International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228374

Analysing and Mitigating the Problem of Internet and Credit Card Fraud In Nigeria

Misol Joan Kangkum*, Agbadua Eshiofuezemhe Godsend
Nigerian Communication Satellite Limited (NigComSat), Obasanjo Space Center, Umaru Musa Yar'Adua Express

Article Info
Volume 8, Issue 3
Page Number : 225-235

Publication Issue :
May-June-2022

Article History
Accepted: 10 May 2022
Published: 30 May 2022

ABSTRACT

Internet fraud connotes fraudulent activities committed via the internet. Technological advancement has increased reliance on the internet for communication and business transactions. This reliance has made internet users vulnerable to internet frauds and other forms of cybercrimes. This paper analyses several forms of internet fraud in Nigeria including credit card fraud. It pulled data related to internet fraud from governmental agencies to articulate the menace of internet fraud and the need for drastic mitigating measures. The study further reviews several approaches to detecting and preventing credit card fraud by financial institutions. It also analysed frameworks that have been put into place by the government to mitigate internet fraud generally. It discovered several challenges to the mitigation and prevention of internet fraud in Nigeria and made several contextual recommendations.

Keywords : Commodity Marketing, Business Transactions, Global Interconnectivity and Communication

I. INTRODUCTION

Technological advancement has brought about several innovations and ease of communication. People can now communicate, transfer files and conduct several transactions across borders easily via the internet. The internet which was created for military purposes and to facilitate communication between governmental science research laboratories has now become a tool of global interconnectivity and communication. The internet is now used as a means of communication, commodity marketing, business transactions, and research (1).

Almost 80% of financial transactions today are internet-enabled. The ease, speed and efficiency provided by internet transactions have made it the first choice of users even if the transaction is meant for the next-door neighbour. The internet-enabled business transactions have

provided ease of international business transactions and collaborations (2). A large sum of money can be transferred between partners and customers hitch-free within seconds with the use of a credit card or wire transfer. Aside from that, the use of credit cards reduced the need to transport large sums of money in cash or keep them in residential safes which can be a security threat.

To every innovation, there is always a disadvantage. The popularity of internet transactions through the use of credit cards has made it an easy target for fraudsters. The same technology has increased the rate of cybercrimes. Internet users are now easy targets for fraudsters who use several tricks to siphon their hard-earned money. Although the crime of fraud is not a rare occurrence in Nigerian society, the use of the internet for financial transactions has opened doors to innovative means of perpetrating fraud.

Since financial transactions such as saving and withdrawal of money are done through banks, banks and their customers are the greatest targets of fraudsters (3). Electronic Banking has made bank users vulnerable to internet fraud attacks. According to data, billions are lost every year to fraudulent attacks against banks and their customers, especially through credit card fraud. This loss calls for effective fraud prevention software and measures (4). Even though we can blame the plight of many bank customers who were victims of internet fraud on ignorance of cyber security measures, bank professionals are well equipped with knowledge of cyber security. However, they lack sophisticated technologies to tackle cybercriminal attacks (5).

Based on its duty to safeguard citizens' properties and secure the economy, several measures have been put in place to combat internet fraud by the government. However, several laws and policies made towards combating this menace have been ineffective due to a lack of strict implementation and compliance. (6).

II. ANALYSIS OF INTERNET FRAUD IN NIGERIA

Internet fraud is a form of cybercrime. Cybercrime is any form of crime perpetrated through the internet. Fraud is one of the numerous crimes committed via the internet on a daily basis. Internet fraud is any fraudulent activity perpetrated online. Internet fraud is the deceptive use of internet tools such as websites, email and some other internet components to make false representations of the availability of goods and services to online users with the intent to defraud them. It may also involve unauthorised transmission and access to funds, devices and other valuable items of victims (7). Internet fraud is one of the greatest challenges to business transactions and the global economy. Billions of dollars are lost globally every year to various forms of internet fraud.

Since the introduction of internet banking in Nigeria in 2003, there has been an increase in the use of electronic-based financial services. Internet banking has brought about ease of financial transactions. Customers no longer need to wait for long hours to save and withdraw cash. E-banking also saves the time required to travel down to banks. Not just that, there is an increase in efficiency and service delivery by banks. With the introduction of the cashless policy by the CBN in 2012, a larger number of Nigerian Bank

users now conduct bank transactions through internet banking, USSD codes, Point of Sales (POS) and Automated Teller Machines (ATM) withdrawal & transfer. Nigeria Inter-Bank Settlement System (NIBSS) Plc. confirmed that electronic channels accounted for N54.98tn of bank transactions by Nigerians in the first 2 months of 2022. This amounted to a 44.49% increase, compared to what was obtained in 2021 during the same period (N37.79tn). The electronic channel was used for financial transactions 882.99 million times during the first 2 months of 2022. As of, May 2022, cashless transactions within the first 4 months of 2022 amounted to N117.33tn (8). The volume of transactions that goes on online has made it an attractive target for fraudsters.

Cybercrime in the form of internet fraud has been the greatest challenge for the Nigerian financial sector (9). More than any other institution, banks are more targeted by fraudsters because they deal in safeguarding customers' money (3). Cyber breach of security targeting banks has been on the increase in recent times. Cyber security breaches targeted at banks and their users in Nigeria include phishing, BVN scam, malware attack, cyberstalking, fake websites, credit card theft and banking fraud (10). Cyber terrorism, password sniffing, and Denial of Service attacks are also forms of breach cyber security.

Phishing in simple terms means identity fraud. It is the impersonation of bank staff, business partners and merchant websites to obtain vital bank details. Several frauds have been perpetrated through phishing. Posing as bank staff to ask for customers' BVN, and creating copycat websites to convince the website users to divulge important details are some of the numerous ways through which phishing has been used to perpetrate internet fraud. Cyber terrorism refers to an attack on government or financial institutions to extract information from their system. This can be perpetrated through Distributed Denial of Services attacks (DDOS). Owners of attacked systems are required to pay ransom to recover access to their systems. Malware attack is the infection of computer systems with worms, viruses, Trojan horses and some other malicious software. Password sniffing involves using malicious programs to monitor the network of an organisation. This program listens to all traffic coming into the network. It copies usernames and passwords inputted by unsuspecting users. This information will be filtered by the same programs and important data will be retrieved. Although encryption and password hashing have decreased the incidence of password sniffing many small organisations are still vulnerable to these attacks.

Internet fraud has led to the loss of funds by bankers and customers. Bankers have also suffered several other losses such as damages to reputation, loss of customers and sanctions by industry reputation in some circumstances (6). According to a report published by NIBSS, Nigeria lost #5billion to bank internet fraud from January to September 2020. In a year, Nigeria loses about 14bn on average. Major means of procuring internet fraud according to the report include social engineering which accounted for 56% of the fraudulent activities. Other channels identified included, non-use of two-step factor verification, compromise of pin codes, phone theft, credit card theft and fake assistance.

Figure 1. NIBSS report on techniques of frauds in 2020. Chart available at https://nibss-plc.com.ng/news/4anqsx5p5wbwt7zx8wrrbs8tda

The figure shows the rate of each technique used in perpetrating fraud. Social engineering 56%, credit card theft 6%, phone theft 6%, missing or lost card 1%, fake assistance 5%, lack of 2 step verification 19%, and robbery 2% (12).

Social engineering involves the psychological or emotional manipulation of people to divulge information and surrender their resources. In the case of internet fraud, it involves psychologically manipulating victims into transferring funds and divulging their vital financial details which include account number, BVN number, credit unique CVC code, credit card pin, internet banking password and credit card expiry date. This vital information is used by fraudsters to syphon money from accounts of unsuspecting victims. Social engineering methods used by Internet fraudsters in Nigeria device several means of defrauding their victims which include;

A. ***Online charity and fundraising for NGOs***: Relying on the moral and religious belief in charity, fraudsters set up fake websites to raise funds for non-existent charity organizations and NGOs. In other cases, they may even pretend to be raising funds for a sick person or orphans. Many Nigerians have been emotionally blackmailed into contributing their hard-earned money towards such fake charitable causes.

B. ***Lottery and betting victory:*** This involves sending congratulatory messages to people who have never partaken in lottery competitions or betting that they have won. These imaginary winners are encouraged to send some amount of money before claiming their prize. Even though this sounds ridiculous, some financial opportunists fall for this trick.

C. ***Impersonation of relatives in distress***: This involves pretending to be relatives of the potential victims and asking them to send money because they are currently in distress. They may pretend to be stranded without transport fare or in police custody. Aside from impersonating relatives in distress, another common method is pretending to be a relative in a foreign country. Once they guess the name of a relative abroad and the victims attest to knowing such a relative, they will tell them they are sending them gifts from overseas. Victims will be required to make certain payments to be able to process such gifts sent from overseas.

D. ***Dating scam***: This is also a popular means of internet fraud devised by young men in Nigeria. They pretend to be a lady by using fake pictures to scam foreigners to send them money under the pretence of dating. Next of kin scam is also another fraudulent means.

This entails calling people to come and claim money belonging to a dead relative (13).

E. ***Credit card fraud***: Credit card fraud through phishing is also a very popular means of social engineering. This involves impersonating bank staff and alerting customers about issues with their bank account through phone calls, SMS, emails and social media. They request bank details as a requirement for fixing the issue with their victims' bank accounts.

- CREDIT CARD FRAUD

Electronic Banking has popularised the use of credit cards to withdraw money or make payments for goods and services. Instead of waiting long hours in banking halls, customers can easily withdraw and transfer money with their credit cards through an ATM or transact through their computer devices or mobile phones. Technological advancement and an increase in reliance on virtual transactions have necessitated the use of credit cards for e-commerce. Consumers who purchase goods online and receive a service virtually need to use their cards as a means of payment (14).

Just as internet banking with the use of credit cards has made life easier for banks and their customers, this same innovative means of the transaction has made banks and their users' common targets and victims of fraudsters. Credit card fraud means physical or non-physical possession and use of a credit card without the consent of its legal owner. Credit card fraud may involve the procurement and use of a physical card and pin to withdraw money without the authorisation of its owner. These fraudulent acts can also be perpetrated with counterfeit cards. This is usually called "Card present fraud". While Card present fraud is decreasing in popularity, the attention of fraudsters has now shifted to the "Card not present fraud", since several transactions with the use of credit cards now take place online. "Card not present fraud" refers to unauthorised access to credit card information such as card number, account number, expiry date, CVC code, card pin and billing address. These fraudsters use this information to conduct online transactions or even withdraw the owner's funds. This vital financial information can be obtained through phishing, spoofing and skimming.

Forms of credit card fraud

A. ***Phishing***: Phishing means identity theft, it simply connotes impersonation. However, this term has a broad meaning in relation to internet fraud. Phishing involves fraudulently influencing unsuspecting credit card users to surrender vital bank details. This can range from impersonating bank staff to requests for customers' credit card details. It can also be perpetrated through websites that require membership or service subscriptions. Fraudsters copy the email format of these websites and try to convince users to surrender their credit card details (16).

B. ***Credit detail theft/skimming:*** Phishing of credit card details cannot be regarded as theft since it was willingly surrendered by the owners, although unintentionally. Credit card skimming is the theft of card details through several fraudulent means. A notorious means of obtaining credit card details is by placing a certain electronic device on ATMs to copy credit card information. This method is termed ATM skimming by the US Federal Bureau of Investigation. The electronic device installed on the ATM accesses and copies the credit card

details through the magnetic stripe on the credit card every time a credit card is inserted into the ATM. Fraudsters may also install cameras invisible to users around the ATM boot to record card details and pins (17). Another form of credit card detail theft is extracting card details from websites where credit card transactions take place. Most e-commerce websites or service subscriptions based websites store credit card information. Fraudsters can use malicious software to hack these websites and copy credit card information. Such information is used to access the victim's credit card and to make a purchase on other e-commerce websites.

C. Bank hacking: This involves hacking the systems of banks with flexible security. By gaining access to the bank system, they either access customers' details or transfer money from multiple accounts to their accounts. In most cases, such amounts transferred are ridiculously low to an extent that victims often overlook them as bank charges.

D. *Point of Sale (POS) fraud:* The increased use of POS also exposed users to risks of credit card fraud. Card details can be fraudulently acquired by POS agents. They can use malicious software to manipulate and acquire security information in customers' credit cards. They can later use information obtained such as unique credit card CVV codes and card numbers to make cardless transactions with payment codes. On the other side of the coin, POS agents also experience fraud by customers through fake alerts. Instead of using credit cards, such customers would opt for making bank transfers to the agent. Upon receiving alerts the customers would be issued cash. However, the agents will later notice the alert was fake and not from a bank after the customer would have left (18). At times, POS terminals can also be a victim of hacking and network breach.

Several reasons have been adduced for the increase in vulnerability of credit card users to cyber fraud in Nigeria. Covid 19 pandemic contributed to the surge in credit card fraud in 2020 (12). The global pandemic caused by coronavirus forced the world to stay indoors. As a means of survival and continuation of business transactions, e-commerce gained more popularity. The rapid increase in online transactions due to the pandemic exposed a lot of credit card users and merchants to online fraud, especially cybercrime illiterates. In the case of Nigerians, they were not only stripped of their card information through e-commerce websites, they were gullible enough to disclose this information to fraudsters who pretended to be sharing palliatives. Several people surrendered their bank information to phishers who told them they were disbursing covid 19 relief funds and needed their account details (19).

The major Impediment to the detection and prevention of internet fraud in Nigeria is the low level of awareness of cyber security among electronic banking users. Many lack adequate knowledge of how to perform card and cardless transactions. As such, they seek the aid of third parties such as family members, friends and even passersby. In most cases, this has amounted to voluntarily surrendering their information to fraudsters even though unintentionally (20).

The increase in credit card fraud necessitates means of mitigating such occurrences. Many individuals have lost a huge amount of money and means of livelihood to internet fraudsters. Aside from the financial loss, internet fraud and

other forms of cybercrimes have dented Nigeria's reputation internationally. This has led to a decrease in foreign investment in the Nigerian economy, stigmatisation of Nigerians in the international labour market and restriction of entry of Nigerians into foreign countries. This has also led to low productivity since more human and financial resources are expended on creating awareness and preventing cybercrimes (21).

Efforts of banks towards mitigating internet and credit card fraud in Nigeria

Despite the ease introduced by card electronic banking, internet and credit card fraud has been a major setback. However, these setbacks cannot justify the abandonment of this innovation. Thus, finding an effective solution will be a step in the right direction. Banks have devised several measures towards preventing cyber-attacks and consumer protection. The majority of banks in Nigeria ensure their staff are adequately trained to quickly detect threats of cyber-attacks and respond swiftly to such situations. A major impediment to the prevention of such attacks has been inadequate investment in advanced software. As technology continues to progress, internet fraudsters are gaining more technological power to attack their victims. Victims who in the case of banks and users are ill-equipped to counter such attacks (5). As such, there is a need for more investment in sophisticated technological tools such as artificial intelligence, machine learning, data mining, sequence alignment, fuzzy logic, and genetic programming to swiftly detect and prevent credit card frauds and system attacks (14).

Aside from bank staff, customers are also encouraged to take several safety measures such as a subscription to bank activity alerts. Regularly checking the statement of account, keeping their bank details confidential, putting in place "second-factor authentication" for e-transactions, and saving contact details of their account officers. These preventive pieces of advice are not enough. There is a need for continuous sensitization of bank customers on cyber security. There is a need for massive collaboration toward national cyber security sensitization to enlighten people on several social engineering techniques of credit card fraud and advanced techniques of detecting malicious software. (5)

Efforts of government towards mitigating internet and credit card fraud

As part of the government's mandate to safeguard citizens' property, national economy and positive international reputation, the government has put in place several legal, administrative and technical frameworks for detecting and preventing internet fraud. Although before 2004, several efforts had been made towards combating cybercrime, the Economic and Financial Crimes Commission (EFCC) was established through the enactment of the EFCC Act 2004. The Act empowered the commission to implement its provisions. The duties of the commission are to identify and investigate activities related to economic and financial crimes. The jurisdiction of the commission extends to issues related to credit card fraud, advance fee fraud, money laundering, illegal charge transfer, and contractual scam (22).

As further measures towards mitigating internet fraud, the Nigerian government published the National Internet Safety Strategy for Combating

Cybercrimes in Nigeria in 2014. This strategy was followed by the enactment of Nigeria Cybercrime (Prohibition, Prevention, etc.) Act in May 2015. The Cybercrime Act serves as a legal, institutional and regulatory framework for preventing, prohibiting, detecting, prosecuting and punishment of cybercrimes in Nigeria. It provides measures for investigating and punishing cybercrimes in Nigeria (23). Not just that, it makes provision for mechanisms for preventing cybercrimes, and protection of national infrastructure, data privacy and intellectual property. The Act through its *section 19* makes it the duty of every bank to put in place measures towards safeguarding the sensitive information of customers. Such sensitive information includes personal details, account numbers, statements of account and other information related to a customer's account (24). As such, the law places a burden on customers to prove negligence on the part of banks in safeguarding their information in case of a data breach.

The Cybercrime Act further prohibits and punishes the following acts:

- Issuing Unlawful Electronic Banking Instructions (section 20).
- Unlawfully Obtaining the Identity of a Bank or Financial Institution with Intent to Defraud (section 22).
- Unlawful Disclosure of a Password or Access Code (Section 28).
- Unlawful Use of a Consumer's Security Code by a Service Provider or Vendor of Computer-Based Services (section 29).
- Unlawful Manipulation of ATM Machines and POS Terminals (section 30).
- Phishing Scams and Electronic Card Fraud (section *32).*

It places further place duty on banks to do the following to prevent internet fraud;

- Duty of Banks and Financial Institutions to Report Cyber Threats.
- Duty of Banks and Financial Institutions to Verify Customer Identity before Executing Electronic Banking Transactions.
- Duty of Banks and Financial Institutions to Reverse Unauthorized Withdrawals

Other laws that criminalise cybercrime in Nigeria include Advanced Fee Fraud and Other Fraud Related Offences Act 2006, Money Laundering (Prohibition) Act 2011, Evidence Act 2011, and Criminal code Act 1990.

Technical efforts made by the government include the partnership agreement between Microsoft and EFCC to identify and prosecute cybercriminals. As the first of its kind in Africa, the memorandum of agreement between Nigeria and Microsoft addresses the issue of internet, phishing, virus, spyware, worms, malicious attacks and several other cyber threats. The use of ADNET to store and retrieve information about cybercrimes and criminals is also another positive technical step by the government (25).

Despite measures put in place by the government to combat internet fraud, ineffective means of implementation of law, noncompliance and several loopholes in the laws and regulations made are impediments to the effectiveness of government efforts towards mitigating internet fraud in Nigeria. There are several loopholes in the Nigeria cybercrime Act that created a route of escape for perpetrators. Even for those that are

prosecuted, the punishment is inadequate to serve as enough deterrence to others (6).

Noncompliance to obligations placed on banks and other payment service providers to create adequate cyber security awareness among financial employees and customers, by "The CBN's Risk-Based Cyber security Framework and Guidelines for Deposit Money Banks and Payment Service Providers 2015", is an example of non-compliance. Despite the legal duty of banks, there are still ineffective awareness programs geared toward the fulfilment of this duty (26).

Investigation and arrest of internet fraudsters is also another challenge. The country's cybercrime intelligence and law enforcement agencies lack sophisticated technologies to keep up with internet fraudsters (27). Thus, there is a need to review laws and regulations relating to cybercrime and restrengthening governmental agencies to fully enforce the law. Government should also increase its financial allocation toward combating cybercrimes and educating citizens on cyber security.

III. CONCLUSION

The study has analysed the prevalence of internet and credit card fraud in Nigeria. It found that bank and their customers are easy to target by internet fraudsters. Based on an analysis of data from government agencies, it found that the rate of internet fraud in Nigeria is growing along with the rapid increase in the usage of electronic banking. The major means of perpetrating internet fraud in Nigeria in recent times is social engineering. The study further analysed credit card fraud as a form of internet fraud. It found and analysed several means of procurement of credit card fraud such as phishing, card detail skimming, bank system hacking and point of sale fraud. It found that poverty and ignorance is a major challenges for Nigerian credit card users. The continuous attack on banks by internet fraudsters is not due to a lack of cyber security knowledge and training by bank managers. Rather it is due to a lack of sophisticated technological tools such as advanced software to prevent and counter cyber security breaches. It was confirmed that as technology continues to advance so as the possibility and tools for perpetrating cybercrimes. Internet fraudsters have now graduated from menial scams to using sophisticated technological tools to invade bank systems. Finally, the study looked into several measures towards mitigating internet fraud in Nigeria and the challenges of both government and banks in the detection and mitigation of internet fraud. This study concludes that major challenges in mitigating internet fraud in Nigeria are inadequate knowledge of cyber security among electronic bank users, inadequate investment in sophisticated anti-cybercrime software by banks and ineffective implementation of laws as well as policies by the government.

IV. REFERENCES

[1]. G. Vladimir. 2005. International cooperation in fighting cybercrime.

[2]. O. E Oruç and Ç Tatar. 2017. An investigation of factors that affect internet banking usage based on structural equation modelling. Computers in Human Behavior. 66, 232-235.

[3]. S. Ibrahim. 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory

of Nigerian cybercriminals. International Journal of Law, Crime and Justice. 47, 44-57.

[4]. B.C Amanze and C.G Onukwugha. 2018 Credit Card Fraud Detection System In Nigeria Banks Using Adaptive Data Mining And Intelligent Agents: A Review International Journal of Scientific Technology Research 7,(7).

[5]. W. Victoria Wang, N. Harrison and J. Jeong. Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability

[6]. A.B Hassan, F.D Lass, and J. Makinde. 2012. Cybercrime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology. 2 (7), 626-631

[7]. Australian federal police.

[8]. Nigeria Interbank Settlement System plc Report, April 2022.

[9]. S.A Ojeka, E. Ben - E. Caleb Ben-Caleb, E- O.I Ekpe. 2017. Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. International Review of Management and Marketing. 7 (2), 340-346.

[10]. B.A Omodunbi, P.O. Odiase, O.M Olaniyan, A.O Esan. 2016. Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology. 1(1), 37-42.

[11]. A.B Hassan, F.D Lass, J. Makinde. 2012. Cybercrime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology. 2 (7), 626-631

[12]. Nigeria Interbank Settlement System Report Insight 2020.

[13]. A. Adebusuyi. 2008. The Internet and Emergence of Yahoo boys sub-Culture in Nigeria, International Journal of Cyber-Criminology, 0794-2891, Vol. 2(2) 368-381) (13)

[14]. S Benson, E. Raj, A Annie. 2011. Analysis on credit card fraud detection method. International Conference on Computer, Communication and Electrical Technology (ICCCET), 152-156, 2011)

[15]. F. Wada and G.O dulaja 2014. "Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation, "Afr J Comp &ICT, Vol 4(3).

[16]. B. A. Omodunbi, P. O. Odiase, O. M Olaniyan and A. O. Esan. 2016. FUOYE Journal of Engineering and Technology, Volume 1,(1). FBI 2011. Scam and safety measures.

[17]. Ijeoma OPARA and Harrison Edeh. March 10, 2022. Fraudsters dent Nigeria's multi-billion-naira POS business. International Centre for Investigative Reporting.

[18]. Oludayo Tade. January 31, 2022 "COVID-419': how cybercriminals in Nigeria exploited schemes to help people in need. THE CONVERSATION.

[19]. C.O Ifeanyi. 2015. Overview of electronic banking in Nigeria, International Journal of Multidisciplinary Research and Development (2015)2 (7)340; U Kama and M Adigun, Financial Inclusion in Nigeria: Issues and Challenges, Central Bank of Nigeria Occasional Paper (August 2013) (45)31–33

[20]. O.I Okon. ASSESSMENT OF NATIONAL INTERNET SAFETY STRATEGY IN COMBATING CYBERCRIME IN NIGERIA. World Atlas Journal of Library and Information Science, 4(1)

[21]. Economic and Financial Crimes Commission (Establishment) Act 2004.

[22]. Cybercrimes (Prohibition and Prevention, etc) Act, 2015.

[23]. Central Bank of Nigeria, Consumer Protection Framework, 7th of November, 2016.

[24]. M.Chawki. 2009. Nigeria Tackles Advance Fee Fraud, 2009. Journal of Information, Law &Technology (JILT).

[25]. PO.J Uchenna Jerome Orji. 2019. Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. Tilburg Law Review 24(1), pp. 105–124.

[26]. S. O Dada, S.A. Owolabi, and A.T Okwu. 2013. Forensic accounting is a panacea for the alleviation of fraudulent practices in Nigeria. International Journal of Business Management and Economic Research. 4 (5), 787-792.

Cite this article as :

Misol Joan Kangkum, Agbadua Eshiofuezemhe Godsend, "Analysing and Mitigating the Problem of Internet and Credit Card Fraud In Nigeria", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 3, pp. 225-235, May-June 2022. Available at doi : https://doi.org/10.32628/CSEIT228374
Journal URL : https://ijsrcseit.com/CSEIT228374