CONCEPTUALIZING CYBER SCAM IN NIGERIA*

Abstract
Cyber scam is a white-collar crime committed by the use or manipulation of non-conventional tools such as phones, faxes, computers and other internet-enabled information technology devices within cyberspace. It thrives on the vulnerability of the victim and the witty deception of the cyber scammer. Cyber scam is unlike conventional crimes, and thrives on the violent and merciless disposition of the criminal which renders the victim helpless and in desperate fear for his life or safety of his family, as the case may be. This socio-legal and doctrinal research conceptualizes cyber scam within the broad family of cybercrimes. It explores certain forms of cyber scam as well as common modus operandi of cyber scammer in Nigeria. It also highlights some of the reasons why people indulge in cyber scam in Nigeria as well as core vulnerabilities of cyber scam victims. The research is primarily expository as it offers imperative elementary knowledge for safeguarding potential victims of cyber scam in Nigeria and beyond.

Keywords: *Cyber scam, Conceptualization, Security, Crime, Nigeria.*

1. Introduction

Cyber scam belongs to the family of cybercrimes which involves deceit via the use of phones, faxes, computers, ICT and other internet-enabled devices online, to dupe greedy, careless, unfaithful and emotionally vulnerable persons of huge sums of money and/or valuables. Suffice to say, that the growth and advancement in information technology facilitate cyber scam and allied cybercrime and cause incidental threats[1] in Nigeria and beyond.[2] This paper conceptualizes cybercrime and explains the initial formats and proposals which are sent to the potential cyber scam victim in order to gain his confidence, which is vital for making him part with money and valuables whenever the need arises in the course of his victimization. The study makes bold to posit that in appropriate cases, most victims of cyber scam are so easily deceived because they deliberately circumvent basic e-commerce procedures so as to lubricate their inert greed for disproportionate size of reward, that is,

[*]**Aloy OJILERE**, **LL.B (Hons.), BL, LL.M, PhD**, is an academic in the Faculty of Law, Imo state University, Owerri, Nigeria. He teaches Human Rights, Gender Studies and Jurisprudence. His research interest is in Cybercrime, Cybersecurity and safe e-commerce. He is also grounded in the judicialization, globalization and constitutionalization of fundamental rights in Nigeria, India and South Africa. Email: aloyojilere@yahoo.com; aloyojilere@imsu.edu.ng. Phone: +2348033277550;

***Prof. USF NNABUE, Ph.D,** is a Professor of Jurisprudence and an expert in International Economic Law. He is the pioneer Dean of Law, Imo State University, Owerri, Nigeria. Email: usfnnabue@yahoo.com.; and

[*]**Ikenga K. E. ORAEGBUNAM, PhD (Law), PhD (Phil.), PhD (Rel. & Soc.), Med, B.Th., BL,** Ag Head, Department of International Law & Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria. E-mail: ik.oraegbunam@unizik.edu.ng. Phone: +2348034711211.

[1] A. Kigerl, 'Routine activity theory and the determinants of high cybercrime countries', *Social Science Computer Review, 30*(4), 2012, 470-486.

[2] N. Kshetri, 'Pattern of global cyber war and crime: A conceptual framewor', *Journal of International Management*, *11*(4), 2005, 541-562.

a high value reward for small investment, [3] lack of emotional control and high romantic beliefs, and infidelity. [4] This research has the potential of saving many otherwise future victims of cyber scam, having provided them with sufficient knowledge or education which is confirmed by other researchers to be imperatively consequential to the global war against all manner of cybercrime.[5]

2. Concept of Cyber Scam

Cyber scam is a form of cybercrime. It involves the use of internet-enabled computers, phones and other smart electronic telecommunication and/or information gadgets/devices to commit fraudulent financial or depressive crimes on cyberspace.[6] It is a unique form of crime[7] and part of a global phenomenon which is threatening the economy of nations.[8] Like cybercrime, it has no precise definition or appellation.[9] Innovatively, Balogun and Obe describe it by the terms, 'E-crime' or 'electronic crime', that is, any crime accomplished through the knowledge or use of electronic devices like computers, phones and other handheld devices.[10] Taylor, Fritsch and Liederbach call it digital crime[11] while McQuade refers to it as computer crimes or high tech crime.[12] Holt describes it purely as technology-enabled crime.[13] All the above tags fit cyber scam and cybercrimes generally. However, by whatever name so called, cybercrime is a traditional offence facilitated by new tools and devices which bring unique challenges to old crimes.[14] It is either facilitated by the use of information and telecommunication technology including phones, faxes, emails, dating sites and

[3] M. Button, C. M. Nicholls, J. Kerr & R. Owen, 'Online frauds: Learning from victims why they fall for these scams', *Australian & New Zealand journal of criminology*, *47*(3), 2014, 391-408.

[4] T. Owen, W. Noble, & F. C. Speed, 'The Challenges Posed by Scammers to Online Support Groups: The 'Deserving' and the 'Undeserving' Victims of Scams' In *New Perspectives on Cybercrime*, 2017,. 213-240. Palgrave Macmillan, Cham.

[5] M. Grobler, J. Jansen van Vuuren, & J. Zaaiman, 'Preparing South Africa for cyber crime and cyber defense'. https://researchspace.csir.co.za/dspace/bitstream/handle/10204/7140/Grobler_2013.pdf?sequence=3 (18/4/2018).

[6] O. Longe, O. Ngwa, F. Wada, V. Mbarika & L. Kvasny, 'Criminal uses of information & communication technologies in sub-Saharan Africa: trends, concerns and perspectives', Journal *of Information Technology Impact, 9*(3), 2009, 155-172.

[7] K. Jaishankar, 'Cyber criminology: Evolving a novel discipline with a new journal', *International Journal of Cyber Criminology*, *1*(1), 2007, 1-6.

[8] O. R. Ehimen, & A. Bola, 'Cybercrime in Nigeria.' *Business Intelligence Journal*-January: 2010, 93-98.

[9] S. Gordon, & R. Ford, 'On the definition and classification of cybercrime.' *Journal in Computer Virology* **2**(1), 2006, 13-20.

[10] V. F. Balogun, & O. O. Obe, O. O., 'E-crime in Nigeria: Trends, tricks, and treatment', *The Pacific Journal of Science and Technology* 11, 2010, 343, 355.

[11] R. W. Taylor, E. J. Fritsch & J. Liederbach, Digital *crime and digital terrorism*. Prentice Hall Press, 2014.

[12] S. McQuade, *Understanding and Managing Cybercrime,* Boston: Allyn & Bacon, 2006 .; O. J. Olayemi, 'A socio-technological analysis of cybercrime and cyber security in Nigeria.' *International Journal of Sociology and Anthropology* **6**(3), 2014, 116.

[13] T. J. Holt, 'Exploring the intersections of technology, crime, and terror', *Terrorism and Political Violence*, *24*(2), 2012, 337-354.

[14] McQuade (n. 12)

other social media, or committed directly against computers and computer systems.[15] Some common cybercrimes targeted at computers and computer systems include web jacking, viruses, malwares and worms attack,[16] intellectual property crimes, password sniffing, magic bomb, cyberterrorism and cybersquatting[17] but these are outside the purview of this paper. Nonetheless, any criminal activity in Nigeria or elsewhere that uses a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of cybercrime.[18]

Cyber scam, like most cybercrimes, is high-tech and internet-aided white collar crime[19] which thrives on cyberspace and the victims may include the elderly,[20] other individuals, government institutions, public or private corporations and societies, local and international.[21] Titus and Gover[22] opine that they usually involve the deliberate deception or intention of deception with the promise of high or outrageous 'percentage' of financial or other gains which far outweigh 'investment'. It may even be premised on other bogus promise of goods or services which were grossly misrepresented and never intended to be provided.[23]

The notorious scam of 'advanced-fee fraud' in Nigeria, popularly known in the pre-Internet era as 'OBT' (Obtaining by false pretence) or '419'[24], and for which Nigeria is repeatedly thought of as the cradle of global cyber-scam is a form of cybercrime.[25] Scholars like Oraegbunam and Ewulum

[15] K. Dashora, 'Cybercrime in the society: Problems and preventions.' *Journal of Alternative Perspectives in the Social Sciences* **3**(1), 2011, 240-259.

[16] M. McGuire & S. Dowling, 'Cyber crime: A review of the evidence', *Summary of key findings and implications. Home Office Research report*, 2013, *75*.

[17] I.K.E. Oraegbunam & B.E. Ewulum, 'Assessing the Nigerian Cyber-security law and Policy for Protection of Critical Infrastructure for National development. In G. N. Okeke *et al* (eds.) *Law, Security and National Development* 50th Annual Conference of the Nigerian Association of Law Teachers (NALT), held 11-16, June, 2017 at the Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, 2017, 62-98.

[18] Dashora (n.15)

[19] G. Geis, 'Victimization patterns in white-collar crime. *Victimology: A new focus*, *5*, 1973, 86-106.

[20] M. Button, C. Lewis & J. Tapley, 'A better deal for fraud victims: research into victims' needs and experiences, 2009. https://researchportal.port.ac.uk/portal/files/1924328/NFA_Report_1_15.12.09.pdf (14/4/2018).

[21] J. W. Tomlin, 'Victims of White-Collar Crimes.' In: H.J. Schneider (ed.), *The Victim in International Perspective.* Berlin, GER: Walter de Gruyter, 1982

[22] R M. Titus & A. R. Gover, 'Personal fraud: The victims and the scams', *Crime Prevention Studies*, *12*, 2001, 133-152.

[23] Titus & Gover (n. 22) 134.

[24] This tag derives from the provision of section 419 of the Nigerian Criminal Code which criminalizes 'Obtaining by false pretences'. The said section provides that: 'Any person who by any pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years'.

[25] E. E. Adomi & S. E. Igun. 'Combating cyber crime in Nigeria', *The Electronic Library*, *26*(5), 2008, 716-725.

describe it as 'electronic scam' or 'electronic mail scam' and state that in any case, potential victims are promised a substantial percentage of the 'fortune' on the condition that they make a stated deposit to help in the paperwork and facilitate the process.[26]

The exact origin of scams is unknown; however, some scholars believe that scams, alongside theft and the likes, 'have existed for centuries in the offline even before the development in high-tech equipment' and that the same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend' .[27] Others claim that the crime emerged in the 1980s after the collapse of world oil prices left Nigeria's oil-dependent economy desiccated and citizens in need of quick money.[28] Without regard to its origin, this paper contends that the high level of political and economic corruption, unemployment, poverty and frustration in Nigeria lure some Nigerian youths into various vices, especially cyber scam which seems the easier way out. For instance, Balobun and Obe cited the case of a 28-year-old Nigeria man who 'made a fortune through the scam after two years of joblessness despite having diploma in computer science.'[29] It must, however, be noted that cyber scam, like other cybercrimes is a global menace[30] and not a Nigeria-only affair.[31] More so, there is no country in the world where there are no perpetrators and victims of cyber scam or other forms of cybercrime.[32] This possibly explains why Glickman contends that cybercrime is similar to a mafia enterprise.[33] Instructively, aside online dating romance scam, much of the cybercrime in Nigeria and other African countries come from merchants not following standard e-commerce verification procedures.[34]

3. Format or Proposal Prelude to Cyber Scam in Nigeria

In the social language of cyber scammers in Nigeria, the first or opening part of the communication with a potential victim prelude to victimizing him, is called 'format' or 'proposal'. This first contact may take one or several forms.[35] The commonest methods among the Nigerian cyber scammers are by fax messages, voice calls, handwritten or typed letters sent by post, email, Facebook Messenger

[26] Oraegbunam & Ewulum (n. 17).

[27] Dashora (n. 15) 241.

[28] D. J. Smith, . *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria.* Princeton, NJ: Princeton University Press, 2008.

[29] Balogun & Obe (n. 10).

[30]N. Kshetri, 'Pattern of global cyber war and crime: A conceptual framework', *Journal of International Management*, *11*(4), 2005, 541-562.

[31] A. Atta-Asamoah, 'Understanding the West African cyber crime process', *African Security Studies*, *18*(4), 2009, 105-114; R. Leukfeldt, S. Veenstra & W. Stol, 'High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands', *International Journal of Cyber Criminology*, *7*(1), 2013, 1.

[32] Adomi, & Igun (n. 25).

[33] H. Glickman,'The Nigerian '419' advance fee scams: prank or peril?', *Canadian Journal of African Studies/La Revue Canadienne Des Études Africaines*, *39*(3), 2005, 460-489.

[34] Adomi, & Igun (n. 25).

[35] A. Zingerle, 'The Art of Trickery: Methods to establish first contact in Internet scams', In *xCoAx Conference, Porto, Portugal, pages*, 2014.

or other social medium, couched in interesting, friendly, courteous or decently unsuspecting businesslike language. Written proposals usually look real, enticing and generally self-explanatory and understandable, albeit, with dots of grammatical mistakes, typographic errors, misspellings[36] as well as irregular use of upper and lower case alphabets. The written proposal is usually a typical one-fits-all letter for each category of prospective victim, categorized on the premise of their perceived vulnerability. For instance, a proposal for financial windfall will be sent to a businessman or entrepreneur, or a person, who from the nature of his job, is perceived to be rich or capable of sourcing credit from friends, family, sale of property, or financial institutions. In order to look convincing, these formats usually introduce the scammer as a child of a late head of state or other prominent and wealthy politician or public figure. One of such formats available online[37] run thus:

> MOSHOOD SEKO
> ADENUGA STREET,
> APAPA,
> LAGOS.
> FAX 234-1-7597554
>
> I am MOSHOOD Mobutu Sese Seko, son of the late President Mobutu Sese Seko of Congo Democratic Republic former Republic of Zaire. Presently there is a war going on in my country and so my family members escaped to Morroco [sic] while I am presently at Cotonou/Nigeria Border monitoring events.
>
> Because of the present crises, my environment is not conductive [sic] for investment and more over, [sic] most of my fathers [sic] properties and account have been frozen by the present government of Laurent Kabila.
>
> Now, I want to set up a business overseas and I have about $50 Million united state [sic] dollars set aside for this project, [sic] I decided to contact you to help me in setting up a business, but would not want my name or family name to be used.
>
> I am prepared to give you 20% of the total sum if you can assist me in claiming this fund from a security volt [sic] in Europe where my father (Mobutu Sese Seko) deposited this fund before he died.
>
> Please, do contact me immediately for us to discuss. As soon as I hear from you, and confirm your assistance every documents regarding to the claiming of this fund will be handed over to you as the family's foreign partner.
>
> Best regards
>
> MOSHOOD SEKO.

[36]C. E. Drake, J. J. Oliver & E. J. Koontz, 'Anatomy of a Phishing Email', In *CEAS*, August 2004.
[37] http://aima.cs.berkeley.edu/data/spam.txt (15/4/2018).

The proposal or format is different in the case of online dating romance scam. In the case of a widow, divorcee, single lady or estranged wife, perceived to be rich or credit-worthy, a proposal of intention to marry will prevail.[38] Here, the scammer sends a Friend Request to the potential victim on dating sites or other social sites like Facebook and the intended victim innocently accepts same and they open up communication as friends. The fraudster then checks the victim's marital vulnerability, for instance, in relation to being single, estranged, widowed or divorced, and in any case, becomes romantic. The fraudster will confess his 'love' and may even propose marriage. Somewhere in between he secures some level of intimacy, trust and confidence with the potential victim and from this point the 'game' commences, with the victim realizing only when it is already late, that he/she has been fleeced.[39]

4. Forms of Cyber Scam

Without doubt, cyberspace is an amazing global space which allows users to connect instantaneously over boundless distances. Regrettably, its anonymity and reach offer a great tool for criminals,[40] who have taken advantage of the Global Information Infrastructure to commit high tech crime including terrorism, thereby making everyone potentially vulnerable.[41] Communications in the course of this crime may be made through computers, phone calls, text messages, emails, fax messages or other online chats and social media. Victims' email and physical addresses are usually obtained from business journals, telephone directories, newspapers or magazines.[42] Cyber scam may be perpetrated in several forms and the scammers are usually so smart and skilfully manipulative that their victims hardly imagine or know that they are being victimized.[43] Primarily, cyber scammers and fraudsters strive on the real or perceived vulnerability of prospective victims.[44] These may include marriage or romance, contract or inheritance. **For a victim perceived to be an investor or entrepreneur, the proposal may be one for big oil deals in Nigeria (because Nigeria is a major global exporter of oil) or for construction contracts from 'the Federal Government', or to merely provide details of a 'reliable bank account' to which certain 'millions of dollars' accrued from 'over invoiced oil contracts from the Nigerian National**

[38] T. Owen, W. Nobl, & F. C. Speed, The Challenges Posed by Scammers to Online Support Groups: The 'Deserving' and the 'Undeserving' Victims of Scams. In *New Perspectives on Cybercrime* 2017, pp. 213-240. Palgrave Macmillan, Cham.

[39] A. N. Ojilere, & E. Osuji, Central Issues and Challenges in Cyberspace, Cybercrime and Cyber Policing in Nigeria. *Unpublished,* 2018.

[40] M. Grobler & J. J. Van Vuuren, Broadband broadens scope for cyber crime in Africa. In *Information Security for South Africa (ISSA), 2010* (pp. 1-8). IEEE.

[41] S. Basu, *Cloud Crimes: Understanding the Privacy Challenges*. Available from: https://www.researchgate.net/publication/323756519_Cloud_Crimes_Understanding_the_Privacy_Challenges DOI: 10.13140/RG.2.2.10450.86723. (25/3/ 2018).

[42] R. G. Smith, M. N. Holmes & P. Kaufmann, *Nigerian advance fee fraud*. Canberra: Australian Institute of Criminology, 1999.

[43] R. Leukfeldt, S. Veenstra & W. Stol, 'High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands'. *International Journal of Cyber Criminology*, 2013, *7*(1), 1.

[44] Ojilere & Osuji, (n.19).

Petroleum Commission (NNPC)'45 will be transferred for a 'future investment' or 'purchase of large properties or estate' in the account owner's home country. The hidden bait is that the victim will receive between 20%-40% 'of the total money while 10% will be set aside for all incidental expenses and payments' (suggesting that the victim will lose nothing or contribute nothing apart from nominating a bank account, since whatever upfront payment or 'advance fee' he may be compelled to make will be refunded from the 10% set aside for all monetary incidentals). Without doubt, several 'charges' will continue to arise and the scammer will continually urge the greedy victim to pay them all, for as long as he awaits the remittance of 'the millions of dollars' into his nominated bank account (after all, 10% of the total sum is 'set aside for refunding such incidentals'!). This scenario underscores the truth that much of the cyber scam victims in Nigeria and other African countries are merchants who deliberately ignore or try to cut standard corners of e-commerce[46] with the unlawful intention of illegally earning a high value reward for little or no investment.[47]

Another form of cyber scam popular in Nigeria is the online dating romance scam. It is a relatively new form of fraud that became apparent around 2008.[48] In this crime, perpetrators pretend to initiate a relationship through online dating sites then defraud their victims of large sums of money.[49] The scammer may request for the victim's mailing address with the pretext of sending her 'birthday gifts', 'valentine's day gift' or other 'big surprise' but eventually the fake 'parcel' will get 'stuck in transit' because the exact contents were undeclared and 'Customs' scanning machines revealed it actually contains 'precious and expensive jewelries'. At this point the victim because more curious and would gladly pay the 'customs duties' and 'handling charges' into a nominated bank account. Of course, there was never a parcel but so much money may have been lost. This confirms the fact that online dating romance cyber scam usually thrives on the victim's misplaced trust, lack of emotional control and high romantic beliefs, greed and infidelity. [50] Nonetheless, online dating romance scam is acclaimed to be one of the most traumatizing forms of cyber scam because of the double tragedy of emotional damage (heart break) and losing cash or other valuables.[51] And

[45] NNPC is deceitfully cited in this scam because Nigeria is an oil exporting country with petroleum, oil and gas as the main stay of its economy. It is therefore expected that NNPC can award contracts running into tens or hundreds of millions of dollars.

[46] Adomi & Igun (n. 25).

[47] M. Button, C. M. Nicholls, J. Kerr, & R. Owen, 'Online frauds: Learning from victims why they fall for these scams'. *Australian & New Zealand journal of criminology*, 2014, *47*(3), 391-408.

[48] M. T. Whitty, & T. Buchanan, 'The online romance scam: A serious cybercrime'. *Cyberpsychology, Behavior, and Social Networking,* 2012, 15(3), 181-183.

[49] Whitty & Buchanan (n. 48).

[50] T. Owen, W. Noble & F. C. Speed, 'The Challenges Posed by Scammers to Online Support Groups: The 'Deserving' and the 'Undeserving' Victims of Scams. In *New Perspectives on Cybercrime*, 2017 (pp. 213-240). Palgrave Macmillan, Cham.

[51] M. T. Whitty, & T. Buchanan, 'The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, 2016, *16*(2), 176-194. https://lra.le.ac.uk/bitstream/2381/33450/2/Whitty%20%26%20Buchananpsychological_impact_romance_scam_final%20version.pdf (14/4/2018).

regrettably, some of the victimized end up in 'street crimes' such as prostitution, drug sale and abuse, shoplifting and check or credit card fraud, just to earn a living.[52]

Another form of cyber scam common to cyber scammers in Nigeria involves a proposal made to a potential victim to fraudulently lay claim to certain huge funds as sole beneficiary and next of kin of a deceased wealthy man or woman, using his personal information and bank details.[53] The letter below is a typical proposal/format which explains this scam elaborately:

> Sir/Madam,
> Urgent Attention
> I am Mr. John Benson PA to late Umar Bongo the President of Gabon who just passed away few day now. Before I contacted you, I have asked God Almighty to direct me to an honest and trustworthy person that will not betray me when this deal is achieved. The deceased (my boss) had Deposited a consignment/fund, valued at (US$30M) in one of the security company in South Africa which I have all details so I need you to be the next of kin as a reminder was send to me by the security firm that they are expecting my boss next of kin. So that is why I have decided to contact you to assist me in repatriating this benefit left behind by my boss before they get confiscated or declared unserviceable since it is not compulsory that the next-of kin must be a blood relation to the deceased, but could be anybody and after that, w e canshare it thus: 50% to me 40% to you, while 10% should be given to any Orpha nage Home in my country.
> Please I will like you to tell me a little more about yourself, especially with the following information: Full Name, Address, Country, Age, Occupation and Photo Copy of Your ID or International Passport. Be rest assured that this deal is 100% risk free and legal and I guarantee that this will be executed under a legitimate arrangement that will protect you from any breach of the law.
> Thanks and waiting in anxious for your prompt response, as I came into South Africa today to see the lawyer in charge of the fund deposit.
> Yours Faithfully
> Mr. John Benson

Surprisingly, these cyber scammers have also victimized highly placed Nigerian public officers, and even national security personnel. The following report by Balogun and Obe is quite revealing:

> In 2004, the Inspector General of the Nigerian Police, Mr. Tafa Balogun, was tricked by fraudsters to the tune of millions of Naira equivalent of MTN recharge cards. The perpetrators called the Inspector General on his mobile phone and pretended to be Rtd. General Ibrahim Babangida (a former Nigerian Head of State), hence requesting recharge cards bi-weekly for a period of close to six weeks. It was the General's aides who eventually cautioned him that the General

[52] M. E. Gilfus, 'From victims to survivors to offenders: Women's routes of entry and immersion into street crime'. *Women & Criminal Justice, 1993, 4*(1), 63-89.

[53] Oraegbunam & Ewulum (n. 17).

> would not personally be requesting recharge cards in this absurd manner. The fraudsters were eventually located and arrested.[54]

From the forgoing, Basu's recent conclusion is true, that, with advances in technology and the use of phones and internet-enabled devices, everyone is a potential victim of cybercrime,[55]

5. Impact of Cyber Scam

The complex and borderless scope of cyber scam, like other forms of cybercrime, has multiple damaging effects on both the victim and society.[56] The depression, emotional damage and lingering effects on cyber scam victims can be critical.[57] According to Dashora,[58] the damage dealt is largely psychological and intangible, making legal action against the variants more difficult. This is true because reports reveal that some victims of cyber scam and their family members sell their choicest property or take huge bank loans to fund the 'investment' or 'transactions' that they became so impoverished and frustrated with life and huge debts.[59] Others may be engage in illicit drugs, prostitution, shoplifting and other street crimes to earn a living.[60] In unbearable cases, the victims commit suicide.[61] Unfortunately, majority of cyber scam victims neglect to file complaints, while some are unable to file complaints because they feel ashamed, greedy or stupid, or don't even 'know' their scammers, thereby making it less likely for the fraudster to get caught.[62] Aside personal or human trauma and emotional damage, cyber scam also impacts negatively on the political, economic and domestic national psyche as well as the global integrity of a nation.[63] For instance, international financial institutions now view paper-based Nigerian financial instruments with suspicion. Nigerian bank cheques and bank drafts are not considered as risky instruments in international financial instruments.[64] Worst of all, Nigeria is acclaimed the 56th out of 60 countries in Internet usage but the third in the fraud attempt category, hence, Transparency International list

---

[54] Balogun & Obe, (n. 10) 343, 347.

[55] Basu (n. 41).

[56] O. M. Olanrewaju & F. O. Adebiyi, 'The Impact of Mobile Information and Communication Technology on Cybercrime in Nigeria'. *International Journal of Engineering*, 2014, *3*(8)

[57] B. Atkins & W. Huang, 'A study of social engineering in online frauds', *Open Journal of Social Sciences*, *1*(03), 2013, 23.

[58] Dashora (n. 15).

[59] M. Button, C. Lewis, & J. Tapley, 'Not a victimless crime: The impact of fraud on individual victims and their families'. *Security Journal, 27*(1), 2014, 36-54.

[60] Gilfus (n. 52).

[61]R. G. Brody & F. S. Perri, 'Fraud detection suicide: the dark side of white-collar crime.' *Journal of Financial Crime*, *23*(4), 2016, 786-797.

[62] R. Fried, 'Cyber scam artists: A new kind of. com.', 2001, *Crime scene investigator network*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.454.1487&rep=rep1&type=pdf (14/4/2018).

[63] F. B. Okeshola & A. K. Adeta, 'The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria'. *American International Journal of Contemporary Research*, *3*(9), 2013, 98-114.

[64] Balogun & Obe (n. 10).

Nigeria as one of the most corrupt countries in the world.[65] Interestingly, most developing countries, including Nigeria,[66] recognize the importance of sustainably outlawing malicious Computer-related acts (including cyber scam) in order to promote a secure environment for e-commerce, hence, they quest for a standard model for achieving this goal.[67]

6. Legal Approach to Cyber Scam in Nigeria

There is no criminal jurisprudence in Nigeria which defines or criminalizes cyber scam as a distinct offence. However, the cumulative import of certain legislation in Nigeria demonstrates government's legislative approach for tackling cyber scam in Nigeria.[68] Sections 418 and 419 of the Nigeria Criminal Code[69] are the foremost provisions for defining and prosecuting cyber scam in Nigeria, since it is a crime rooted in false pretence and deception. Section 419 criminalizes 'Obtaining by false Pretences' (OBT)[70] while section 418 defines 'a false pretence'. The said section 418 defines 'a false pretence' as any representation made by words, writing or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true. The said section 419 describes as felony, the conduct whereby any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, and makes it punishable on conviction, with three years' imprisonment.

Relatedly, section 383(1) of the Code provides that a person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing. However, the fact that relevant provisions of the Nigerian Criminal Code do not make restitution of the proceeds of scam an integral part of the punishment for OBT is a drawback in the fight against cyber scam in the country. Furthermore, under Part 2 of the Economic and Financial Crime Commission Act, 2004 which provide the legal framework for the establishment of the Economic and Financial Crime Commission, the Commission is *inter alia*, empowered to undertake the investigation of all financial crimes, including advance fee fraud, computer credit card fraud, contract scam, money laundering, counterfeiting, illegal charge transfers, futures market fraud and fraudulent encashment of negotiable instruments. Another legislation relevant to combatting cyber scam in Nigeria is the Advance Fee Fraud and Related Offences Act 2006. Its section 23 defines 'false pretence' as 'a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.' It also defines 'economic crime' as ' the nonviolent criminal and illicit activity committed with the objectives of earning wealth

[65] Balogun & Obe (n. 10).

[66] See the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.

[67] M. Olusola, O. Samson, A. Semiu & A. Yinka, 'Cyber crimes and cyber laws in Nigeria'. *The International Journal of Engineering and Science (IJES)*, *2*(4), 2013, 19-25.

[68] Olusola *et al* (n. 67).

[69] Cap C38. Laws of the Federation of Nigeria, 2004.

[70]This section suggests why cyber scam (also known as Advance Fee Fraud) in Nigeria is locally known as 'OBT' and globally described by the alternative term, '419'.

illegally, either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting, and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes and prohibited goods.' The Act is one of the foremost Nigerian legislation on cyber scam and allied cybercrime including the regulation of cybercafés and Internet service providers, albeit it does not cover several forms of cybercrime and computer abuse or misuse.[71]

Although not specifically stated, the Nigerian National Cybersecurity Policy (NCP), 2014 which mainly seeks to protect Critical National Infrastructure (CNI) may logically apply for combatting cyber scam in Nigeria. The Policy sets out strategic intent of government for safe national and economic presence on cyberspace, and Part 1.3 thereof lists Cybercrime (invariably including Cyber scam) as one of the national cybersecurity threats understood to pose significant inimical challenges to Nigeria's security and national growth. The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 may also be applicable for combatting cyber scam in Nigeria, as it seeks to protect Critical National Information Infrastructure (CNII) by creating a legal, regulatory and institutional framework for the *prohibition*, *prevention*, detection, investigation and prosecution of *cybercrimes* and for other related matters.[72] Its section 33 criminalizes computer related fraud with specific reference to Electronic Cards Related Fraud. However, sections 30 and 58 of the Act seem specifically instructive in the tackling of cyber scam in Nigeria. Section 30 of the Act provides that where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purpose of a criminal investigation or proceeding, a judge may, on the basis of information on Oath; order a service provider, through the application of technical means, to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data or traffic data associated with specified communications transmitted by means of a computer system. Sections 58 Act defines *Computer* as 'an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic or storage function and includes any data storage facility and all communication devices that can directly interface with a computer through communication protocols.'[73] Mobile phones and fax machines which are common ICT tools used in the commission of cyber scam, no doubt, fall under this definition, being *inter alia,* electronic, communication and high speed data processing devices performing logical, arithmetic or storage function.

---

[71] F. Wada & G. O. Odulaja, 'Assessing cyber crime and its impact on e-banking in Nigeria using social theories. *African Journal of Comp & ICTs*, *5*(1), 2012, 69-82.

[72] Part 1 of the Act lists Its objectives as (a) to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; (b) ensure the protection of critical national information infrastructure; and (c) promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

[73]This definition, however, excludes portable hand held calculators, typewriters and typesetters or similar devices. Section 58 *ibid.*

Under the Act, punishment for cyber scam is generally decisive and follows the criminological theory of deterrence. Section 12(1) criminalize cyber scam and prescribe an imprisonment of not less than five years or a fine of not less than N10,000,000.00 (Ten Million naira, nearly $USD 30,000) or to both fine and imprisonment upon conviction, for any person who with intent to defraud sends electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss.

Under the Act, a court may also make an Order of forfeiture of proceeds, assets and equipment/tools of the cyber scam,[74] or as the case may be, an additional Order for payment of compensation or restitution against the convict.[75] This same punishment applies to any person found guilty of attempting to commit any offence under the Act, or does any act preparatory to or in furtherance of the commission of an offence under the Act, or abets, aids or conspires to commit any offence under the Act.

The Act also establishes the Cybercrime Advisory Council which shall create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybe Part VI of the Act empowers law enforcement officers to search the bodies or premises of suspected/actual offenders and if need be, arrest them or seize or retain the tools of their illicit trade,[76] investigate them and if need be,[77] search them without warrant, and prosecute them.[78] Most fundamentally, 'one of the most remarkable landmarks of the Cybercrimes Act'[79] is contained in section 50(4) which provides that an Order for stay of proceedings shall not be made by any court with respect to any criminal charge brought pursuant to the Act. These provisions, make it obvious, without prejudice to certain notable evidential gaps,[80] that the Act generally, is a commendable legal, procedural and institutional advancement for combatting cyber scam and cybercrimes, as well as for promoting safe e-commerce and use of cyberspace in Nigeria.

7. Conclusion

Cyber scam is a global menace and every user of cyber-enabled devices as well as e-commerce is a potential victim. And like other cybercrimes, it can only be minimized and not completely eradicated.[81] This paper explores common forms of cyber scam and shows that although cyber scam is popular in Nigeria, it is a global factor which has battered the collective domestic and international

[74] Section 31, *ibid.*

[75] Section 32, *ibid.*

[76] Section 27, *ibid.*

[77] Section 28, *ibid.*

[78] Section 30, *ibid.*

[79] I. K. E. Oraegbunam, 'Towards Containing the Jurisdictional Problems in Prosecuting Cybercrimes: Case Reviews and Responses.' *Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 7*, 2016, 26-40; Oraegbunam & Ewulum (n. 17) at 72.

[80] Oraegbunam & Ewulum (n.17).

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

image of Nigeria, [82] its citizens as well as its financial practices and corporate institutions.[83] It confirms that name-dropping and deceit are crucial factors in most cyber scam proposals. It further confirms that victimization and vulnerability to cyber scam vary in relation to individual attitude to greed, fidelity, and adherence to standard e-commerce procedures. It concedes, and as is evident from section 56 of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015, that cyber scam, like most cybercrimes, is extra-territorial and transnational in nature and therefore requires joint and collaborative global efforts and measures to deal with.[84] The paper is significant because it raises vital conceptual and theoretical awareness necessary for the understanding of cyber scam in Nigeria, and possibly insulating potential victims of future cyber scam.

[82] M. C. Ogwezzy, 'Cybercrime and the proliferation of yahoo addicts in Nigeria' *AGORA Int'l J. Jurid. Sci.: 2012, 86.*

[83] Adomi & Igun (n. 25).

[84] Oraegbunam (n. 79); I. K. E. Oraegbunam, 'Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea from International Law? *Nnamdi Azikiwe University Journal of International Law and Jurisprudence, 6*, 2015, 57-65. For the avoidance of doubt, the said section 56 of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 permits the exchange of valuable or critical information between local and international Cybercrime and law enforcement agencies for combatting cybercrime and promoting cybersecurity.