Journal of Information, Law & Technology

Nigeria Tackles Advance Fee Fraud

Dr. Mohamed Chawki
Senior Judge, the Council of State, Egypt; Senior Legal Adviser, Ministry of State for Military Production; Postdoctoral Fellow, ISPEC, University of Aix – Marseille III, France
mohamed_chawki@hotmail.com

This is a **refereed article** published on 28 May 2009.

Citation: Chawki, M., 'Nigeria Tackles Advance Free Fraud', 2009(1) Journal of Information, Law & Technology (JILT), <http://go.warwick.ac.uk/jilt/2009_1/chawki>

Abstract

Nigerian 419 scam is a major concern for the global community. The introduction, growth and utilization of information and telecommunication technologies (ICTs) have been accompanied by an increase in illegal activities. With respect to cyberspace, anonymous servers, hijacked emails and fake websites are being used as a tool and medium for fraud by cyber scammers. Nigerian advance fee fraud on the Internet is an obvious form of cybercrime that has been affected by the global revolution in ICTs. This form of crimes is not exclusive to advance sums of money to participate into business proposals but also covers romance, lottery and charity scams. Estimates of the total losses due to this scam vary widely. In the United Kingdom, a report conducted by a research group concluded that Internet scams in which criminals use information they trick from gullible victims and commonly strip their bank accounts cost the United Kingdom economy £150 million per year, with the average victim losing £31,000.[1] Thus, there is a need for international cooperation to stamp out such illicit activities and protect Internet users. Although new techniques are constantly being implemented and regulations being adopted to combat and eradicate diverse forms of advance fee fraud, yet cyberspace is also providing new means and tools that facilitate committing these scams. Accordingly, this paper seeks to address and analyse some issues related to the use of cyberspace for fraud by cyber scammers especially in Advance Fee Fraud and the techniques used. It will also provide an analysis of the existing legislative and regulatory framework and their efficiency in combating this form of cross-border crime taking Nigeria as a case study. Finally, the paper will conclude by discussing some measures to fight the use of Internet in illegal activities, especially with respect to AFF.

Keywords: Cybercrime, Advance Fee Fraud, 419 Scam.

'Why do some very clever people do this instead of a legitimate job, which may pay just as much but without the risk of prison? It's because I enjoy the power. The power of the burglar or the car thief or mugger in physical. The power of the con artist like me is mental'

Quote from a scammer

1. Introduction

The term '419' is coined from section 419 of the Nigerian criminal code (part of Chapter 38: Obtaining Property by false pretences; Cheating) dealing with fraud. Nowadays, the axiom '419' generally refers to a complex list of offences which in ordinary parlance are related to stealing, cheating, falsification, impersonation, counterfeiting, forgery and fraudulent representation of facts (Tive, 2006, p. 3). The main difference between '419' scam and stealing is the 'false pretence' which is the major element in '419' scam. According to Section 23 of the advance fee

[1] *See* Nigeria Scams Cost UK Billions, *BBC News*, [20 – 11 – 2006].

fraud[2] decree: '*False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true*'. Section 383 sub-section 1 of the Nigerian Criminal Code states: '*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*'. It must be noted that falsification, impersonation, forgery and fraudulent representation of facts are all related tools that combine to either abet or facilitate the advance fee fraud (Tive, 2006, p. 4). Advance fee fraud did not start with the Internet, although the Internet enables the criminals to reach a greater number of potential victims more quickly and economically, and sometimes without being traced (Reich, 2004, p. 2).

In the United Kingdom, the Audit Commission has conducted four triennial surveys of computer-related fraud based on a definition referring to: '*any fraudulent behavior connected with computerisation by which someone intends to gain financial advantage*'. Such a definition is capable of encompassing a vast range of activities some of which may have only the most tenuous connection with a computer (Chawki, 2005, p. 41). The Council of Europe, in its report on computer-related crime advocates the establishment of an offence consisting of: '*The input, alteration, erasure or suppression of computer data or computer programmes [sic], or other interference with the course of data processing, that influences the result of data processing thereby causing economic loss or possessor loss of property of another person, or with the intent of procuring an unlawful economic gain for himself or for another person*' (Chawki, 2005, p. 42). However this definition is broad in scope. It would appear for example that the proposed offence would be committed by a person who wrongfully uses another party's cash dispensing card to withdraw funds from a bank account. Although there can be little doubt about the criminality of such conduct, the involvement of the computer is purely incidental. In most areas of traditional legal interests, the involvement of computer data does not cause specific legal problems. The respective legal provisions are formulated in terms of results and it is completely irrelevant if this result is achieved with the involvement of a computer or not.

The *Online Etymology Dictionary* associates 419 scam to a nineteenth century British slang 'scamp', which means 'cheater' or 'swindler'. All the same, ever since 1963, when some scholars say the term 'scam' made it into written literature for the first time, the central meaning has not changed – it is a trick, a ruse, a swindle, a racket (Igwe, 2007, p. 6). Although 419 is broached as a global phenomenon, it did emerge from Nigeria and was the brainchild of a group of Nigerian nationals (Igwe, 2007, p. 6). Therefore, a frontal battle against 419 ought not to overlook its place of origin and the numerous factors that gave birth to it. Many specialists in African studies claim without substantiating details that the game began in the 1980s with the Nigerian petroleum companies as major players. Some argue to the contrary, maintaining that 419 evolved from various types of tricks played since time out of mind, mostly in Igbo land in southeastern Nigeria (Igwe, 2007, p. 6). Neither of these arguments is far from the truth, since both the oil industry and local intelligence have influenced the evolution of the scheme. The fact is that human beings tend to look for scapegoats all the time. In doing so, we often adopt limited views that undermine the idea that a single incident is often the result of a chain of combining

[2] Advance Fee Fraud connotes the demand for and payment of an advance fee in the form of tax, brokerage, legal fees, etc. under the pretence that such fees are needed to consummate the deal.

and complementary forces and actions. A massive amount of advance fee fraud messages are sent out every day around the world, though many recipients ignore or discount their content.[3] At the same time, a small percentage of all recipients respond to these messages and become victims who lose money or have their identities stolen at the hands of fraudsters (Holt et al., 2007, p. 138).

2. The Operation of the Scheme

Advanced Fee Frauds commence with the receipt of an official-looking letter or email, usually purporting to be from the relative of a former senior government official, who, prior to their death, accrued a large amount of money which is currently being held in a bank account within the country from which the letter was being sent (Wall, 2007, 90). The sender of the following typical 419 letter invites the recipients to assist with the removal of the money by channeling it through his or her bank account. In return for collaborating, the recipient is offered $ 12 million, 20 per cent of the 460 million to be transferred (Wall, 2007, 91). Once recipients respond to the sender, an advanced fee is sought to pay for banking fees and currency exchange. As the victim becomes more embroiled in the scam and pays out money, it becomes harder to withdraw. Needless to say, the majority, if not all, of these invitations are bogus and are designed to defraud the respondents, sometimes for considerable amounts of money (Wall, 2007, 92). Another technique employed by the scammers is to invite the victim to visit the scammers in their 'home' country to explain their situation in person and ask for money and assistance. This ploy is relatively uncommon, though it can lead the victim to be held hostage or killed (Holt et al., 2007, p. 140). A final method requires the victim to provide the scammer with personal information,[4] such as their name, address, employer, and bank account information. The initial request may be made under the guise of assuring the sender that the recipient is a sound and trustworthy associate (Holt et al., 2007, p. 140). However the information is surreptitiously used by the sender to drain the victim's accounts and engage in identity theft. [5]

3. The Nature and Extent of the Problem

Advance Fee Fraud is a vexing threat and a major problem. It takes diverse forms and degrees ranging from advancing sums of money to murder (Tenfa, 2006, p.11). Furthermore, law enforcement officers find it difficult to identify and apprehend cyber scammers. This may be due to the fact that perpetrators can use technology to conceal their identities and physical location, thereby frustrating law enforcement efforts to locate them (Chawki et al., 2006, p.5). The traditional model of law enforcement assumes that the commission of an offence involves

[3] For instance in February 2000, the US Security and Exchange Commission brought charges against a Florida woman. She had promised 100% weekly returns through a Bank debenture trading programme. She raised $1.5 million through the scam by soliciting customers over the Internet. Customers invested from $25,000 to $50,000. The funds raised through the scam ended up in an individual's Bank account, who withdrew some of the funds at a casino. *See* T. Oriola, Advance Fee Fraud on the Internet, *Computer Law and Security Report* (2005), 21, p. 239.

[4] Although data and information are synonymous according to most dictionaries, some people like to think of data as 'raw' information or as collections of symbols that are not structured and labelled for people to use.

[5] The term 'identity' is commonly used arbitrarily and imprecisely in popular media and literature and the terms 'identity theft' and 'identity crime' are frequently used interchangeably. The *Oxford English Dictionary* defines 'identity' as '*the set of behavioral or personal characteristics by which an individual is recognized*'. Collins, J (2005), Preventing Identity Theft Into Your Business (New Jersey:John Wiley), 7.

physical proximity between perpetrator and victim (Brenner, 2004, p.6). This assumption has shaped our approaches to criminal investigation and prosecution.[6] Real-world criminal investigations focus on the crime scene as the best way to identify a perpetrator and link him to the crime (Chawki, 2008, p. 13). However, in automated or cybercrime there may either be no crime scene or there may be many crime scenes, with shredded evidence of the crime is scattered throughout cyberspace [7] (Parker, 2002). In this respect Dana van der Merwe (2008, p. 104) argues that:

> '[T]he true problem of the information and communication era seems to be to decide exactly how much value should be attached to a given piece of information, especially when that information is stored electronically and digitally. The only field of law which advertises itself as a specialist in the area of verifying facts is the law of evidence. Unfortunately, like all other fields of law this field sometimes finds itself struggling to adapt to a new world in which paper is being phased out of general commercial transactions and to decreasing contact between human beings and the information needed to conduct business.'

Accordingly, identifying an electronic crime scene can be a daunting task when the perpetrator may have routed his communications with the victim through computers [8] in three or four countries, with obscure networks that are inaccessible to investigators (Chawki et al., 2006, p.5).[9] Very few estimates are available for advance fee fraud, and many of those published are more than a decade old.[10] With regard to the United States, a number of conflicting figures have been published. Some examples include the following (Bocij, 2006, p. 103):

- The FBI reported that victims of advance fee fraud suffered an average had tripled since 2001, as had total losses, growing from $ 17 million to $ 54 million.

[6] Cybercrime is of borderless nature and conventional boundaries are no longer the norm. A virus for instance can cause widespread consequences worldwide. The gathering of admissible evidence in another country could be extremely difficult. The successful investigation and subsequent prosecution of some cybercrime will depend greatly on the co-operation between the different countries during the investigation process. Maat S (2004), Cybercrime: A Comparative Law Analysis (Thesis, UNISA), 210.

[7] The term cyberspace literally means 'navigable space' and is derived from the Greek word *kyber* (to navigate). In William Gibson's 1984 novel, the original source of the term, cyberspace refers to, a navigable, digital space of networked computers accessible from computer consoles, a visual, colourful, electronic, cartesian datascape known as 'The Matrix' where companies and individuals interact with, and trade in, information.

[8] The concept *computer* was defined in section 1(1) of the Computer Evidence Act as *any device or apparatus, whether commonly called a computer or not, which by electronic, electro-mechanical, mechanical or other means is capable of receiving or absorbing data and instructions supplied to it, of processing such data according to mathematical or logical rules and in compliance with such instructions, of storing such data before or after such processing, and of producing information derived from such data as a result of such processing*. Act 57 of 1983.

[9] The distinction between 'traditional crime' and 'new crimes' was made by K. Burden and C. Plamer was made in their article 'Cybercrime – A New Breed of Criminal?' (2003) 19(3). The authors distinguished on page 222 between true cybercrimes and simply e-enabled crimes in which the act was known to the world before the advent of the World Wide Web, but in now increasingly perpetrated over the Internet. Maat, S (2004), Cybercrime, A Comparative Law Analysis (Thesis, UNISA), 4.

[10] According to the Special Fraud Unit Section, Nigeria Police Force, between 1998 and 2000, the following nationals complained to the Nigerian police as victims of advance fee fraud scam: Germany 24; United States16; Japan 6; Canada 5; India 5; Iran 5; South Africa 2; Egypt 2; New Zealand 2; Philippines 1; Saudi Arabia 1; Korea 1; Taiwan 1; Israel 1; and Nigeria 113. *See* T. Oriola, Advance Fee Fraud on the Internet, Computer Law and Security Report (2005), 21, p. 239.

- An estimate that has been quoted widely in the media claims that losses in the United States amount to $ 1 million to $ 54 million.
- In 2005, the average loss from 419 frauds was estimated at $ 6,937 by the National Consumers League. Other advance fee frauds resulted in an average loss of $ 1,426. However, an estimate from the FBI places the average loss from 419 FRAUD IN 2005 at $ 3, 000.

It is also difficult to obtain realistic estimates for other countries. However, the available information suggests that average losses are similar to those experienced in the United States. Some examples of losses experienced by other countries include (Bocij, 2006, p. 103):

- In Canada, Phone Busters received 167 complaints over the period from January 2004 to September 2004. Victims lost a total of approximately $ 4.2 million.
- A 2004 estimate suggests that annual losses in South Africa are in the region of R100 million (approximately $ 16.5 million).
- In the United Kingdom, the National Criminal Intelligence Service (NCIS) reported that 150 people were defrauded for a total of £ 8.4 million, an average loss of £ 56,675, or almost $ 100,000. Total losses each year could be in the region of £ 150 million, or approximately $ 262 million.

4. Evaluation of the Current Situation in Nigeria

According to 2007 Internet Crime Report prepared by the National White Collar Crime Centre and the FBI, Nigeria currently ranks third in the world with 5.7 per cent of perpetrators of cybercrime (2007 Internet Crime Report, p.9). Though the perpetrator percentage of 5.7 from Nigeria appears low, we can regard it as rather high considering that less than 10 per cent of the 150 million population of Nigeria use the internet (Delta State University Report). In Africa, though internet use is higher in South Africa, cybercrime perpetrators percentage is higher for Nigeria than RSA as it is mentioned in the report. Cybercrime has a negative impact on Nigeria. It can be explained in the terms of the following statistics (WITFOR 2005):

- Annual global loss of $ 1.5 billion in 2002.
- 6% of global Internet spam in 2004.
- 15.5% of total reported FBI fraud in 2001.
- Highest median loss of all FBI Internet fraud of $ 5,575.
- VeriSign, Inc., ranked Nigeria 3rd in total number of Internet fraud transactions, accounting for 4.81% of global Internet fraud.
- American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up 900% in 2001.

Nigerian Cybercrime has the potential to impact technology growth which is a key requirement for productivity improvement, and ultimately for socio-economic growth because (WITFOR 2005):

- International financial institutions now view paper-based Nigerian financial instruments with scepticism. Nigerian bank drafts and checks are not viable international financial instruments.
- Nigerian ISPs and email providers are already being black-listed in e-mail blocking blacklist systems across the Internet.
- Some companies are blocking entire Internet network segments and traffic that originate from Nigeria.
- Newer and more sophisticated technologies are emerging that will make it easier to discriminate and isolate Nigerian e-mail traffic.
- Key national infrastructure and information security assets are likely to be damaged by hostile and fraudulent unauthorized use.

Accordingly cybercrime has created an image nightmare for Nigeria. When one comes across phrases like 'Nigerian scam', the assumption that crosses one's mind is that all (or conservatively most) scam e-mails originate from Nigeria or Nigerians – though this is actually not the case (Adomi, 2008, p. 720). Advance fee fraud has brought disrepute to Nigeria from all over the world. Essentially, Nigerians are treated with suspicious in business dealing. Consequently, the honest majority of Nigerians suffer as a result (Adomi, 2008, p. 720).

5. Advance Fee Fraud Combating Efforts in Nigeria

It has been argued that organized crime[11] weakens the very foundation of democracy, as there can be no good governance without rule of law (Ngor, p. 172). This observation is quite apt for the situation in Nigeria. As the nation faces the challenges of nurturing a stable democracy, after many years of military dictatorship, organized crime poses a great threat to the survival of the country (Ngor, p. 172). Therefore, the Nigerian government has mapped out policies and strategies to deal decisively with crimes that are transnational in nature and scope.

5.1 Legislative Approaches

The Nigerian government has over the years enacted far-reaching laws aimed at checkmating transnational organized crime and punishing the perpetrators of these crimes. Under this sub-section we shall focus on the Criminal Code Act, Economic and Financial Crimes Commission Act 2004, Computer Security and Critical Information Infrastructure Protection Bill 2005 and Advance Fee Fraud and other Fraud Related Offences Act 2006.

(A) Criminal Code Act

[11] The involvement of organised crime groups in the field of computer fraud was illustrated when a Russian group attacked one of the known US banks in New York via data networks in 1994. Operating from St. Petersburg, the group succeeded in causing the American bank to transfer over US$ 10 million to foreign accounts. The arrested perpetrators possessed false Greek and Israeli passports which were forged in a quality which could be produced in Russia only by members of the former Russian secret service KGB. M. Lyman, M and Porter, G, Organized Crime (New Jersey:Prenhall); Sieber, U (1998), Legal Aspects of Computer Related Crime, (European Commission), 25.

Advance fee fraud scam under the Nigerian Criminal Code Act, qualifies as a false pretence (section 418), while a successful Internet scam would amount to a felony under section 419. This section provides as follows:

'Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. If the thing is of the value of one thousand naira or upwards, he is liable to imprisonment for seven years. It is immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretence. The offender cannot be arrested without warrant unless found committing the offence.'

Furthermore, a suspect could alternately be charged under section 421 of the Criminal Code Act which provides as follows:

'Any person who by means of any fraudulent trick or device 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 or to pay or deliver to any person any money or goods, or any greater sum of money or greater quantity of goods than he would have paid or delivered but for such trick or device, is guilty of a misdemeanour, and is liable to imprisonment for two years. A person found committing the offence may be arrested without warrant.'

The Criminal Code is a British legacy which predates the Internet era and understandably does not specifically address email scams (Oriola, 2005, p.240). Advance fee fraud methodology obviously falls within the remit of the Act for the following reasons: first, there is a false pretence to the existence of non-existent money; second, a solicitation for financial help to get the fictitious money released; and third, the fraudulent retention of various fees paid to the scammers to release the phony millions of dollars. The scammers' modus operandi fits snugly the elements of the offence under section 419 of the Criminal Code Act cited above, and have been used for years by the Nigerian law enforcement agencies for prosecuting alleged acquisition of property by false pretence (Oriola, 2005, p.240). However, the Criminal Code Act provisions on advance fee fraud are ill-suited for cyberspace criminal governance. Oriola argues that (2005, p.241):

> 'Although section 419 of the Criminal Code Act deems advance fee fraud a felony, the provision that an advance fee fraud suspect cannot be arrested without a warrant, unless found committing the offence, does not reflect the crime's presence or perpetration in cyberspace. Only in rare circumstances could a suspect be caught in the act because most of the scam emails are sent from Internet cafe´s. Aside from the fact that the country lacks the resources to police every known cyber cafe´, doing so could actually raise privacy or other rights issues (…) If found guilty, an advance fee fraudster is liable to a mere three years imprisonment or seven years if the value of stolen property exceeds 1000 naira. The punishment, to say the least, is paltry relative to the enormity of the crime and unjust rewards that characteristically run into millions of dollars. Thirdly, in criminal trials, the State is the complainant, and there is hardly any compensation for victims of crime under the Nigerian criminal justice system. The victims could no doubt

resort to civil court for remedies. However, the prospects for success for the plaintiff in the typical advance fee fraud case scenario are extremely slim. For instance, a contract to assist in the transfer from Nigeria of millions of dollars illegally to a foreign account, or to pay bribes to certain government officials to ensure release of such moneys, or to facilitate advance fee payment for patently illegal activities, would be unenforceable. The plaintiff would be branded as a party to a culpable crime by the Nigerian courts'.

(B) Economic and Financial Crimes Commission Act 2004

The Economic and Financial Crimes Commission (Establishment) Act was adopted in June 2004. It repealed the Financial Crimes Commission Act of 2002 and establishes a Commission for Economic and Financial Crimes. Under this act, the Commission has the power to investigate all financial crimes relating to terrorism, money laundering, drug trafficking, etc. Sections 14 – 18 stipulate offences within the remit of the Act. This includes offences in relation to financial malpractices, offences in relation to terrorism, offences relating to false information and offences in relation to economic and financial crimes. The Act defines Economic and Financial Crimes as:

'the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes 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, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited goods, etc.'.

Although this definition does not refer directly to advance fee fraud or internet scam it could be argued that a direct reference to email frauds in the Economic and Financial Commission Act is superfluous and therefore unnecessary, since the Commission is already charged inter alia, with administering the Advance Fee Fraud and other Related Offences Act, which directly governs advance fee fraud in cyberspace (Oriola, 2005, p.244).

(C) Money Laundering (Prohibition) Act 2004

Another related law on Internet scam regulation in Nigeria is the Money Laundering (Prohibition) Act 2004. It makes provisions to prohibit the laundering of the proceeds of crime or an illegal act. Although advance fee fraud is not expressly mentioned in the Act, proceeds of the scam would appear covered under section 14(1) (a) which, prohibits the concealing or disguising of the illicit origin of resources or property which are the proceeds of illicit drugs, narcotics or any other crime. The Act also implicates any person corporate or individual who aids or abet illicit disguise of criminal proceeds. Section 10 makes life more difficult for money launderers. Subsection (1) places a duty on every financial institution to report within seven days to the Economic and Financial Crimes Commission and the National Drug Law Enforcement Agency any single transaction or transfer that is in excess of ¼N1m (or US$7,143) in the case of an

individual or ¼N5m (US$35,714) in the case of a body corporate (Chukwuemerie, 2006, p. 178). Any other person may under sub-section (2) also give information on any such transaction, or transfer. Under sub-section (6) even if a transaction is below US$5,000 or equivalent in value, but the financial institution suspects or has reasonable grounds to suspect that the amount involved in the transaction is the proceed of a crime or an illegal act it shall require identification of the customer. In the same way, if it appears that a customer may not be acting on his own account, the financial institution shall seek from him by all reasonable means information as to the true identity of the principal (Chukwuemerie, 2006, p. 177). This enables authorities to monitor and detect suspicious cash transactions.

(D) Computer Security and Critical Information Infrastructure Protection Bill 2005

In 2005, the Nigerian government adopted the Computer Security and Critical Information Infrastructure Protection Bill (known as the Cybercrime Bill). The Bill aims to '*secure computer systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain computer based activities*' and to impose liability for global crimes committed over the Internet. The Bill requires all service providers to record all traffic and subscriber information and to release this information to any law enforcement agency on the production of a warrant. Such information may only be used for legitimate purposes as determined by a court of competent jurisdiction, or other lawful authority. The Bill does not provide independent monitoring of the law enforcement agencies carrying out the provisions, nor does the Bill define 'law enforcement agency' or 'lawful authority.' Finally the Bill does not distinguish between serious offenses and emergencies or minor misdemeanours. As a result it may conflict with Article 37 of Nigeria's Constitution, which guarantees the privacy of citizens including their homes and telephone conversations, absent a threat on national security, public health, morality, or the safety of others.

(E) AFF and other Fraud Related Offences Act 2006

Another relevant legislative measure in the fight against advance fee fraud on the Internet is the Advance Fee Fraud and other Fraud Related Offences Act 2006. This is a replacement of an Act of the same title passed in 1995. The act prescribes, among others, ways to combat cybercrime and other related online frauds. The Act provides for a general offence of fraud with several ways of committing it, which are by obtaining property by false pretence, use of premises, fraudulent invitation, laundering of fund obtained through unlawful activity, conspiracy, aiding, etc. Section 2 makes it an offence to commit fraud by false representation. Subsection (2)(a) and (2)(b) makes clear that the representation must be made with intent to defraud. Section 3 makes it an offence if a person who is being the occupier or is concerned in the management of any premises, causes or knowingly permits the premises to be used for any purpose which constitutes an offence under this Act. This section provides that the sentence for this offence is the imprisonment for a term of not less more than 15 years and not less than five years without the option of a fine.

Section 4 refers to the case where a person who by false pretence, and with the intent to defraud any other person, invites or otherwise induces that person or any other person to visit Nigeria for

any purpose connected with the commission of an offence under this Act. The sentence for this offence is the imprisonment for a term not more than 20 years and not less than seven years without the option of a fine.

According to section 7, a person who conducts or attempts to conduct a financial transaction which involves the proceeds of a specified unlawful activity with the intent to promote the carrying on of a specified unlawful activity; or where the transaction is designed to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of a specified unlawful activity is liable on conviction to a fine of N l million and in the case of a director, secretary or other officer of the financial institution or corporate body or any other person, to imprisonment for a term, not more than 10 years and not less than five years.

However, while in previous laws the onus was on the government to carry out surveillance on such crimes and alleged criminals, the new law vests this responsibility on industry players, including ISPs and cybercafé operators, among others. While the Economic and Financial Crimes Commission (EFCC) becomes the sub-sector regulator, the Act prescribes that henceforth, any user of Internet services shall no longer be accepted as anonymous. Through what has been prescribed as due care measure, cybercafés operators and ISPs will henceforth monitor the use of their systems and keep a record of transactions of users (Adomin, 2008, p.290). These details include, but are not limited to, photographs of users, their home address, telephone, email address, etc. So far, over 20 cybercafés have been raided by the EFCC as of August 7, 2007. The operators appear set to comply with the law by notifying users of the relevant portion of the law, corporate user policy, firewall recommendation, protection procedure, indemnity and right of disclosure, and so forth (Adomin, 2008, p.290).

5.2 Administrative Measures

Administrative measures chiefly involve the setting-up of special bodies by the Nigerian government to combat advance fee fraud. Equally important, however, are the technical measures which these bodies then take to prevent and/or prosecute this activity, and these will also be examined below. It must be emphasised that many European countries have established special computer units to take specific measures against cybercrime. The following are some examples of these bodies:

(A) The Economic and Financial Crimes Commission (EFCC)

The Economic and Financial Crimes Commission (EFCC) is a Nigerian law enforcement agency that investigates financial crimes such as advance fee fraud (419 fraud) and money laundering (Online Wikipedia). The EFCC was established in 2003, partially in response to pressure from the Financial Action Task Force on Money Laundering (FATF), which named Nigeria as one of 23 countries non-cooperative in the international community's efforts to fight money laundering. EFCC is an inter-agency Commission comprising a 22-member Board drawn from all Nigerian Law Enforcement Agencies (LEAs) and Regulators. The Commission is empowered to investigate, prevent and prosecute offenders who engage in *'money laundering, embezzlement, bribery, looting and any form of corrupt practices, illegal arms deal, smuggling, human trafficking, and child labour, illegal oil bunkering, illegal mining, tax evasion, foreign exchange*

malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes, and prohibited goods' (Ribadu, 2006, p. 4).

The Commission is also responsible for identifying, tracing, freezing, confiscating, or seizing proceeds derived from terrorist activities. EFCC is also host to the Nigerian Financial Intelligence Unit (NFIU), vested with the responsibility of collecting suspicious transactions reports (STRs) from financial and designated non-financial institutions, analyzing and disseminating them to all relevant Government agencies and other FIUs all over the world (Ribadu, 2006, p. 4). In addition to any other law relating to economic and financial crimes, including the criminal and penal codes, EFCC is empowered to enforce all the pre- 1999 anti-corruption and anti-money laundering laws. Punishment prescribed in the EFCC Establishment Act range from combination of payment of fine, forfeiture of assets and up to five years imprisonment depending on the nature and gravity of the offence (Ribadu, 2006, p. 4). Conviction for terrorist financing and terrorist activities attracts life imprisonment. It must be mentioned that EFCC has excellent working relationship with major Law Enforcement Agencies all over the world (Ribadu, 2006, p. 8). These include the INTERPOL, the UK Metropolitan Police, FBI, Canadian Mounted Police, the Scorpions of South Africa, etc.

(B) Nigerian Financial Intelligence Unit (NFIU)

In 2005, the EFCC established the Nigerian Financial Intelligence Unit (NFIU). The NFIU draws its powers from the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission Act of 2004. It is the central agency for the collection, analysis and dissemination of information on money laundering and terrorism financing. All financial institutions and designated non-financial institutions are required by law to furnish the NFIU with details of their financial transactions. Provisions have been included to give the NFIU power to receive suspicious transaction reports made by financial institutions and non-designated financial institutions, as well as to receive reports involving the transfer to or from a foreign country of funds or securities exceeding $10,000 in value (International Narcotics Control Strategy Report, 2006, p. 2). The NFIU is a significant component of the EFCC. It complements the EFCC's directorate of investigations but does not carry out its own investigations. It is staffed with competent officials, many with degrees in accounting and law (International Narcotics Control Strategy Report, 2006, p. 2).

The NFIU is playing a pivotal role in receiving and analyzing STRs. As a result, banks have improved their responsiveness to forwarding records to the NFIU (International Narcotics Control Strategy Report, 2006, p. 2). Under the EFCC act, whistle-blowers are protected. Nigeria has no secrecy laws that prevent the disclosure of client and ownership information by domestic financial services companies to bank regulatory and law enforcement authorities (International Narcotics Control Strategy Report, 2006, p. 2). The NFIU has access to records and databanks of all government and financial institutions, and it has entered into memorandums of understandings (MOUs) on information sharing with several other financial intelligence centres. The establishment of the NFIU is part of Nigeria's efforts toward removal from the NCCT list (International Narcotics Control Strategy Report, 2006, p. 3).

(C) Nigerian Cybercrime Working Group (NCWG)

The NCWG is an inter-agency body comprising law enforcement, intelligence, security as well as ICT agencies of Government and key private sector ICT organizations (NCWG website, 2008). It was established by the Federal Executive Council (FEC) on the recommendation of his Excellency President of Nigeria on March 31 2004. The group was created to deliberate on and propose ways of tackling the malaise of Internet 419 in Nigeria. This includes (NCWG website, 2008):

- Educating Nigerians on cybercrime and cybersecurity;
- Undertaking international awareness programs for the purpose of informing the World of Nigeria's strict Policy on Cybercrime and to draw global attention to the steps taken by the Government to rid the country of Internet 419 in particular and all forms of cybercrimes;
- Providing legal and technical assistance to the National Assembly on cybercrime and cybersecurity[12] in order to promote general understanding of the subject matters amongst the legislators;
- Carrying out institutional consensus building and conflict resolutions amongst law enforcement, intelligence and security Agencies in Nigeria for the purpose of easing any jurisdictional or territorial conflicts or concerns of duties overlap;
- Reviewing, in conjunction with the Office of the Attorney General of the Federation, all multilateral and bilateral treaties between Nigeria and the rest of the World on cross-border law enforcement known as Mutual Legal Assistance Treaties (MLAT), for the purpose of amending the operative legal framework to enable Nigeria secure from, as well as render, extra-jurisdictional assistance to its MLAT Partners in respect of cybercrime.

5.3 Technical Measures

Criminals are often quicker to exploit new technologies than law-enforcers who, to some extent, always seem 'behind the game'. In order to salvage Nigeria from the negative consequences of cyber crime, the government has been making frantic efforts to ensure that this malaise is nipped in the bud. These efforts are discussed below:

(A) Regulation of Cybercafés

Cybercafé also known as internet cafe or PC cafe is a place where internet public access services are provided by entrepreneurs for a fee (Adomi, 2007). While in the USA and Western Europe,

[12] The main goal of Internet security is to keep proprietary information confidential, to preserve its integrity, and to maintain its availability for those authorized to view that information. When information is accessed and examined by unauthorized individuals, it is no longer confidential.. If data are tampered with, modified, or corrupted by intruders there is a loss of information integrity. Sometimes this can happen inadvertently, but most often it is the intentional act of a hacker or a disgruntled employee seeking revenge. If information is deleted or becomes inaccessible to authorized users, there is a loss of availability. Spinello, R (2002), Regulating Cyberspace: The Policies and Technologies of Control (U.S.A.: Spinello), 207.

the term cybercafe refers often to true cafes offering both internet access and beverages, in Nigeria and other parts of Africa, cybercafes can refer to places offering public internet access in places like restaurants or hostels, or they are locations that are wholly set aside for public access internet services (Adomi, 2007). Cybercafés in Nigeria render overnight browsing, a special internet service is offered by cybercafes from 10.00 p.m. to 6.00 a.m. This service allows users who have a lot to obtain from the net to do so at a minimal cost (Adomi, 2007).

Though overnight browsing is very important and useful to cybercafe users, it was banned by the EFCC and the Association of Cybercafe and Telecentres Owners (ATCON) in Nigeria (Adomi, 2008).The ban is coming on the heels of several attempts by the EFCC to arrest the ugly trend through raids, arrests, and precautions of cybercafes and cyber criminals as a result of the constant embarrassment posed to the Nigerian Federal Government by their nefarious activities. Some Nigerian fraudsters have perfected the act of using the internet via cybercafes as their criminal platform to dupe unsuspecting citizens across the globe (Adomi, 2008). This ban on night browsing is likely to negatively affect clients who use the cafes for academic and other useful and positive purposes in night browsing sessions. Other decisions of EFCC and ATCON reached to combat cyber crime include (Adomi, 2008):

- Undertaking international awareness programs for the purpose of informing the World of Nigeria's strict Policy on Cybercrime and to draw global attention to the steps taken by the Government to rid the country of Internet 419 in particular and all forms of cybercrimes;
- That each sector of the telecom industry, namely the global system for mobile communication operators, private telecomm operators and cybercafes should come up with a due care document that would be a standard guide and proffer measures for the effective policing of cyber crime in Nigeria;
- That all cyber cafes must be registered with the Corporate Affairs Commission, NCC and EFCC;
- That cybercafes will now be run on membership basis instead of pay-as-you-go;
- All cybercafes must install acceptable hardware surveillance;
- The architecture of cyber cafes must be done such that all computers are exposed;
- ATCON members must subscribe to registered and licensed ISP in the country;
- Each cybercafe is expected to be a watchdog to others, as they have been detailed to have direct access to EFCC (Adomi, 2008).

(B) Government Partnership with Microsoft

The Government of Nigeria and Microsoft Corp signed a Memorandum of Understanding defining a framework for co-operation between Microsoft and the Economic and Financial Crimes Commission (EFCC) of Nigeria with the aim of identifying and prosecuting cyber criminals, creating a safe legal environment and restore hundreds of millions of dollars in cost investment. This agreement is the first of its kind between Microsoft and an African government and will give the EFCC access to Microsoft technical expertise information for successful enforcement. The Memorandum combats issues such as spam, financial scam, phishing, spyware, viruses, worms, malicious code launches and counterfeiting. Microsoft is expected to instruct Nigerian investigators on techniques of extracting useful information from PCs

compromised by botnet attacks, how to monitor computer network to detect such attacks, and how to identify the people behind them. Microsoft will also provide leads on spam emanating from Nigeria, enabling the authorities to pursue investigations more quickly and successfully (Adomi, 2008). Microsoft is known for conducting a worldwide analysis of spam sent to e-mail accounts that it establishes and monitors for this purpose (Adomi, 2008).

(C) ADNET

ADNET is a computer network with powerful capabilities for the storage and retrieval of data concerning Nigerian crime (Buchanan, 2001, p.43). ADNET is a secure system and can be accessed through dedicated ADNET terminals in the task force cities. In conjunction with the NCI working group, an outside private contractor trains and provides support to investigators working Nigerian crime cases (Buchanan, 2001, p.43). ADNET terminals are also located in Lagos, Nigeria and Accra, Ghana, so that data can be accessed close to sources of much of the Nigerian crime activities. Several federal law enforcement agencies contribute and access ADNET data. In the last two years the number of records in the NCI database has increased dramatically, making the network a potentially valuable resource to law enforcement. Some of this data consists of information collected from prior criminal investigations, including aliases used by persons involved in Nigerian criminal activities (Buchanan, 2001, p.43).

6. The Quest for Legislative Harmonisation

Considerable differences still exist in legislative responses to advance fee fraud. Despite common legal histories, there are differences in the definition of crimes, the penalties applicable to forms of these crimes and the extent of criminalization. Although these differences reflect the position of criminal law general in each country, there is increasing recognition that legislative differences can impede effective law enforcement with the international nature of much advance fee fraud. In this regard, governments must provide for:

- Effective criminalization of cyber – offences. The legislation of different countries should be as harmonized as possible.
- Conditions facilitating direct cooperation between State institutions, as well as between State institutions and the private sector.
- Investigative procedures and institutional capacities which allow criminal justice agencies to cope with advance fee fraud.

The 'Budapest' Convention on Cybercrime (ETS 185) of the COE helps countries to respond to these needs. It is thus imperative that countries ratify this Convention since it is an effective tool for counter action. What is needed is close co-operation and co-ordination and also harmonised arrangements for effective prosecution of transnational criminals. As noted in the 2003 Council of Europe report, effective law enforcement requires 'sufficient resources to finance law enforcement units trained and dedicated to fight cybercrimes'.[13] The development of methods and tools to provide information and assistance for victims of advance fee fraud by NGOs and other agencies active in the field of cybercrime must be supported.

[13] 2003 Report, 75.

7. Future Trends

Further research is needed on other unexplored areas of Internet based fraud, e.g. matrimonial web sites, where the Internet is likelier to be used to attract victims, or facilitate transactions with them. Prospects for co-operation with computer experts, and businesses which operate Internet gateways should be explored. There are already examples of codes of conduct, which have been introduced online to tackle the problem of cybercrime and advance fee fraud. A self-regulation system should also be introduced. Self-regulation is based on three key elements: first, involvement of all interested parties (government, user associations, and access providers) in producing new strategies; secondly, implementation of these strategies by the party concerned; thirdly, evaluation of the measures taken. Self-regulation can be backed by clear legal regulation and this is what the term 'co-regulation' means. A co-regulatory system is one in which the public authorities accept that protection of the society can be left to self -regulatory schemes, but reserve the right to intervene, if self-regulation fails to work.

For the purpose of prosecuting advance fee fraud scammers, we should use: local, regional and national co-ordination and information sharing mechanisms; national liaison officers posted overseas or links with liaison officer networks; Europol and its Liaison Bureaux; Interpol's National Contact Bureaux; Eurojust; and direct bi-lateral contacts. Channels that already exist for other purposes should be activated and adapted. Finally, we need to make the laws more effective by improving the quality of criminal codes and increasing the penalties to match the seriousness of loss. Laws will be effective against scammers who are deterred by criminal law and frightened by the prospect of incarceration; however, there will always be scammers who are motivated to engage in online fraud to overcome these laws and the efforts of the criminal justice community.

8. Conclusion

Cyberspace is still very largely *terra incognita*, and that leaves plenty of scope for criminal activity. It should be noted that technology is truly a double-edged sword that has transformed the classical and traditional forms of criminal behaviour. The proliferation of ICTs and progressive development in digital transactions and communications have created new opportunities and opened up new windows which have resulted in the emergence of new forms of criminal behaviour and cybercrime. On such a basis, advance fee fraud ranks amongst the most important and virulent forms of cybercrime; not only due to its adverse impact on the development of cyberspace but also due to the diversity of means and methods that could be utilized in committing this crime as well as the inherent risk of using advance fee fraud as a leeway and instrument to commit other crimes using the stolen identities of victims. Furthermore, advance fee fraud could have a devastating impact on the financial security and credit scoring of victims. Being aware of the potential and actual risks associated with this serious exploitation of ICTs, the author has, throughout this article, attempted to provide a comprehensive overview of the fundamental issues and potential solutions pertinent to this form

of criminal behaviour. Largely, it is submitted that advance fee fraud should be subject to a global principle of public policy that aims at combating and preventing this form of organized crime through raising global awareness, increasing literacy rates, coordinating legislative efforts on national, regional and global levels, establishing a high level global network of cooperation between national, regional, and international enforcement agencies and police forces.

References

Books

Bocij, P (2006), The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals (Westport: Praeger Publishers).

Chawki, M (2008), Combattre la Cybercriminalité (Perpignan: Editions de Saint Amans).

Igwe, C (2007), Taking Back Nigeria from 419: What to do about the Worldwide E-mail Scam - Advance Fee Fraud (Bloomington: iUniverse).

Milhorn, T (2007), Cybercrime: How to Avoid becoming a Victim (Boca Raton: Universal Publishers).

Ogunjobi, T (2008), Scams and How to Protect Yourself (Morrisville: Lulu).

Smith, R, Grabosky, P and Urbas, G (2004), Cyber Criminals on Trail (Cambridge: Cambridge University Press).

Tive, C (2006), 419 Scam: Exploits of the Nigerian Con Man (Bloomington: iUniverse).

Van der Merwe, D, Roos, A, Pistorius, T, and Eiselen, S (2008), Information and Communications Technology Law (Durban: LexisNexis).

Wall, D (2007), Cybercrime: The Transformation of Crime in the Information Age (Cambridge: Polity Publishers).

Weisman, S (2008), The Truth about Avoiding Scams (Saddle River: FT Press).

Yar, M (2006), Cybercrime and Society (Thousand Oaks: Sage Publications).

Thesis

Champy, G (1990), La Fraude Informatique (Aix – en - Provence, University of Aix-Marseille III).

Chatarodjana, C (1997), Preuve Informatique en Matière d'Acte Juridique: Une Etude Comparative des Systems Français et Quebecois (Quebec, University Laval).

Chawki, M (2006), Le Droit Penal à l'Epreuve de la Cybercriminalité (Lyon, University of Lyon III).

Daragon, E (1996), Droit de la Preuve et Informatique (Grenoble, University of Grenoble I).

Frydlender, A (1985), La Fraude Informatique, Etude Phénoménologique et Typologique Appliquée au Contexte Français (Paris, University of Paris 9).

Maat, S (2004), Cybercrime: A Comparative Law Analysis (Pretoria, University of South Africa).

Nadine, A (1994), Les Infractions Pénales Favorisées par l'Informatique (Montpellier, University of Montpellier 1).

Tenfa, D (2006), Advance Fee Fraud (Pretoria, University of South Africa).

Journal Articles

Adomi, E (2008), 'Combating Cybercrime in Nigeria', 26(5) The Electronic Library.

Adomi, E (2007), 'Overnight Internet Browsing Among Cybercafe Users in Abraka, Nigeria', 3(2) Journal of Community Informatics.

Brenner, S (2004), 'Cybercrime Metrics: Old Wine, New Bottles', 9 Virginia Journal of Law and Technology, 6.

Chawki, M (2005), 'A Critical Look at the Regulation of Cybercrime', IV(4) The ICFAI Journal of Cyberlaw.

Chawki, M (2006), 'Anonymity in Cyberspace: Finding the Balance between Privacy and Security', *Revista da Faculdade de Direito Milton Campos*.

Chawki, M and Wahab, M (2006), 'Identity Theft in Cyberspace: Issues and Solutions', 11(1) LexElectronica.

Chukwuemerie, A (2006), 'Nigeria's Money Laundering (Prohibition) Act 2004: A Tighter Noose', 9(2) Journal of Money Laundering Control.

Goodman, M and Brenner, S (2002), 'The Emerging Consensus on Criminal Conduct in Cyberspace', 6(1) UCLA Journal of Law and Technology.

Holt, T and Graves, D (2007), 'A Qualitative Analysis of Advance Fee Fraud Email Schemes', 1(1) International Journal of Cyber Criminology.

Hunter, D (2003), 'Cyberspace as Place and the Tragedy of the Digital Anti Commons', 91(2) California Law Review.

Oriola, T (2005), 'Advance Fee Fraud on the Internet: Nigeria's Regulatory Response', 21(3) Computer Law & Security Review.

Longe, B and Chiemeke, S (2008), 'Cybercrime and Criminality in Nigeria: What Roles are Internet Access Points in Playing', 6(4) European Journal of Social Sciences.

Treaties

Council of Europe Convention on Cybercrime, ETS No. 185, 2001.

Statutes

Advance Fee Fraud and other Fraud Related Offences Act, 2006.
Computer Security and Critical Information Infrastructure Protection Bill, 2005.
Economic and Financial Crimes Commission Act, 2004.
Money Laundering (Prohibition) Act, 2004.
Advance Fee Fraud Decree 1995.

Reports

Breton, T (2005), Chantier sur la Lutte contre la Cybercriminalité, (Paris: French Ministry of Interior).

CLUSIF (2008), Cybercrime Overview 2007, (Paris: CLUSIF).

Fafinski, S and Minassian, N (2008), UK Cybercrime Report 2008, (New York: Garlik).

US Department of State (2008), Money Laundering and Financial Crimes Report, Vol. II, (Washington, DC: US Department of State).

US Department of State (2007), International Financial Scams Report, (Washington, DC: US Department of State).

US Department of State (2006), International Narcotics Control Strategy Report, (Washington, DC: US Department of State).

Internet Sources

Barlow, J 'A Declaration of the Independence of Cyberspace', Electronic Frontier, February 8, 1996. <http://homes.eff.org/~barlow/Declaration-Final.html>

Conference Proceedings

Reich, P (2004), 'Advance Fee Schemes in Country and Across Borders', Proc. Crime in Australia: International Connections, conference organized by Australian Institute of Criminology, Melbourne, Australia.