

E-Banking and Security Challenges in Nigeria: Option for the Banking Sector

Adamgbo Suka L. C, Joel L. Augustine, Zukbee Sirah, Ikole Dornubari

Department of Banking and Finance, Rivers State Polytechnic, Bori, Rivers State, Nigeria

*Corresponding Author

Adamgbo Suka L. C

Email: ludensi@ymail.com

Abstract: Advancements in ICT have reduced the globe to a village where one can reach the world in a click, doing business across international boundaries and making profit beyond imaginations. Yet, in comparison to the developed world, the developing economies are yet to fully embrace the possibilities provided by the internet through electronic banking. This study has examined e-banking and security challenges in relation to the development of the banking sector in Nigeria. The study found out among other things that technological solutions are not enough for the security challenges facing e-banking in Nigeria. The study therefore made suggestions in that light.

Keywords: E-banking; Security; Challenges; Banking sector; Nigeria

INTRODUCTION

Technology has permeated all spheres of life with business not being exception. Technology has brought new possibilities for the businesses of all sizes and formations. The internet has become one of the major channels of communication and has been adopted by the financial institutions all over the world. Though some developing economies like Nigeria are still having challenges in fully and effectively utilizing the internet in the banking sector, the internet is yet the rave of the moment as its use have engulfed the system and attracted the attention of the consumers of banking services through its provision of easy access to banking services.

Laukkanen [1] asserted that the internet is one of the most widely used communication channels ever. Advancements in ICT has reduced the globe to a village where one can reach the world in a twinkle, yet, compared to the developed world, the developing economies are yet to fully embrace the possibilities provided by the electronic banking [2, 3].

Notwithstanding the possibilities and opportunities provided by the internet and electronic banking, it has been observed that some factors are still limiting Nigeria and some other developing economies from making effective use of it. Some of these factors as identified by researchers include: fear and distrust [4]; security, website content and privacy issues [5-8]; lack of adequate infrastructure and government policies [9-13]. Seeing many research findings pointing at security challenges as one of the limiting factors to the full utilization of electronic banking in the developing economy, it becomes very important to take a closer

look at security challenges as it has to do with electronic banking in Nigeria.

The e-banking was introduced in order to give more satisfaction to customers by making transaction easier. Yet many complains still arise and sometimes persist over the e-channels, major of which hinges on security. This makes one wonder how much of an option the e-banking is for the development of the banking sector in a developing economy like Nigeria. They have been distress on the banks over the years [14] but the present security challenges that affect the effectiveness of e-banking comes in another shape. The previous distress as identified by CBN faced by the banks were either internal or external, but the security challenges faced by the banks and their customers as a result of the introduction of the e-banking are both internal and external [15]. The e-banking need a great deal of security for it to be effective and attractive to the consumers. According to Pan and Zinkhan [16] and Hofstede [17], for the e-banking to be secured the parties involved in the transaction or a third party should not have the ability to alter information concerning the other party; operators should make use of cryptology, digital signatures by customers; employ the use of Secure Sockets Layer; Secure Electronic Transactions can also be used to for payments via Visa and Master Card.

According to Ogulowore and Oladele [18], Nigeria has been ranked third highest in internet frauds, and this according to him owes to corruption and its tolerance among public and government agencies, weakness of government institutions like the legislature and the judiciary in making and enforcing laws against

crime and corruption; unemployment; the ever widening stratification between the rich and poor etc. These according to the report of Ogunlowore and Oladele which confirms that of Aminu, 2013 are the reasons why it is still difficult for customers to fully embrace the e-banking services in Nigeria.

It is on this note that this study on E-Banking and Security Challenges in Nigeria: Option for the Banking Sector, shall therefore examine e-banking and security challenges in relation to the development of the banking sector in Nigeria. Its specific objectives are as follows:

1. To examine the concept of e-banking;
2. To find out the success so far of e-banking in Nigeria;
3. To identify the security challenges facing effective implementation of electronic banking system in Nigeria;
4. To suggest possible solutions to the identified security challenges of electronic banking in Nigeria.

To achieve the above objectives, answers to the following research questions shall be sought.

1. What is e-banking?
2. What are the successes so far of e-banking in Nigeria?
3. What are the security challenges facing effective implementation of electronic banking system in Nigeria?
4. What are the possible solutions to the identified security challenges of electronic banking in Nigeria?

CONCEPTUAL FRAMEWORK

E-banking

There have been many different understandings and thus many definitions of the term e-banking. The term is a complex one and mostly defined by context and from the standpoint of the e-channel that is common to the user who intends a definition [19, 20]. Auta [20] agreed that e-banking have not replaced the conventional banking services, but refined it in such a way that services are delivered to the customers directly through interactive e-channels automatically.

According to Furst *et al* [19], e-banking is the employment of a remote delivery channel in performing banking services. Furst did not care to highlight whether the e-banking services is an attempt to quash conventional banking or not. Other assertions abound that doesn't see the e-banking as just one means of making the conventional banking services better for the customers consumption [21-23].

Simpson [24] defined e-banking based on physical characteristics. According to him e-banking has to do with electronic banking services where the customers don't have to go to any particular geographically located building.

Nevertheless and worthy of note, is that the commonly used definition which as well shall be adopted in this discourse is the definition offered by an earlier dated research. The report from the Basel Committee on Banking Supervision [25] defined e-banking as "the provision of retail and small value banking products and services through electronic channels".

The definition by the Basel Committee throws much light on the e-banking as it is commonly observed and used in Nigeria. The acceptance of e-banking in Nigeria is still much limited and therefore has a lot to do with retail and small value banking products [26-30]. Therefore, looking at the security challenges of e-banking will be based on this level of e-banking as defined by the Basel Committee.

Cyber Space

Ibikunle and Eweniyi [31] see cyber space as simply the boundless space known as the internet. It has to do with the unlimited connection of the computers through which information and communication is exchanged globally. This has gone deeper into the transformation of our lifestyle, even in how we do business which the e-banking is the issue of concern in this discourse.

Cyber Crime

This is the series of organized crime attacking both cyber space and cyber security [31]. It involves committing crime against computer systems or the use of the computer in committing crimes [32]. But Laura [33] was more comprehensive in the definition of cyber crime as a criminal activity which uses the information technology infrastructure to gain illegal access, illegal interpretation, data and systems interference, misuse of devices and electronic fraud. All the variables as mentioned by Laura [33] in the definition of cyber crime has much to do with the processes of e-banking, which implies that cyber crime therefore have a lot to do with e-banking.

Cyber Security

The definition of cyber security becomes so sophisticated by the fact that on a daily basis, new dimensions of cyber crime emerge and therefore, calls for new measures in securing the cyber space, which consequently affects the definitions previously made [34-36].

Ibikunle and Eweniyi [31] argue that Cyber-security is just the body of rules put in place for the protection of the cyber space. Yet Schaeffer *et al* being more comprehensive defined cyber security as the body of technology, processes and practices made to protect networks, computers, programmes and data from attacks, damage or unauthorized access. Chaum [37] defined 'security' (in e-banking context) as simply the protection of interest. According to him, people desire that their money be protected and therefore they use the banks.

According to Marinela and Liana [38], the major risks in e-banking are operational, strategic and reputational and security is the major operational risk. But Sokolov [39] argued that an e-banking challenge such as breach of security cut across all the risk categories. For instance, if an unauthorized access to a customer's information is allowed, it is commonly classified as operational risk, but it exposes the bank to legal risk as they will have to answer the questions of how such access was allowed. And by the time the bank is taken to the court, their reputation is in question as customers will begin to doubt the safety of their money in the bank due to such compromise.

In all the definitions, one common factor is the process of trying to protect from unauthorized activities. Therefore, Chaum opined that the government has the responsibility of ensuring that the whole system's integrity is maintained to ensure confidence in the customers. So the government in addition to the commercial banks, should work together to ensure that the system's security is ensured.

E-BANKING IN NIGERIA

It could be said that e-banking came as a reaction to the Structural Adjustment Programme (SAP) of the Babangida administration in 1986. SAP brought an adjustment to the entire Nigerian economy with the banks at the fore front. This programme increased the number of banks from 40 in 1985 to 125 in 1991 [40]. It brought competition to the banks and therefore, to win in the competition one needed to employ every means available. The Societe General Bank started with the Automated Teller Machine in 1990 leading others into the competition by using e-banking.

The Automated Payment Systems in which the major channel is the Automated Teller Machine (ATM) is the first e-banking service brought into Nigeria through the Societe General Bank [41, 42]. The nature of service through the ATM is such that it became very easily and widely accepted through Nigeria. The 24 hours 7days service delivery have made bank customers relax from the rush of getting to the bank before 4pm closing hours. A situation where one can get stranded

on the road for shortage of cash has become much reduced since you can carry your ATM card even while travelling and you can always locate the machines when needed. This has boosted the banking services in Nigeria such that the banks are even making it compulsory to use ATM for transactions within specified amounts.

Apart from the ATM, some other electronic banking services have been introduced into the Nigerian banking system with their attendant level of acceptance. Such other channels include the electronic cards (credit and debit cards), automated delivery channels (online banking and internet banking), telephone banking, image machine and banker automated clearing system (Magnetic Ink Character Recognition) [40].

There have been several research reports on the success of e-banking in Nigeria. Chiemeke et al [27] reported that that the e-banking in Nigeria is just at the interactional level. According to them internet banking in Nigeria serves as means of interaction between the banks and their customers with little transactions.

Using the Extended Technology Acceptance Model, Ayo et al [43] who investigated how much trust have helped in the acceptance and implementation of e-banking in Nigeria argued in confirmation of Ovia [21] that e-banking is increasingly being adopted in Nigeria.

Auta [20] came out with reason why e-banking is still at the basic level of acceptance and use. He offered that the Nigeria bank customers are lacking in knowledge about e-banking. This has been confirmed by many other research reports [29, 30, 44, 45].

GUIDELINES ON ELECTRONIC BANKING IN NIGERIA

In a bid to make electronic banking safe and secure for both the customers and banks, the CBN, being the apex and regulatory bank in Nigeria, have made policy guidelines for e-banking in Nigeria that must be followed by banks operating in Nigeria. The guidelines cover Technology and Security Standards, Monetary Policy, Legal Issues and Regulatory and Supervisory Issues.

The Technology and Security Standards which banks must follow is the concern of this study. This standards are executed and monitored by the CBN as outlined under the following technology and security areas: computer networks and internet, protocols, applications and system software, delivery channels (mobile telephony, ATM, internet banking POS, international card schemes, electronic bill presentments, ISPs, card schemes, electronic funds transfer), standards on security and privacy which covers security and

privacy policies of banks, identification, access control, security log, recovery and business continuity and vendors outsourcing [46]. The question becomes, with all these guidelines put in place by the CBN, why are there security challenges still encountered by customers and banks as well in the processes of e-banking?

SECURITY CHALLENGES AND E-BANKING IN NIGERIA

The internet is sometimes described as a two edged sword, bringing good and bad together. The activities of fraudsters have made the internet a danger zone for many who never trust that one can carry out any activity on the internet without interference from the fraudsters. Such is the nature of cyber space in Nigeria.

Akogwu [47] opined that crime through the internet in Nigeria occur mostly because most of the internet users in Nigeria are lacking in much of the knowledge on how to protect themselves from such crime, since all they know is just how to access the information they need or carry out their transaction.

Folashade and Abinbola [48] asserted that the cyber criminals in Nigeria who are popularly known as “yahoo yahoo boys” take advantage of e-commerce (e-banking) system which uses the internet, as a means of defrauding people of their resources.

An EFCC publication – Zero Tolerance [49] reported a cyber crime involving a retired civil servant who with two other accomplices defrauded a foreign citizen of the sum of USD 1, 714,080 through the internet. Aminu [50] reported that users of e-banking channels in Nigeria have lost several millions of naira to fraudsters.

These situations has laid an impediment to the adoption of e-banking in Nigeria as reported by Master Card [51], consumers are sometimes fooled by website designers who design sites that look like a legitimate vending sites. This makes consumers give up their personal as well as card details which are used by these fraudsters to defraud them of huge sums of money.

Generally, the security challenges to e-banking have been identified by many research reports to come in the form of phishing, reputational loss or damage, insider abuse, vulnerable IT infrastructure, identity management system [50, 52, 53]. And Ibikunle and Eweniyi [31] in confirmation of Thompson [54] had identified emerging cyber tricks in Nigeria as including: beneficiary of a will scam, online charity, next of kin scam, the “winning ticket in lottery you never entered” scam, bogus cashier’s check, computer/internet service time theft, and lottery scam.

Most of these activities become possible for the fraudsters because of the use of e-banking facilities where their physical identity cannot be easily obtained. They therefore use the e-banking facilities to defraud users of same facilities which have made customers skeptical about who to talk to in situations of difficult in the e-banking process. The worst is that sometimes there is an insider facilitating the process for the fraudsters [50, 52, 53]. This situation has therefore limited the full adoption and implementation of the e-banking services in Nigeria as customers are still very skeptical about which service and from who to trust. The question therefore becomes, is e-banking really an option for the Nigerian banking sector, looking at the security situation?

TOWARDS A MORE SECURED E-BANKING IN NIGERIA

Policies have been made and standards laid out to govern the secured operations transactions through e-banking in Nigeria, yet security challenges and fraudulent activities are still reported or experience almost on a daily basis. This points out that there are issues that need to be tackled which goes beyond policy making and standard dictations, which have not be handled or not well handled.

According to Ibikunle and Eweniyi [31] security challenges to e-banking come as a result of issues such as international barriers to law enforcement, unemployment rate in Nigeria, poverty, corruption, lack of standard implementation, lack of communication infrastructure for the law enforcement agents, lack of national functional databases, proliferation of cybercafés, and porous nature of the internet. According to him, tackling the above mentioned issues will head us towards a more secured e-banking among other internet challenges.

Edwin [55] confirming Adesina and Ayo [12] opined that for the e-banking services to really work in Nigeria, that the power and Telecommunication challenges must be solved. A situation where one buys a computer and connects it to the internet to do his transaction, only for him to experience power surge through the power fluctuations and the gadgets or destroyed. When such doesn’t happen, it will be the poor network coverage of the telecommunication companies that will make customers spend hours in transactions that is meant to be for minutes. Considering how precious time is, customers will want this issue corrected or prefer the traditional banking practices of bricks and walls.

Edwin [55] went further by confirming a World Bank Report [56] of the poverty level of

Nigerian citizens as well as the high cost of commodities in the country including computers and communication accessories. Therefore, the point is that the level of poverty has to be reduced and the costs of ICT gadgets reduced or subsidized to enable Nigerians have access to it. This is because some of the incidences of lost of identity through e-banking happen through the use of public facilities like in the cyber cafes where one doesn't have control over the networking.

Adewuyi [40] identified customer/staff alienation and job cut as an area that need to be handled by banks and stakeholders of e-banking to make the future of e-banking in Nigeria more secured and consequently promote its adoption to help develop the nation's economy. The argument here is that the banks should train their staff on IT to enable them serve their customers well. This will enable the staff know the positive use of the internet and therefore how to avoid fraudulent activities occurring on a customer's account through a transaction supervised by the staff. Also laying off staff without reintegration may push the staff into fraudulent activities in the bid to survive.

There are research reports on the way forward for e-banking in Nigeria who focused more on fortifying the e-banking systems with more sophisticated facilities and software [57-59]. But the take of this discourse is on the human resources than the material resources. This is owing to the fact that any technological invention made has always been toppled by new ones and security codes have always been broken. It therefore holds that cyber crime generally can only be minimized if the reason for engaging in it as pointed in studies above is tackled.

CONCLUSION

Having seen the exploits that could be done by the aid of the internet, the cyberspace has hitherto been occupied with various activities among which e-banking is one of the major. Yet in Nigeria, the full acceptance and use of e-banking services is still in doubt because of security challenges which have made many who ventured into it lose large sums of money to fraudsters. This study have identified that the Nigerian economy could develop further than it have if the full implementation of e-banking services is affected. This is due to the efficiency that could be achieved in entrepreneurship by the use of e-banking as the study have identified speed, ease of access and comfort in transaction which e-banking have brought to customers. But all of these value added services are threatened by security challenges in Nigeria.

Therefore, the study has considered the concepts of e-banking; investigated the success so far of e-banking in Nigeria; identified the security challenges

facing effective implementation of electronic banking system in Nigeria; and have discovered that major among the security challenges doesn't originate from the banking sector. The studies have discovered that corruption, poverty and unemployment are the major reasons why young person's engage in fraudulent activities.

It is true as many studies have suggested that some security measures could be taken technologically to stop or minimize these security challenges. But this study have discovered that such security measures will be short-lived as they will still be toppled by the innovativeness of these young people who see this as their own means of survival and therefore can do anything to brake codes, shutdown systems, write programmes that will help them achieve their ambition. It therefore follows to say that to solve this problem; the root causes should be arrested. And this study, haven discovered among other things that poverty, unemployment and corruption are the major causes of the security challenges facing e-banking in Nigeria, suggests that these issues be solved in other to create confidence and trust from the customers towards e-banking services in Nigeria.

RECOMMENDATIONS

It is not to be contended that e-banking have come to stay and its value is in no doubt needed to develop the Nigerian economy. Therefore, this discourse unequivocally recommends that e-banking and its use in the Nigerian banking sector be promoted. But for its use to be adopted by customers, the security challenges must have to be tackled, and to do that, the study makes two phases of recommendations as follows:

Phase 1

1. The Nigerian government in conjunction with stakeholders of the banking sectors should work together to create jobs for the teeming youths. Creating jobs here does not really mean engaging the youths in government establishments as is commonly seen. They can have establishments of their own and employ others. They militants were granted amnesty because we value the oil revenue and were no longer comfortable with their disturbances; therefore the online fraudsters can as well be granted amnesty of their own nature. This could be done by establishing them in what they know how to do. This young people are innovative in ICT and if they could be empowered, they could make positive use of their ability.
2. A general improvement in the standard of living of the average Nigerian citizen should be the focus of the government. This could be achieved if corruption is sincerely tackled by the government

of the federation. To fight corruption, we need to have the spirit of patriotism in every Nigerian. This is because, Nigeria being a pluralistic entity, makes it difficult for one to do a thing for the good of the generality of the nation without remembering the ethnic group he is coming from. Therefore, a general orientation towards the spirit of patriotism should be adopted.

Phase 2

If the above recommendations are settled, then the educational, legislative and technological approach to tackling the security challenges could be followed thus:

3. The users of the cyber space at various levels should be educated on the security challenges and how to avert them. This could be incorporated in the school curriculum for the future of the Nigerian economy.
4. Information dissemination on timely basis of new trends in cybercrime and measures taken to avert them should be effected over the federation, and to users of the cyber space.
5. The government should make and implement laws on cyber crime, considering the nature and trends of cyber crimes in order to make laws that agree and work with international treaties and conventions on cyber crimes.
6. These laws can only work if the security agencies are empowered and informed on the new trends of cybercrime and therefore trained on cyber security. This is because you cannot prosecute the criminals until they are apprehended.

REFERENCES

1. Laukkanen T; Internet versus Mobile Banking: Comparing Consumer Value Perceptions. *Business Process Management Journal*, 2007; 13(6): 788-797.
2. Akinci S, Aksoy S, Atilgan E; Adoption of Internet Banking Among Sophisticated Consumer Segments in an Advanced Developing Country. *International Journal of Bank Marketing*, 2004; 22(3): 212-232.
3. Al-Somali SA, Gholami R, Clegg B; An Investigation into the Acceptance of Online Banking in Saudi Arabia. *Technovation*, 2009; 29: 130-141.
4. Pucihar A; E-marketplace Adoption Success Factors: Opportunities and Challenges in Electronic Business in Developing Countries. Hershey: Idea Group, 2006; 88-117.
5. Al-Khalidi MA, Wallace RS; The Influence of Attitudes on Personal Computer Utilization among Workers: The Case of Saudi Arabia. *Information & Management*, 1999; 36: 185-204.
6. Suganthi B, Balachandran I; Internet Banking Patronage: An Empirical Investigation of Malaysia, *Journal of Internet Banking and Commerce*, 2001; 6(1): 134-145.
7. Almogbil A; Security, Perceptions, and Practices: Challenges Facing Adoption of Online Banking in Saudi. Unpublished Ph.D. Thesis, George Washington University, Washington, 2005.
8. Ndubisi NO; Customers' Perceptions and Intention to Adopt Internet Banking: The Moderation Effect of Computer Self-Efficacy. *AI and Society*, 2007; 21(4): 315-327.
9. Abor J; Technological Innovations and Banking in Ghana: An Evaluation of Customers' Perceptions. *Ife Psychologia*, 2005; 3(1): 170-187.
10. Ezeoha EE; Regulating Internet Banking in Nigeria: Problems and Challenges. Part I *Journal of Internet Banking and Commerce*, 2005; 11(1).
11. Atemnkeng U, Nzongang P; Market Structure and Profitability in the Banking Industry of CFA Countries: The Case of Commercial Banking in Cameroon, 2006, available at www.jsd-africa.com. Accessed 18th October, 2015.
12. Adesina AA, Ayo CK; An Empirical Investigation of the Level of Users' Acceptance of E-banking in Nigeria. *Journal of Internet Banking and Commerce*, 2010; 15(1): 234-245.
13. Lichtenstein S, Williamson K; Understanding Consumer Adoption of Internet Banking: An Interpretive Study in the Australian Banking Context. *Journal of Electronic Commerce Research*, 2006; 7(2): 50-66.
14. CBN; Guidelines and Incentives on Consolidation in the Nigeria Banking Industry. Press release - April 11, 2005 on Banking Sector Consolidation: Special Incentive to Encourage Weaker Banks, 2005.
15. Olowookere S, Popo-ola EA; Accessing E-Banking Based on Resilient Transaction. M.Sc. Thesis, Department of Computer Science, Blekinge Institute of Technology, 2008.
16. Pan Y, Zinkhan G; Two Models of Online Patronage: Why Do Consumers Shop on the Internet? In Gao, Y. (Ed.). *Web systems design and online consumer behavior*. Hershey: Idea Group Publishing, 2005.
17. Hofstede G; *Cultures and Organisations: Software of the Mind*. London: McGraw-Hill, 1991.
18. Ogunlowore AJ, Oladele R; Analysis of Electronic Banking and Customer Satisfaction in Nigeria. *European Journal of Business and Social Sciences*, 2014; 3(3): 14 - 27.
19. Furst K, Lang WW, Nolle DE; Who offers Internet Banking? *Quarterly Journal, Office of the Comptroller of the Currency*, 2000; 19(2): 27-46.

20. Auta EM; E-banking in developing economy: Empirical evidence from Nigeria. *Journal of Applied Quantitative Methods*, 2010; 5(2):212-222.
21. Ovia J; Internet Banking: Practices and Potentials in Nigeria. A paper at the conference organized by the Institute of Chartered Accountants of Nigeria (ICAN), Lagos, 2001.
22. Pyun CS; Internet Banking in the US, Japan and Europe. *Multinational Business Review*, 2002; 73:81.
23. Gonzalez ME; An Alternative Approach in Service Quality: An E-Banking Case Study. *Quality Manage*, 2008; 43.
24. Simpson J; The Impact of the Internet in Banking: Observations and Evidence from Developed and Emerging Markets. *Telematics and Informatics*, 2002; 19: 315-330.
25. Basel Committee Report on Banking Supervision; Risk management for electronic banking and electronic money activities, Switzerland: Bank of International Settlements, 1998.
26. Idowu PA, Alu AO, Adagunodo ER; The Effect of Information Technology on the Growth of the Banking Industry in Nigeria. *The Electronic Journal on Information Systems in Developing Countries*, EJSDC, 2002; 10(2): 1-8.
27. Chiemeké SC, Ewiewkpaefe AE, Chete FO; The Adoption of Internet Banking in Nigeria: An Empirical Investigation. *Scholarlink Research Institute Journals*, 2006; 3(2): 23-40.
28. Agboola AA; Electronic Payment Systems and Telebanking Services in Nigeria. *Journal of Internet Banking and Commerce*, 2006; 11(3): 345-358
29. Maiyaki A, Mokhtar SS; Effects of electronic banking facilities, employment sector and age group on customers' choice of banks in Nigeria, *Journal of Internet Banking and Commerce*, 2010; 15(1): 1-8.
30. Ajah I, Chibueze I; Loan Fraud Detection and IT Based Combat Strategies *Journal of Internet Banking and Commerce*, 2011; 16(2): 237-250.
31. Ibikunle F, Eweniyi O; Approach to Cyber Security Issues in Nigeria: Challenges and Solution. (IJCRSEE) *International Journal of Cognitive Research in science, engineering and education*, 2013; 1(1): 1-11.
32. Aaron JB; Towards a Culture of Cyber Security Research. *Harvard Journal of Law and Technology*, 2008; 22: 230-240.
33. Laura A; Cyber Crime and National Security: The Role of the Penal and Procedural Law. Nigerian Institute of Advanced Legal Studies, 1995. Retrieved from <http://www.nials-nigeria.org/pub/lauraani.pdf>. on 29 October, 2015.
34. Strassmann PA; Cyber Security for the Department Of Defense, 2009. Retrieved November, 8, 2015
- From <http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf>.
35. Olumide OO, Victor FB; E-Crime in Nigeria: Trends, Tricks, and Treatment. *The Pacific Journal of Science and Technology*, 2010; 11(1): 34-45.
36. Roseline OM; Cyber Capacity without Cyber Security: A Case Study Of Nigeria's National Policy for Information Technology (NPFIT). *The Journal Of Philosophy, Science & Law*, 2012; 12(1): 56-68.
37. Chaum D; *Scientific American*, 1992; 137-42
38. Marinela V, Liana AP; Considerations regarding the Security and Protection of E-banking Services Consumers' Interests. *Amfiteatru Economic*, 2010; 12(28): 388-403
39. Sokolov D; E-banking: Risk Management Practices of the Estonian Banks. Working Papers in Economics. School of Economics and Business Administration, Tallinn University of Technology (TUTWPE), 2007; 22(156): 21-37.
40. Adewuyi ID; Electronic Banking in Nigeria: Challenges of the Regulatory Authorities and the Way Forward. *International Journal of Economic Development Research and Investment*, 2011; 2(1): 149-156.
41. Agboola AA; Optimizing the Use of Information and Communication Technology (ICT) in Nigerian Banks. *Journal of Internet Banking and Commerce*, 2002; 13(1): 456-470.
42. Idowu AA; Automated Banking and the Nigerian Economy. Ede: Christatosh Consults, 2005.
43. Ayo CK, Adewoye JO, Oni AA; The State of e-Banking Implementation in Nigeria: A Post-Consolidation Review. *Journal of Emerging Trends in Economics and Management Sciences*, 2010; 1(1):37-45.
44. Adepoju SA, Alhassan M E; Challenges of Automated Teller Machine (ATM) usage and Fraud Occurrences in Nigeria: A case Study of Selected Banks in Minna Metropolis. *Journal of Internal Banking and Commerce*, 2010; 15(2).
45. Olanami OO; Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Journal of Internet Banking and Commerce*, 2010; 15(1): 245-267.
46. CBN; Guidelines on Electronic Banking in Nigeria, 2003. <http://www.cenbank.org/out/publications/bsd/2003/e-banking.pdf>.
47. Akogwu S; An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria (Unpublished B.Sc project). Department of Sociology, Ahmadu Bello University, Zaria, 2012.
48. Folashade BO, Abimbola KA; The Nature, Causes and Consequences of Cyber Crime in Tertiary

- Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, 2013; 3(9): 98-114.
49. Zero Tolerance; Retiree in Trouble over Internet Fraud. Economic and Financial Crime Commission, 2006; 1(2).
50. Aminu SA; Challenges Militating against Adoption of Online Shopping in Retail Industry in Nigeria. Journal of Marketing Management, 2013; 1(1): 23-33
51. Master Card; Online shopping in Asia/Pacific – Patterns, trends and future growth, 2008. Available from www.mastercardworldwide.com. Accessed November 13, 2015.
52. Longe OB, Chiemekwe S; Cyber Crime and Criminality In Nigeria – What Roles Are Internet Access Points In Playing? European Journal Of Social Sciences, 2008; 6(4): 256-264.
53. Adebusi A; The Internet and Emergence of Yahooboys Sub-Culture in Nigeria. International Journal Of Cyber-Criminology, 2008; 2(2): 368-381.
54. Thompson D; Police Powers – Where's the Evidence?. Proceedings of the Australian Computer Abuse Inaugural Conference, 1989.
55. Edwin A; A Qualitative Study of the Problems and Prospects of Online Banking in Developing Economies – Case of Nigeria. Journal of Internet Banking and Commerce, 2012; 17(3): 1-20.
56. World Bank; National Economic Profiles: Nigeria, 2012.
<http://www.worldbank.org/wbsite/external/countries/africaext/ntgeriaextn>. Accessed 26 October, 2015.
57. Ikechukwu G; Enhancing the Performance of Banking Operations through Appropriate Information Technology in Nigeria Banking Industry. Ibadan: Spectrum Books, 2000.
58. Christopher GC, Mike LV, Amy W; A Logit Analysis of Electronic Banking in New Zealand, International Journal of Bank Market, 2006; 24: 360-383.
59. Emeka RN; Improving the Security of the Internet Banking System Using Three-Level Security Implementation. IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), 2014; 4(6): 167-176.