risk society theory propounded by German Sociologist, Ulrich Beck. The theory states that there is a movement away from traditional and industrial society and towards a new modern 'risk society' which is individual, global and self-confrontational (reflexive). [22] cited in [21] defines the risk society as "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself". The nature of modern societies is such that risks multiply with the increasing 'complexities' of societal systems of production, consumption, governance and technological control and as [16] cited in [19] posit, high modernity is characterized by the production and distribution of risks from an increasingly complex techno-scientific system. Consequently, the risk society is one where every citizen is exposed to some degree of technological dangers such as cybercrimes. The positive role of the internet technology revolution on the development of the society cannot be overemphasized, however like every other technological innovation it came with it unintended risks which includes cybercrime.

Effect of Cyber Crime on the Economy

According to [12], commercial banks experience huge financial losses each year which are often kept hidden from the public in order to protect investor and customers from been alarmed by the high level of insecurity or to protect their reputation. For instance, in 2019, the Apex bank (CBN) confirmed that transaction valued at N6.5 trillion was stolen by hackers of commercial banks in Nigeria. Similarly, Nigeria Inter-bank System (NIBSS) states that between 2014 – 2018, commercial banks lost over N12.30 billion to internet fraud in Nigeria [17]. Recent report from African Academic Network on Internet [12] indicates that point of sale (POS) might be susceptible to data breach as a result of its global growth. In 2013, a Trojan POSRAM malware was used to steal payment card information of about 70 million customers belonging to a retail giant, banking with a commercial bank in Nigeria. Such huge losses are not good for the economy of the country, and make one to wonder how banks are able to recover from such. The Economic and Financial Crimes Commission Report [15] places Nigeria as third among the top ten sources of cyber crime in the world with 8 per cent, following after the United States with 65 per cent of cyber-criminal activities and the United Kingdom with 9.9 per cent.

The incidence of cybercrime has also given Nigeria a bad image as one of the most corrupt nations in the world. This tarnished national image affects the

way Nigerians are treated abroad with suspicion and extreme caution as Nigerians are stereotyped to be 419ers. More so, private companies around the world are beginning to take steps geared towards blocking e-mail originating from the country and financial instrument are accepted with extreme caution. Foreign investors are also scared of the country, considering it as risky and unattractive business zone [10].

In the same vein, Identity takeover affects online banking, thereby affecting the economy. This is because new accounts can be taken over by identity thieves, thus raising concerns regarding the safety of financial institutions in Nigeria. Unfortunately, greater access to credit, an abundance of information, faster electronic communications, and intense competition among financial institutions make it easier for perpetrators to steal identities and falsify information. The growth of online banking presents opportunities for perpetrators of cyber crime to embezzle money using wire transfer or account takeover. Sometimes, criminals submit fraudulent online applications for bank loans; interrupt online exchange by engaging in denial of service attacks, and compromising online banking payment systems [8].

[4], equally expressed concern over the cost of application fraud alone, and argued that the situation poses a real and constant threat to profitability and may raise the price of goods and services for consumers. Certain factors however complicate the fight against cyber crime. For instance, Information Technology (IT) professionals have joined in the business of hacking, and unfortunately, technological evolution is not able to keep up pace with the rate of change in cyber laws and principles. Also, the unwillingness by banks to pay extra cost to track cybercriminals coupled with the fact that cybercrimes are very difficult to discover make it hard to combat the menace.

CYBER SECURITY MEASURES

In Nigeria, certain measures have been put in place to combat cybercrime. They include:

i. The Nigeria Criminal Code Act 1990 - The specific provisions relating to cyber crime is section 419 which states that: 'Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years." [8].

ii. The establishment of the Economic and Financial Crime Commission Act, 2004. Some of the major responsibilities of the Commission, according to part 2 of the Act, include: the investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.

iii. Advance Fee Fraud and Related Offences Act 2006: According to Section 23 of the advance fee fraud Act [3]. 'False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.' Economic crime is defined by the Act as " the non-violent criminal and illicit activity committed with the objectives

of earning wealth illegally, either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting, and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labor, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes and prohibited goods." Advance Fee Fraud and Other Fraud Related Offences Act 2006 is currently the only law in Nigeria that deals with internet crime issues, and it only covers the regulation of internet service providers and cybercafés [5].

iv. The signing into law of the cybercrime prohibition act, 2015 (prohibition, prevention, etc) by the Nigeria senate to protect banks from cybercriminal.
v. Conversion of the Nigeria Financial Intelligence Agency (NFIA) into a full-fledge agency, thus empowering them with the power to carry out their role effectively without interference.
vi. Stakeholders from financial sector, National Information Technology Development Agency (NITDA), ICT professionals, law enforcement agency have come together to pilot programs like Computer Emergency Responds Teams (CERT) with the aim of re-orientating customers, banks staff and others.

CONCLUSION/RECOMMENDATION

This paper specifically assessed cyber crime and its effect on the banking institutions in Nigeria. The effect of cybercrime on the economy was examined, while existing measures used in combating cyber crime in the banking industry were reviewed. Nigeria ranks high amongst the cybercrime impacted countries, regrettably, the country's response to lessen cybercrime is still very low due to limited technology and lack of cyber security experts. Consequently, this study supports the suggestion made by [10] on the need to set up an Anti-Scan Centre in the geopolitical zones in Nigeria, in alliance with other international anti scam centers, to obstruct fund transfer and every other medium used by cybercriminals to perpetrate crime. Also, investors and customers should endeavour to protect themselves from cyber criminals by adopting simple security tips such as having updated and original anti-virus software to avoid disclosing personal information to third parties. Similarly, using of very strong password and changing password at intervals, ignoring email requests for financial or person details to unblock accounts will help to prevent security breaches. Lastly, the use of artificial intelligence in combating cybercrime should be widely encouraged in Nigeria.

REFERENCES

1. Agba, P.C. (2002). *International Communication Principles, Concepts and Issues.* In Okunna,C.S. (ed) Techniques of Mass Communication: A Multi-dimensional Approach. Enugu: New Generation Books.
2. Agboola, A. A. (2006). Electronic Payment Systems and Tele-banking Services in Nigeria,*Journal of Internet Banking and Commerce*, 11(3).

http://www.arraydev.com/commerce/jibc
3. Aribake, F. O. (2015). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A conceptual Review. *International Journal of Trade, Economics and Finance*, 6(5).
4. Atherton, M. (2010). Criminals switch attention from cheques and plastic to internet transactions. *The Sunday Times* of March 10, 2010
5. Chiemeke, S. C., Evwiekpaefe, A. & Chete, F. (2006). The Adoption of Internet Banking in Nigeria: An Empirical Investigation. *Journal of Internet Banking and Commerce*, 11(3).
6. Ewelukwa, N. (2011). *This Day Newspaper, Nigeria,* March 31,.2011
7. EFCC/ NBS/ (2010). Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria. Summary Report.
8. Halder, D. & Jaishankar, K. (2011). Cybercrime and the Victimization of Women: Laws, Rights, and Regulation. Hershey, PA, USA: IGI Global.
9. Internet World Statistics, (2018).www.internetworldstats.com," InternetWorldStats, 5 November
10. Jackson, T.C.B., Jack, & Robert, W. E. (2016). Cybercrime and the Challenges of Socio-Economic Development in Nigeria. JORIND 14(2) . www.transcampus.org/journal; www.ajol.info/journals/jorind
11. Kamini, D. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences* , 3(1), 240-259.
12. Katsikas, S. K. (2000). Health care management and information system security: awareness, training or education? *International Journal of Medical Informatics*, 60(2); 129-135
13. Liao, Z. & Wong W. K. (2008). The Determinants of Customer Interactions with Internet-Enabled e-Banking Services. *The Journal of the Operational Research Society*, 59(9), 1201-1210.
14. Litan, A. (2004). Phishing attack victims likely targets for identity theft. Available: http://www.gartner.com/DisplayDocumen t?doc_cd=120804
15. Loftness, S. (2004). Responding to "Phishing" Attacks. *Glenbrook Partners.*
16. Longe, O. B. & Longe, F. A. (2005). The Nigerian Web Content: Combating the Pornographic Malaise Using Web Filters. *Journal of Information Technology Impact*, 5(2).
17. Ogbonnaya, M. (2020). Cybercrime in Nigeria demands public-private action. Senior Research Consultant, ISS Pretoria.
18. Ogunlere, S. (2013). Impact of Cyber Crime on Nigeria Economy. *ResearchGate,* 2, 12.
19. Ogunwale, H. (2020). The Impact of Cybercrime on Nigeria's Commercial Banking System. *Research Gate*. https://www.researchgate.net/publication/347388290
20. Onuora, A. C., Uche, D. C., Ogbunude, F. O. & Uwazuruike, F. O. (2017). The Challenges of Cybercrime in Nigeria: An Overview. *AIPFU Journal of School of Sciences,* 1(2), 6-11.
21. Roger, E. S. (2008). Rogers Communications Inc, 2008 Annual ReportAPWG (Anti-Phishing Working Group) . Phishing Activity Trends Report. Available: http://www.antiphishing.org
22. Sesan, G., Soremi, B. & Oluwafemi, B. (2013). Economic Cost of Cybercrime in Nigeria. Cyber Steward Network Project of the Citizen Lab; University of Toronto.
23. Shehu, A.Y. (2014). Emerging Issues in Cyber-Crime: Causes, Implications and Effects for

theLegal Profession. *Online Journal of Social Sciences Research,* 3(7), 169-180.

24. Smith, R.G., Holmes, M. N. & Kaufmann, P. (1999). Nigerian advance fee fraud. Trends and Issues in Crime and Criminal Justice, No. 121. Australian Institute of Criminology, Canberra. Available online at: http://www.aic.gov.au
25. Wada, F. & Odulaja, G. O. (2012). Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation. *African Journal of Computing & ICT,* 4(3), 69-82.
26. World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm