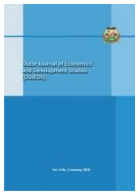
DUTSE JOURNAL OF ECONOMICS AND DEVELOPMENT STUDIES (DUJEDS)
DEPARTMENT OF ECONOMICS AND DEVELOPMENT STUDIES
FEDERAL UNIVERSITY DUTSE
E-Mail: dujeds@fud.edu.ng



ELECTRONIC BANKING IN URBAN DUTSE: ACHIEVEMENTS AND IMPLICATIONS

Ali Ado Siro
Department of Sociology, Criminology and Security Studies Program Federal University Dutse, Jigawa State, Nigeria

Lawan Hamisu Lampo
Department of Sociology, Criminology and Security Studies Program Federal University Dutse, Jigawa State, Nigeria

Abstract
Electronic banking is an emerging issue in Nigerian banking sector. It modernizes the transactions processes and operational procedures in commercial banks. It also makes the banking industry to have accurate, speedy and easy accessible services to everyone. Hence, it contributes to the economic and business development in the country. However, with all these advantages, its adoption created a new way of committing fraud against banks in a Nigerian modern banking industry. This study was conducted in Dutse metropolis, Jigawa State, Nigeria. Thus, the research investigated the benefits of electronic banking among customers of commercial banks in the study area and how such means are utilized to defraud the customers by some fraudsters and or cybercriminals. Being purely quantitative, the sample size of the study is one hundred and forty (140) respondents although only one hundred and twenty-three (123) questionnaires were analyzed due to non-return cases. Respondents were purposively selected. The findings revealed that, modern electronic banking is the easiest and simplest platform that the customers enjoy. On the other hand, it was also revealed that, the most commonly techniques being used by fraudsters in defrauding their victims consist of sending text messages, malicious codes and identity thefts. To combat the problems of electronic fraud in Dutse, both commercial banks, relevant authorities and customers should collaborate to set-free the banking industry from this financial and or economic dilemma that affects the public financial security.

Keywords: Banking, Fraud, Achievements, Technology, Transaction,

Introduction

Initially, banking transaction management and operations were not technology based. This characterized the banking sector as slow and boring in terms of service delivery. Long queues in the banking hall, too much time consuming, poor record keeping and huge cost in providing banking services remained the order of the day. However, the adoption of modern technology in banking industry comes with new dimensions of operations. According to Raghavan and Parthiban (2014), the coming of information technology diversifies banking transactions and make banking operations and processes simpler by ordering, summarizing and customizing the whole process.

Electronic banking simplifies banking transactions by allowing customers to access their account or perform transactions without necessarily being physically at the bank. According to Mia, Rahman, and Uddin (2007), the adoption of information technology in banking transactions has created a new door of opportunities to the banking industries. Oseiwen (2017) added that, the use of information technology in banking transactions gives everyone a chance for easy access to banking activities such

as, retrieving an account balance, electronic money transfers and checking an account history.

According to CBN[1] (2003), technology has created an economical means for banking industries to deliver services to their customers. Hence, it enables customers to access banking services all the times, i.e. 24 hours a day and 7 days in a week. It also enables customers to access banking services from distant places such as homes, offices, shops, etc. John and Rotimi (2014), added that, the adoption of technology in banking industry plays a crucial role by improving commercial banks' service delivery, decongestion of queues in the banking hall, promotion of international payments, tracing personal banking transactions and transfer deposit to a third party. Neff (2014) added that, electronic banking transactions and operations are managed and delivered under some channels such as ATMs[2] , POS[3], internet banking, mobile banking, TV banking, web purchases, tele-banking and PC[4]-banking.

Nevertheless, the adoption of information technology in banking industry, though is a great achievement, but possesses some negative consequences. According to Nwogu and Odoh (2015), the use of information technology instigates many challenges to the banking industry in terms of risk exposure. Siddique and Rehman (2011) added that, information technology is the most powerful technology which is fast, quick and accurate in banking sector, and the massive use of its apparatus such as computers, mobile phones, internet and other associated technologies are the routes which gave rise to various achievement in banking industries and simultaneously instigates means for fraudsters to defraud electronic banking users. The fraudulent techniques include sending messages to the bank and non-bank users requesting them to update their account details, spamming, phishing, denial of service and many more (Nwogu & Odoh 2015).

According to Ezeoha (2005), electronic fraud is the most popular crime currently being committed against commercial banks, and it can be committed through the use of computers, mobile phones, and other internet[5] means. Malphrus (2009) concludes that the electronic banking provides fraudsters with ample opportunities to attack customers who are not physically present at the web to authenticate transaction. It is on this basis that, the current study is directed to unveil the both achievements and implications of electronic banking among the commercial banks' customers in Dutse metropolis within the context of cybercrime analysis.

The adoption of high technology in modern banking industry simplifies almost everything in the sector. It benefits not only the banking sector alone but the business transactions and economic development of Nigeria. The adoption of electronic banking technology shifted the banking operations and transactions from primitive banking era to modern machine era; where customers can enjoy banking services at their own comfort anytime, anywhere. With all its benefits, the adoption of this modern technology paves ways for electronic fraud, in which all the banks, their customers, and the country suffer (Neff, 2014).

Nevertheless, the incessant increase of electronic fraud in banking sector come to necessitate the creation and implementation of various strategies by both government, banking industries and other financial institutions in order to provide security for electronic banking platform. Esan et al (2016) assert that, in 2015, the Nigerian government initiate the Bank Verification Number (BVN) in order to serve as a universal identification among all banks in the country. This was done with the sole aim of reducing the incessant electronic fraud in the banking sector, while for fraudsters BVN is a suitable means to use in defrauding banking users. No doubt, it has been witnessed that message like "Dear customer due to the BVN error your ATM will be de-activated. To re-activate, call this number for more information" (Nwogu & Odoh, 2015:11). Thus, the major concern of this research is to highlight some achievements and implications of electronic banking utilization in Urban Dutse, Jigawa State, Nigeria.

Conceptual Framework and Review of Related Literature

Electronic banking can simply be defined as the use of technological gadgets in order to perform banking transaction and operation without the use of cash or cheque. According to Farooqui and Rajam (2017), electronic banking refers to conducting basic transactions by banks' customers globally via electronic media from their offices or homes with the use of computers, phones, or other technological devices. Driga and Isaac (2014) opine that, the common definition of electronic banking is the one provided by Bassel Committee on Banking Supervision. It was defined as "the provision of retail and small value banking products and services through electronic channels as well large vale electronic payments and other wholesale banking services delivered electronically" (Driga & Isaac, 2014:15).

[1] CBN refers to Central Bank of Nigeria.
[2] ATMs refer to Automated Teller Machines.
[3] POS refers to Point of Sale.
[4] PC refers to Personal Computer
[5] Internet is a short form of international network that connects people for web services throughout the world.

Central Bank of Nigeria's Annual Report defines electronic banking as a means whereby banking businesses are transacted using automated processes and electronic devices such as personal computers, telephones, fax machines, internet, card payments and other electronic channels. Some people adopt electronic banking for information purpose, some for simple transactions such as checking account balances as well as transmission of information, while others facilitate funds transfer and other financial transactions. Many systems involve a combination of these capabilities (CBN, 2003).

Electronic fraud on the other hand is the use of information technology to initiate behavior that can be used to impersonate a particular individual/organization in order to commit crime against others. Chakraborty (2013) defines it as any behavior conducted virtually by one or more persons with the intent to obtain a dishonest advantage over others. Idolor (2013) defined it as the deliberate use of information technology for an act of deception aimed at causing a person or organization to give up money or some vital information. According to Saulawa (2016), electronic fraud is a medium whereby perpetrators traffic emails requesting the addressee to provide them with information or to transfer money from his account to another in form of advance.

Based on the above conceptualizations, it can be concluded that electronic banking and electronic fraud are inter connected with one another. Hence, while electronic banking provides opportunity for simplicity and speed transactions to customers, electronic fraudsters use the same technique to defraud bank users. Sravanthi (2016) observed that customers rely heavily on technology for their banking transactions which increase the number of online transactions. The electronic banking has had many advantages, and, at the same time disadvantages by allowing customers' information to be available on the fore of criminals. This affects the confidence and belief of the banks' customers and in turn pose effects to efficient service delivery of the banking sector.

Siddique and Rehman, (2011) added that technology has generally become a lifeblood in today's banking industry. Meanwhile, the modern banking sector primarily focuses on customer satisfaction. Thus, with these effects, such satisfaction is hampered. Similarly, Oseiwen (2017) added that, customers' satisfaction is part of the business life of any corporate entity. Therefore, in order to provide maximum satisfaction effectively, electronic banking was introduced. Ironically, this creates some sophisticated forms of fraud such as; ATM Fraud, Credit card theft, Phishing, and Identity thefts.

Achievements of Electronic Banking

Electronic banking records various achievements ranging from the bank itself, customers, government, and among business to business (B2B), and business to customers (B2C). Dennis (2013) argued that, from government and business perspective, electronic banking plays a vital role by serving as an intermediate for payments between individuals, organizations or between buyers and sellers. Hassan, Mamman, and Farouk (2013) added that, the adoption of electronic banking changed the distribution channels of the banking sector, particularly in terms of money exchange, and by enabling individuals to pay any goods or services without moving with the money physically and perform it in a jiffy. Elisha (as cited in Hassan, Mamman, and Farouk, 2013) supports by arguing that, electronic banking is convenient and flexible to private businesses and government transactions by enabling speed, efficiency, accessibility in different sector categories.

Electronic Banking as a Process of Electronic Fraud

Electronic banking is a great improvement and development in the modern banking industry. It simplifies transaction processes and enables speedy service delivery. Thus, it is beneficial to commercial banks, customers, government and entrepreneurs in a developing economy like Nigeria. Despite these benefits, electronic banking also paves new ways of committing fraud against banks and their customers in the cyberspace.

According to Yazdanifard, Wanyusouff, and Sade (2011), electronic banking provides opportunities for fraudsters to initiate ways of defrauding bank users by accessing crucial information. The processes of generating such information include but not limited to: phishing, using false web site addresses and names for fraudulent purposes. Also, fake emails or fake websites are sent to customers that look original while in the real sense, they are not. The fraudsters can access customers' information by hijacking the banks' websites thereby asking customers to provide account pin codes, passwords or any other vital information that could only be accessible to either the assigned banker or the customer.

No doubt, electronic banking plays a significant role by enabling various organizations and governments to fulfill official transactions within an eye blink. Conversely, electronic banking serves as a process of electronic fraud. This argument was supported by the works of Gates and Jacob (2009). According to these scholars, fraud is a very real threat to the modern banking payment system

efficiency. This is because, electronic payments give room for fraudsters to deduct some amount from a salary earner/worker who belongs to a public or private organization. Other techniques used by electronic fraudsters include: identity deception, use of malicious codes, sending SMS, data modifications, and use of online shopping platforms to gather information on their potential victims.

Theoretical Perspective

This article employed Routine Activity Theory (RAT) in order to explain how electronic banking becomes an opportunity of electronic fraud to fraudsters. Kenneth (2016) argued that, Routine Activity Theory was initially developed by Cohen and Felson in the late 1970s. While other theories examine the causes of crimes and characteristics of criminals, Routine Activity Theory places much emphasis on how daily activities of people attract the rate of their victimization and what attracts offenders to engage in crime. Argun (2016) added that, Routine Activity Theory was used to explain changes in crime trends over time. Accordingly, it has however been progressively used much more generally to determine, define and prevent crime problems.

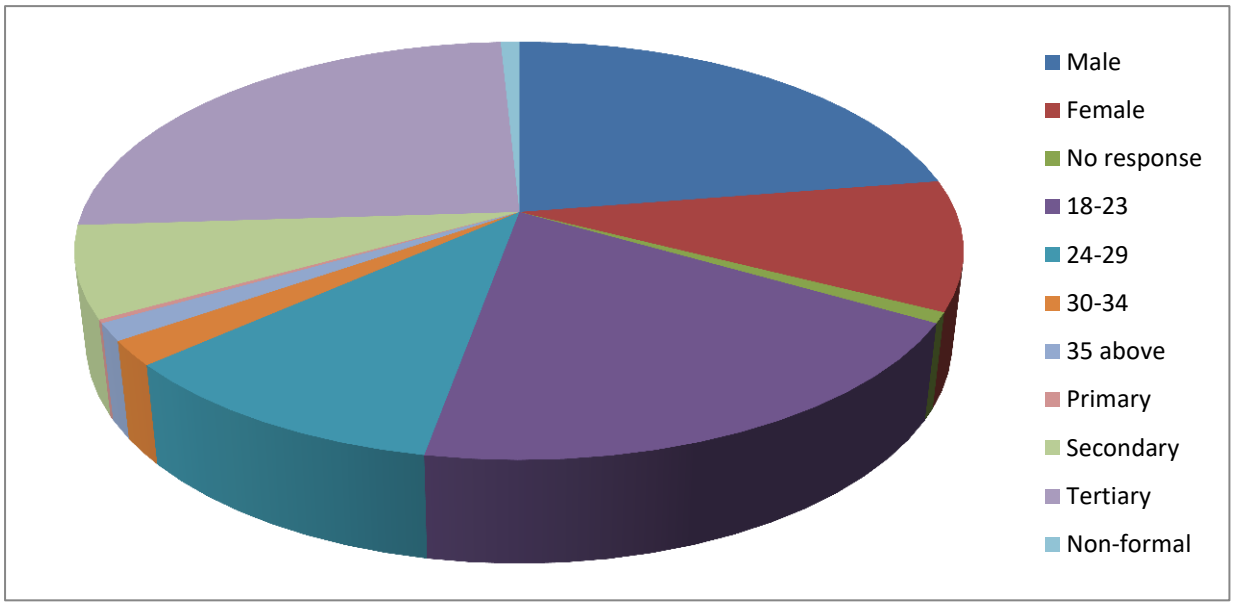
The theory is based on the premise that; crime is an outcome of three basic elements. These consist of: potential offender, suitable target, and absence of a capable guardian. In other words, crime can only occur as a result of contextual linkage of these three elements at one time. Meanwhile, absence or weakening of any element may hamper the occurrence of the crime. Argun (2016) summarized the major propositions of the theory. He argued that, crime can only be committed if a likely offender thinks that a target is suitable, visible and accessible and if, a capable guardian is absent. Daily regular activities of life can put people in a situation that makes them vulnerable to criminal victimization. Thus, Routine Activity Theory can be said to be suitable in explaining the phenomenon of electronic fraud in Dutse metropolis, Jigawa State, Nigeria.

The movement of people from traditional system of banking operations and transactions to the modern technological based operations and transactions plus the changes being experienced in daily public activities of commercial banks and their customers expose the whole to the cybercrime threats. In summary, this opens spacious opportunities to fraudsters in perpetrating financial crimes. Using the three basic elements of Routine Activity Theory, it can simply be argued that, the electronic fraudsters or cyber criminals occupy a potential offender position. The suitable target in electronic banking is the availability and easy accessibility and or vulnerability of customers' information on the web, while the motivated offender (fraudster/cybercriminal) is the one who accesses that bank customers' information and considered them suitable to commit the cybercrime in the absence of a capable guardian and or less possibility of apprehension of the offender by the relevant authorities. Thus, with such coordinates, electronic banking provides a room for perpetual victimization.

Methodology

The research design is survey and is purely quantitative. The study population consist of only banks' officials and banks' customers. The sample size is one hundred and forty (140) respondents. Similarly, the sampling technique is purposive as the researcher used his discretion for selection during the fieldwork. This became necessary as there was no sampling frame available that consist of all the commercial banks' customers. Meanwhile, the customers were not only from a single bank but all the 11 (eleven) banks within the study area. The method of data collection remained the structured interview using questionnaire while the mode of administering the questionnaire consist of both 'self' and 'researcher' administrative approaches. This was necessary as not all the respondents were literate to read, understand and respond to the questions in the questionnaire. Out of the distributed copies of the questionnaire, only 123 were retrieved. The data collected were analyzed using statistical package for social sciences (SPSS version 20). And, they were presented in both pie chart and simple frequency/percentage tables.

Data Presentation and Discussion



Source : **Siro & Lampo, 2018**

Fig. 1: Socio-Demographic Characteristics of the Respondents

From the pie chart above, it shows that, male respondents are the majority compared to their female counterparts in the sample. Males are 83 and females are 37. Seventy-two of the respondents who are the majority are between the ages of 18 and 23, while those over 35 years formed the respondents' minority segment. On educational statuses, majority of the respondents are in tertiary educational level with 93. The minorities are however those with primary school qualification, followed by respondents with non-formal education. And, respondents with secondary school certificates are only 26. The findings indicate that, majority of the respondents are males because they are probably easily accessible than the females. On respondents' age, those between 18-23 years are the majority because they are youth and are the dominant segment of the Nigerian population who are likely to have engaged in banking activities.

Using Routine Activities Theory on socio-demographic characteristics of the respondents, the theory pinpoints that the daily activities and life style of males and females differ. Hence, females' routine activities were domestic centered, while males engage in most tasking struggles of life for their families' survival. Perhaps, that is why males can be found in various places that are exposed to dangers and which make them more vulnerable to fraudsters and or cyber criminals. These places include: markets, shopping malls, banks, etc.

Techniques Used by Electronic Banking Fraudsters

Table. 1 : Common Techniques Used by Fraudsters for Financial Victimisation

Variables	Frequency (Y-N)	Total (Y &N)	Percent (Y-N %)	
Sending Electronic Mail	Y=115 - N=8	123	94-6 =100	
Data Modification	Y= 90 - N=33	123	73-27=100	
Identity Deception	Y= 99 - N=24	123	80-20=100	
Malicious Code	Y=104 - N=19	123	85-15=100	

Source : **Siro & Lampo, 2018**

From the Table above, the symbol ''Y'' stands for "Yes" while ''N'' stands for "No". The findings demonstrate that, 115 respondents represented by 94% indicated that, sending emails is one way through which electronic fraud is being committed in the banking sector. Similarly, 90 responses represented by 73% identified Data Modification as another way of defrauding bank customers. Likewise, 99 responses represented by 80% believed that Identity Deception is another way of electronic banking fraud while 104 respondents represented by 85% had the view that, the use of Malicious Code is one way of defrauding bank customers electronically. From these findings, it could be established that, all the four mentioned techniques are effective in electronic banking

fraud. However, sending mails remained the most common and utilizable in the electronic banking cyber crime

Going by the Routine Activity Theory, sending electronic mails to bank customers as a major technique used by electronic fraudsters is the easiest way through which bank customers are always victimized. This is because; the use of modern technology enables fraudster's access online banking transactions of majority potential victims. In addition, Malicious Code, Identity Deception, and Data Modification were all explicitly explained by the routine activities theory as dominant in the business daily living vis-à-vis modern banking (Kenneth, 2016). Hence, more opportunities are opened to fraudsters such as easy accessibility, target vulnerability as well less possibility of apprehension due to the lack of and or absence of capable guardians (deterrence factors) in the cyberspace.

Table 2: Other Additional Techniques Utilized by Electronic Banking Fraudsters

Response	Frequency	Percent
Requesting BVN Code	42	34
Calling People	35	29
Hacking	19	15
Identity Theft	15	12
Using Internet	12	10
Total	123	100

Source : **Siro & Lampo, 2018**

Table 2 above indicates that, requesting BVN[6] code as agreed by 42 respondents and represented by 34% is the major technique used by electronic fraudsters. This is because, BVN is a strategy initiated by the government in order to reduce the commercial banking fraudulent activities in Nigeria. However, regarding the implementation of BVN, the reverse is the case. This is due to the fact that; fraudsters consider it as a new way to defraud bank customers since majority of the customers are ignorant about why the policy was introduced. Thirty-five respondents represented by 29% identified calling people via mobile phone as a technique of electronic bank fraud. Hacking is the third as believed by 19 respondents as represented by 15% in the sample. The use of identity theft is the fourth among the categories with 15 respondents, and represented by 12%. Lastly, only 12 respondents represented by 10% in the sample believed that, the general internet usage by fraudsters is responsible for electronic banking fraud. Thus, the utilization of technique of requesting BVN maintains the highest position for being additional way which the fraudsters use in defrauding commercial bank customers.

Conclusion and Recommendations

Despite the achievements and records being maintained through the modernization of commercial banking sector in Nigeria, information technology in the country generally brought a lot of challenges to socio-economic relationship between the banks and their respective customers. However, both operations and the overwhelming transaction processes are not free from any evil act, but even make the fraudulent acts speedy, simple and easy accessibility to customers (the potential victims). Meanwhile, there had never been any evil intent from the onset of the creation of electronic banking in the country. But people with criminal intent (*mensrea*) do therefore act (*actus reus*) to cheat the commercial bank customers form both literate and non-literate bank user population. In summary, **''Electronic Fraudsters''** use techniques such as sending email, impersonating bank web site, hacking, use of master code and many more. Thus, it is concluded that, electronic banking in Nigeria is beneficial and achieved a lot prospects in the country. However, it has come with a number of implications detrimental to financial security of the banking population. Therefore, the prevention of electronic banking fraud can be effective as a whole, if both relevant authorities in the country, banking industry and their customers can collaborate in fighting the menace.

Based on the concluded results, the following recommendations are provided to engender policy implementation:

i. More counter technological strategies should be introduced in commercial banking industry to curtail electronic banking fraud from the grassroots.
ii. There should be ways to enlighten bank customers on privacy of their banking details against the accessibility of the third party.
iii. More security personnel are needed to facilitate effective and fraud-free banking services.

[6] BVN is an acronym that stands for: Bank Verification Number. It is a new policy introduced by the current democratic regime to checkmate financial corruption.

References

Argun, U. (2016). Examination of Routine Activities Theory and the Property Crime: Turkish National Police. *International Journal of Human Sciences*. Volume 13, Issue 1, 13-25.

CBN (2003). Report of the Technical Committee on Electronic Banking.

Chakraborty K.C (2013). Financial Inclusion and Banks: Issues and Perspectives.

Driga, I. & Isaac, C. (2014). Electronic Banking Services Features, Challenges, and Benefits. *Annals of the University of Petronas, Economics* 14 (1), 49-58.

Esan A. O. et. al (2016). *Cybercrimes in Nigeria: Analysis, Detection and Prevention*. FUOYE. *Journal of Engineering and Technology*, Vol, 1, Issue,1. 390-401.

Ezeoha A. E. (2005). Regulating Internet Banking in Nigeria: Problems and Challenges, Part 1. Journal of Internet Banking and Commerce, Vol.10, No.3. 45-58.

Farooqui, A. & Rajani, P. (2017). Electronic banking Issues and Challenges. *JOSR Journal of Business and Management* (JOSR-IBM). Volume 19, Issue 10, 19-33.

Gates, T. & Jacob, V. (2009). *Payment Fraud: perception versus reality a conference summary*. Federal Bank of Chicago

Hassan, S.V., Mamman, A. & Farouk, M. A. (2013*).* Electronic Banking Products and Performance of Nigerian listed Deposit Money Banks: Ahmadu Bello University Zaria. *American Journal of Computer Technology and Application*. Vol. 1, No. 10, 29-43.

Idolor, E. J. (2010). Bank Frauds in Nigeria: Underlying Causes, Effects and Possible Remedies. *African International of Accounting, Economics Finance and Banking Research*, Vol. 6, No. 6, 19-34.

John, A. & Rotimi, O. (2014). Analysis of Electronic Banking and Customers Satisfaction in Nigeria. *European Journal of Business and social Sciences*, Vol. 3, No. 3, 14-27.

Kenneth, D. P. (2016). Routine Activities Theory and Research Ethics: A criminological Approach, CSU 2016 –talk. Docx.

Malphrus S. (2009). *Perspective on retail payments fraud*. Federal Reserve Bank of Chicago

Mia, H. A., Rahaman, M. A., & Uddin, M. (2007). Electronic Banking: Evolution, Status, and Prospects. *Journal of The Institute of Cost and Management Accounts of Bangladesh*. Volume XXXV, Number 1. 490-520.

Murat, D. (2011). How The Routine Activity Theory Help Police Understand and Prevent. *Turkish Journal of Police Studies*. Vol.13, No. 1, 14-27.

Neff (2014). Electronic Fraud: Fighting the Battle, Winning the War. *Central Bank of Nigeria Annual Report, 2014*.

Nwogu, E., & Odoh, M. (2015). Security Issues Analysis on Online Banking Implementation in Nigeria. *International Journal of Computer Science and Telecommunication,* Volume 6, Issue 1, 39-55.

Osewon, S.O. (2017). Electronic Banking in Nigeria: Issues and Challenges. *Research Journal of Finance and Accounting.* Vol. 1., No. 1, 200-213.

Raghavan A.R & Parthiban, L. (2014). The effect of Cybercrime on a Banks Finances. *International Journal of Current Research and Academic Review*, Vol. 2., No. 2, 22-43.

Saulawa, M. A. (2016). An Overview of the Legal Framework of Advanced Fee Fraud and Cybercrime in Nigeria. HALREV. Hassanuddin University, Makassar, South Sulawasi, Indonesia, Volume 2, Issue 2, 19-31.

Siddique, M. & Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector: An Overview. *International Journal of Business and Information Technology*. Vol.1, No. 2, 10-21.

Sravanthi, G. (2016). Management of Risk Issues in Banking. Journal of Recent Research Aspects. Vol.3, No. 2, 200-207.

Yazdamfard, R., Yusoff, W. F. & Sade, A. (2011). Electronic Banking Proud: The Need to Enhance Security and Customer Trust In Online Banking. Malaysia. *International Journal in Advances in Information Sciences and Service Sciences*. 10 (61): 505-509.