Legal Framework for the Regulation of Electronic Frauds in Nigeria

Festus O. Ukwueze and Uju Obuka *

1. Introduction

Advancements in Information Communication Technology (ICT) have not only made lives easier for humanity but have dramatically changed the way human beings live by almost totally obliterating the difficulties posed distance in space and even time. People are now able to transact businesses from the comfort of their homes; work and be paid electronically; have their ailments diagnosed and receive medical prescriptions without visiting a doctor's clinic and even engage in leisure activities using all manner of electronic equipment. ICT has enabled people to communicate more effectively and at lower cost over long distances without the inhibition imposed by geographical boundaries. This has enormously enhanced the process of globalization of economic and social life.

The first set of institutions to embrace this technological innovation in their dealings in the 80s were banks and other financial institutions in Europe and the Western World which started using ATM[1] and magnetic stripe cards to provide account systems.[2] Nigeria has joined the rest of the world in the use of ICT in banking and other spheres of business and social life. Banks, schools, financial institutions, hospitals and government departments now heavily utilize information technology in their operations. This same technology that has provided so many benefits has, however, created enormous opportunities for offenders who are able to communicate

---

* Festus O. Ukwueze, LL.M. BL, pnm: Lecturer, Faculty of Law, University of Nigeria, Enugu Campus; E-mail: festus.ukwueze@unn.edu.ng; Website: http://www.unn.edu.ng and Uju Obuka, LL.M. BL., Lecturer Faculty of Law, University of Nigeria, Enugu Campus; E-mail: uju.obuka@unn.edu.ng. Website: http://www.unn.edu.ng .

1 ATM is the acronym for Automated Teller Machine.

2 See A. L. Ajayi: "Legal Framework for Handling ATM and Other Electronic Frauds" *The Nigerian Banker,* April – June 2010, pp. 26 – 41. available online at www.cibng.org/admin/ publications/Nigeria%20Banker%20April%20 June%202% 20 2010.pdf; last accessed on 12/3/11.

with each other in secret, disguise their identities in order to avoid detection and manipulate electronic payment systems to obtain funds illegally. The risk of fraud is one of the principle barriers to electronic transactions. This therefore requires that adequate mechanisms, legal and otherwise, be put in place to balance and handle issues and challenges of the emerging electronic market place.

This paper therefore examines the current legal framework for the regulation of electronic frauds in Nigeria. Electronic frauds, no doubt, are corollaries of electronic transactions. The diverse forms of electronic transactions will be highlighted in order to identify the multifarious nature of frauds associated with such transactions. After highlighting the legal issues associated with e-transaction, relevant Nigerian statutes dealing with electronic fraud will be analysed to determine their adequacy or inadequacy taking into cognizance the position in some other jurisdictions. Recommendations will be made on how to improve observed shortcomings in the applicable statutes as well as new areas of legal intervention required to enable the country keep up with the dynamics of modern ICT.

2. Electronic Transactions in Nigeria

Traditionally, businesses were conducted by physical contact between the contracting parties and payment for such goods and services were effected by barter system and later by the use of monetary instruments in the form of cash, cheque, money order, etc. In the past few years, business activities globally have largely depended on the deployment of information and communications technology. Many people have taken to on-line business transactions in one way or the other even without knowing it.[3] Some are already living a web lifestyle. People who do not have their businesses on-line at least use e-mail facilities, do on-line transactions or get on-line to search for one information or the other.[4]

Improvements in ICT, especially the rapid advances in the use of the internet, improved production capabilities, demanding customers and accelerated flow of capital across political boundaries

---

3 A.S Adepoju and M.E Alhassan: "Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria- A Case Study of Selected Banks in Minna Metropolis" *Journal of Internet Banking and Commerce*, August 2010 Vol. 15 No. 2.

4 *Ibid.*

create business opportunities and fuel competitions as well.[5] The use of information and communication technology in business has enabled customers to pay for goods and services, withdraw or transfer funds anywhere in the world. Similarly, this new technology has facilitated the process of buying and selling over electronic lines both locally and globally culminating in what has come to be known as electronic commerce.[6]

Electronic commerce was actually what prompted electronic banking all over the world. Electronic commerce has revolutionized commercial undertakings globally. This revolution requires a corresponding payment system that can equalize the emerging phenomena. Electronic banking is one area of e-commerce that has proved successful in Nigeria.[7] Customers' insatiable appetite for efficient services has compelled financial institutions to fast-forward to a more radical transformation of their business systems and models by embracing e-banking.[8] Nigerian banks and other financial institutions are seriously into new electronic delivery channels for banking products and services with a view to delivering better services and satisfying customers the more.

Electronic transaction is fast growing and the global penetration has necessitated the need for improvement, and the success of the system depends on efficient and trustworthy data communication device that is ever ready to meet the challenges or demands of the emerging electronic market place. It was in a bid to keep abreast with advancements in technology and improve the quality of their services to the teeming Nigerian populace that propelled Nigerian banks to invest so much on technology and widely adopt electronic networks in their services. They have actually digitalized all their services. According to Ezeoha,[9] the hype of e-

---

5 Ajayi, *loc. cit.* Note 2 above.

6 *Ibid.*

7 *Ibid.*

8 J. Ovia: "Internet Banking, Practices, and Potentials in Nigeria" available at www.zenithbank.com/internet-practices, accessed on 23/2/2011.

9 Ezeoha, E- Banking, quoted in Adepoju and Alhassan, *loc. cit*. Note 3 above.

commerce, e-banking and e-everything is gradually being embraced by Nigerian financial institutions who are poised to be in the vanguard of narrowing the digital divide.

The evolution of information and communications technology has thus given rise to electronic means of doing business. As the technology develops, the range of devices and processes used to transact business electronically continues to increase while the percentage of cash and cheque transaction continues to decrease. The internet has the potential of becoming the most active trade intermediary in no distant time. Internet or on-line shopping has revolutionized retailing by allowing consumers to sit in their homes and buy an enormous variety or products and services from all over the world.

Competition, innovation and investment in hi-tech communications and information technology equipment have almost rendered obsolete traditional ways of doing business.[10] Modern ICT's innovations in the manner of doing business include:

2.1 Buying and Selling of Goods and Services

The recent trend in information technology has moved businesses from the usual brick and mortar environment to an electronic platform where businesses are consummated without physical contact between the contracting parties. E-commerce commonly consists of the buying and selling of products or services over electronic systems such as the internet and other computer networks. The amount of trade conducted via electronic means has increased tremendously with widespread internet usage. There are so many types of businesses that can be conducted electronically namely: business to business which is electronic commerce that is conducted between businesses and is accessible to all the contracting parties. Secondly, there is the business to consumer type of electronic commerce which is that type of electronic commerce that is conducted between businesses and consumers. In this type of e-commerce, the consumer has direct access to the seller usually through the internet.

---

[10] Babalakin: "Cybernetic Banking (Changing the Banking Landscape in Nigeria)" available at www.babalakinando. com. 2002 accessed on 12/3/2011.

Electronic commerce is one of the newest and fastest developing business environments. So many advantages are associated with e-commerce the greatest being that businesses are able to reach out to larger markets at relatively lower costs than traditional mode of doing business and a lot of time is saved unlike in traditional mode of buying and selling.

This same technology that has provided many benefits has however created enormous opportunities for economic offenders to manipulate electronic payment systems to obtain funds, goods and services illegally. The risk of fraud is one of the principal obstacles to electronic commerce being widely accepted especially in a developing nation like Nigeria where e-commerce activities is relatively low.

2.2 Payment Systems

The emergence of e-commerce has created new financial needs that in many cases cannot be effectively fulfilled by the traditional payment systems.[11] This has resulted in all the stake holders exploring various types of electronic payment system to match the emerging electronic environment. As payment is an integral part of every business, so is electronic payment an integral part of e-commerce because it enables consumers to pay for goods and services electronically.

The complex nature of e-commerce has given rise to different electronic payment systems. Some electronic payment systems are simply electronic version of existing payment systems such as cheque and credit cards while others are based on the digital currency technology and have the potential for definitive impact on today's financial and monetary system.[12]

In its generic sense, electronic payment encompasses all payment made to businesses, banks, or organizations which are executed using electronic medium. The first type of electronic payment system to be concluded in 1960 was the Electronic Fund

---

11 S. Sumanjeet: "Emergence of Payment Systems in the Age of Electronic Commerce: The State of the Art," *Global Journal of International Business Research,* Vol. 2, No. 2, 2009.

12 *Ibid.*

Transfer (EFT) which is a technology that allows the transfer of funds from the bank account of one person or organization to that of another. The rapid growth of e-commerce in the last few years has resulted to the emergence of different electronic payment systems. According to Anderson,[13] there are basically, four types of electronic payment systems namely, online credit card payment system, electronic cheque system, electronic cash system and smart card based electronic system.

(a) Online Credit Card Payment System

This type of electronic payment system very closely resembles the traditional credit card but further seeks to extend the functionality of existing credit cards for use as online shopping payment tools. This payment system is by far the most widely used and has been widely endorsed by vendors and consumers alike. The greatest advantage associated with this type of electronic payment system is its time effectiveness.

(b) Electronic Cheque Payment System

This type of electronic payment system is used widely around the world replacing the need of traditional paper cheques. It functions just the same way as the conventional cheque but it has an advantage over the conventional paper cheque in that it does not require consumers to continually send sensitive financial information over the web and they are much faster than paper based traditional cheque.

(c) Electronic Cash Payment System (e-cash)

E-cash is a new concept in online payment because it combines computerized convenience with security and privacy that improve on paper cash. The convenience and low transaction cost that this type of electronic payment system has makes it an attractive payment system to use online. But it is highly susceptible to forgery as it is relatively easy to create and use e-cash unlike other electronic payment systems.

(d) Smart Cards Based Electronic Payment System

---

13 Anderson, "Electronic Payment System" quoted in Sumanjeet, *loc. cit.*, note 11 above at p.18.

This type of electronic payment system has become widely recognized in many areas of the e-business. They have all the qualities of credit card and in addition have microprocessors which store far greater information than credit cards and have more security features when compared to credit card and electronic cash. Because of the encrypted information of smart cards, they are proven to be one of the most secured ways of doing online business.

2.3 Electronic Banking

Banking has indeed come a long way from the time of ledger cards and other manual filling systems to electronic means of payment. Most banks today have electronic systems to handle their daily voluminous task of information retrieval, storage and processing irrespective of whether they are automated or not. Banking today has gone beyond routine storage and retrieval of information.

The technological revolution world-wide has positively affected banking practices and customers are spoilt for choice between the different electronic payment services now available.[14] Electronic banking generally refers to the use of information and communication technology by banks to provide services and manage customer relationship more quickly and most satisfactorily.[15] The global and competitive nature of the economy has propelled banks to continue to strive for new innovations to remain afloat in business. This invasion of banking by technology has rendered banking services more appealing.[17] The click of a mouse today offers bank customers services at a much lower cost and also empowers them with unprecedented freedom in choosing vendors for their financial needs.[16] One of the benefits banks derive from electronic banking products and service delivery is improved efficiency and effectiveness on their operations so that more transactions can be

---

14 Babalakin, *loc., cit*. Note 10 above.

15 A. B. Dogarawa. "The impact of E-banking on Customer Satisfaction in Nigeria" available at www.mpra.ub.uninuen- chen.de/23200IMPRA accessed on 14/2/2011.

17 *Ibid.*

16 *Ibid.*

processed faster and most conveniently which will undoubtedly impact significantly on the overall performance of the banks.[17] On the side of customers, they stand to enjoy quick service delivery reduced frequency of going to banks physically and reduced cash handling which will give rise to higher volume of turnover.

Electronic banking could come in the following variants: internet banking, telephone banking, television based banking, mobile phone banking, PC[18] banking and ATM. All these devices enable customers to perform banking transactions electronically without visiting financial institutions.

3. Nature and Types of Electronic Fraud

There have been debates about whether unlawful activities involving computers and the internet should be classified as crimes or civil wrongs.[19] Literally, the term "fraud" means "Deception in order to gain by another's loss; craft; trickery; guile[20]...deceit, impersonation with intent to deceive...deception done with the intention of gaining an advantage; a snare; deceptive trick; a cheat or swindler."[21]

This is akin to the meaning of the term in law which connotes any artifice or deception practised to cheat, deceive, or circumvent another to his detriment. The authors of a widely used law dictionary define the term comprehensively thus:

> 1. A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment. Fraud is usually a tort, but in some cased (especially when the conduct is wilful) it may be a crime....

---

17 *Ibid.*

18 Person Computer.

19 P. Barton and V. Nissanka: "Cyber-crime--Criminal Offence or Civil Wrong?" (2003) *Computer Law and Security Report* , Vol. 19. No. 5, p. 401.

20 See, *The New International Webster's Comprehensive Dictionary of the English Language*, Encyclopaedic edition, 2004, p. 502. *The Chambers Dictionary,* New edition, 1998, p.636.

21 *The Chambers Dictionary,* New edition (New Delhi: Allied Chambers Ltd., 1998) p. 636.

2. A misrepresentation made recklessly without belief in its truth to induce another person to act.

3. A tort arising from a knowing misrepresentation made to induce another to act to his or her detriment.

4. Unconscionable dealing; especially in contract law, the unfair use of the power arising out of the parties' relative positions and resulting in an unconscionable bargain.[22]

Fraud therefore is essentially a civil wrong but will constitute a crime where the fraudulent act or omission in question has been prohibited by a penal statute. This is consistent with the constitutional provision that no person shall be convicted of an offence unless that offence is defined and the penalty therefore is prescribed in a written law.[23] Although electronic frauds are usually referred to as offences or crimes,[24] there is no doubt that unless a particular act constituting fraud has been prohibited by a penal statute, such an act will remain within the realm of civil wrong. However, because electronic fraud is usually committed by persons who may not be in geographical proximity with the victim (in fact the perpetrator and the victim may not even be in the same continent) makes resort to civil action based on the tort of deceit or fraudulent misrepresentation in contract to redress it very inappropriate. It is usually carried out furtively such that even where the perpetrator and the victim are within the same legal jurisdiction, the victim might not have adequate technical know-how and resources necessary to carry out the sort of investigation that would identify the perpetrator. This makes resort to public law, criminal law in particular, more appropriate in dealing with same.

---

22 B. A. Garner (ed.), *Black's Law Dictionary,* (8th edn.) (West Minn.: West-Thompson, 2004), p. 685.

23 See Section 36 (12), Constitution of the Federal Republic of Nigeria, 1999 (as amended). See also the case of *Aoko v Fagbemi* (1963) All NLR 400.

24 See Ajayi, *loc. cit.* Note 2 above.

Electronic fraud is fraud committed by electronic means, usually in the course of electronic transaction. Commonest means of electronic transaction in Nigeria is the internet, through e-mails or websites. It includes electronic banking (e-banking) and payment by electronic means of money transfer (e-payment). All these means are often commonly referred to as electronic commerce (e-commerce). Electronic fraud is a term used to describe conducts or acts where computers or other electronic devices are utilised in some manner to facilitate the commission of offences or other forms of the breach of law.

The common forms of electronic fraud in this country include electronic card fraud (including credit card and ATM frauds), advance fee schemes, electronic auction or retail-based fraud schemes, stock scams, computer hacking, offensive, menacing or harassing mails. Electronic card fraud is characterised by unauthorised withdrawal or transfer of funds from someone's bank account. It includes unauthorised access to banks account and other confidential information through internet banking facilities, with customers' passwords and User ID[25] being extracted by hackers and subsequently used for perpetration of fraud. In the case of a credit card account this may involve unauthorised use of the card details, usually obtained fraudulently, to spend money from the account. For ATM accounts it involves withdrawal of money from the account from a cash point without the consent of the account holder. ATM fraud can take various forms including card skimming, where the card's magnetic stripe details and PIN[26] are captured at the ATM by a modified card reader known as skimming device. The captured details are then used to produce a counterfeit card for subsequent fraudulent cash withdrawals from the account. The account details and PIN can also be obtained through the use of fake ATM machines placed in a public place. Such a machine will not dispense cash and will continually show operational error yet all the cards used on it are copied.

Other forms of ATM fraud include card capture, distraction, shoulder surfing, cash trapping network attack on ATMs, viruses and malicious softwares and phishing (same messages designed to entice

---

25 User Identity.

26 Personal Identification Number.

a user to provide his or her personal details). Scammers can clone the home pages of companies and other organisations such as banks and government agencies[27] and use such to obtain personal details of a prospective victim.

Advance fee schemes involve fraudsters sending scam mails to prospective victims. These messages are often referred to as "Nigerian" or "419" scams because the e-mails often come from individuals who claim to reside in a foreign country such as Nigeria or other African nations.[28] 419 is a reference to section 419 of the Nigerian Criminal Code Act[29] which deals with obtaining property by false pretence. So much has been written about the bad image and unpleasant reputation which incidents of cyber-based fraud has brought to this country that it will serve no useful purpose revisiting the wealth of literature on the subject.[30] The scammers usually seek to lure the recipient by claiming to need assistance in transferring large sums of money out of the country. In return, the sender will share a portion of the sum with the individual who aids them. The allurement usually manifests by the sender posing as a public official

---

27 See the case of *Mike Amadi v Federal Republic of Nigeria (*Unreported) judgement of the Court of Appeal (Lagos Judicial Division), Appeal Case No: CA/L/389/2005 delivered on Monday the 11th day of June 2007, before their Lordships; Dalhatu Adamu, OFR, JCA, M.B. Dongban – Mensem, J.P. J.C.A and Paul Adamu Galinje, J.C.A. , where the appellant, Amadi, cloned the official website of the Economic and Financial Crimes Commission, which he used to transact fraudulent financial business with several persons. Amadi was later arrested over the fraud of the $125, 000, charged to court and eventually sentenced to 16 years imprisonment. See Y. I. Arowosaiye, "The New Phenomenon of Phishing, Credit Card Fraud, Identity Theft, Internet Piracy and Nigerian Criminal Law" paper presented at the 3rd Conference on Law and Technology organised by the Faculty of Law, University of Kebangsaan, Malaysia and Faculty of Law, University of Tasmania, Australia, November 11 - 12, 2008.

28 R. G. Smith, M. N. Holmes and P. Kauffman: *Trends and Issues in Crime and Criminal Justice No. 121: Nigerian Advance Fee Fraud,* Australian Institute of Criminology: http://www.aic.gov.au/publications/tandi/ti121.pdf; retrieved on 15/03/2011.

29 Cap. 38, Laws of Federation of Nigeria, 2004 (hereinafter LFN 2004).

30 See for example, Smith, Holmes and Kauffman, *loc. cit.,* note 28 above.

who has been able to scoop funds from a business or government contract and needs a contact to help get the money they illegally obtained out of an account; a banker trying to close a dead customer's account using the potential victim as the deceased's next of kin; or the relative of a deceased military or political figure who is trying to claim an inheritance.[31] The majority of scams implicate the sender in some form of illegal behaviour. In turn, the sender attempts to ensnare the recipient in this illicit, yet ultimately false, transaction.[32]

Fraudsters sometimes offer to sell to their victims all manner of things including lucrative stocks, machineries, medical and pharmaceuticals, etc. at ridiculously low price. The prospective buyer is lured into willingly parting with his or her money for the items that will never be sent.

The forms that fraud on the internet can take is not exhaustive neither will it be necessary to attempt to exhaust them in chapter work of this size.

4. Legal Issues in Electronic Transactions in Nigeria

Advancement in science and technology particularly ICT, no doubt, has added a great deal to the quality of human life in the contemporary world. ICT is weaving the world together into a global village and many of the difficulties which hitherto hampered international and even national commercial transactions have become history. Following the emergence of electronic commerce as a result of the development of the internet, commercial transactions are now conducted between parties from different parts of the world who may never see themselves in their lifetimes.[33]

The growth of telecommunication technology has facilitated the process of buying and selling over electronic lines, both locally and globally. E-commerce facilitates international co-operation through trade, making goods and services available to consumers all over the world irrespective of distance. It has greatly expanded the consumer base for manufacturers or producers of goods and services,

---

31 E. Edelson: "The 419 Scam: Information Warfare on the Spam Front and a Proposal for Local Filtering" *Computers and Security* (2003) Vol. 22 (5), pp. 392-401.

32 Holt and Graves, *loc. cit.*

33 T. I. Akomolede: "Contemporary Legal Issues in Electronic Commerce in Nigeria" *Potchefstroom Electronic Law Journal,* 2008 Vol.3.

and brought about significant reduction in the costs of service delivery.[34] The traditional buying and selling process is being gradually replaced by internet trading, especially in more advanced countries. The consumer today is able to access goods and services from the remotest parts of the world without having to travel there or see the suppliers.[35]

Conversely, e-commerce has also brought with it a number of legal and socio-economic issues, especially in developing nations such as Nigeria. These issues include the extent to which the communication between the parties is protected (data protection), the formation of contract on the internet, the legal means of effecting payment in e-commerce, which court will assume jurisdiction in the event of a dispute between parties to an internet contract, and what law or laws (law of the seller or that of the buyer) will govern the transactions. Other issues are cyber crimes that are threatening e-commerce, and also the mode of proving internet-related transactions.[36] Legal regulation should necessarily focus on these identified issues. An examination of our laws relating to these issues is necessary for a determination of the adequacy or otherwise of our current regulatory framework for electronic fraud.

4.1 Data Protection

A serious source of concern for internet users in Nigeria is the protection of data on the web. Vast amounts of information about people are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. According to Lord Hoffman "...The right to keep oneself to oneself, to tell other people that certain things are none of their business is under technological threat."[37] Trading on the internet is through the transmission of electronic data from the suppliers or producers of

---

34 D. Chaffey: *E-Business and E-Commerce Management, (*2nd ed), (Harlow: Prentice Hall, 2003) p. 16.

35 O. Bali, *Information Technology and the Law* (Lagos: Legal Digest Publishing, 2002), p. 53.

36 Akomolede, *loc. cit.,* p.3.

37 Per Lord Hoffman in *R. v Brown* [1996] 1 All ER 545 at 556.

goods and services to the buyers, and vice versa. In view of the openness and accessibility of the internet the protection of such data poses a very serious challenged to policy and law makers.

In a number of jurisdictions protective legislation have been enacted to deal with the matter.[38] Presently, there is no legislation on the protection of data in Nigeria, and the situation portends a great danger for consumers in e-commerce. It has been suggested that a cue be taken from such jurisdictions, where there are principles that govern the protection of the data or communication between the parties in all internet transactions.[39]

4.2 Formation of Contract

Another vexed issued in most electronic transactions is the determination of the moment when a contract can be said to have come into existence so as to give rise to the existence of rights and obligations between the parties thereto. In contrast, traditional commercial transactions do not pose any significant problem because there are elaborate common law and statutory rules that govern the questions of offer and acceptance in contract. The special nature of internet contracts renders most of the common law rules inapplicable to such contracts.[40] The rules relating to acceptance by post and telegraph[41] are not appropriate for the internet transactions. In sales over the internet, both the display and the actual sale are often fused.[42] One way to obviate this quagmire is for the online seller or website owner to design the web page in such a way that it must clearly indicate that the information contained on the web in respect of a particular product or service is meant to elicit an offer and is not

---

38 For instance, the Data Protection Act 1984 was enacted in the UK and it harmonised earlier legislation, policies and directives meant to protect communication through the internet. See also the Electronic Communications Privacy Act 1988 in the USA.

39 Akomolede, *loc. cit.,* note 33 above.

40 See G. J. H. Smith, *Internet Law and Regulation* (London: Sweet and Maxwell, 2007) Chapter 10: Electronic Contracts and Transactions.

41 *Adams v Lindsell* (1818) 1 B&A 681 and *Dick v US* F. Supp. 326 (1949). For a statutory provision on this point, see for example, s. 120 (1) and (2), Contract Law, Cap. 26, Revised Laws of Enugu State of Nigeria, 2004.

42 See the case of *Harvela Investments v Royal Trust Company of Canada* [1986] AC 207.

in itself an offer.[43] The analogy has always been to liken a website to a shop in such a way that the product information on the website constitutes an invitation to make an offer.[44]

It accords with good sense and commercial necessity that the web owner should clearly indicate if the display or advertisement of his goods on the web amounts to a direct offer to whoever comes in contact with the site, or an invitation to make an offer. The approach would save a lot of time and expense that would otherwise have been wasted on frivolous or unnecessary litigation. According to Gringas and Nabarro[45] the best practice legally is to make any offer by e-mail subject to a date on which the offer will lapse. An objective date and time must be specified. If no intention is shown as to the lifespan of the offer, the courts would imply that the offer lapses after a reasonable time.[46]

A contractual situation that is often peculiar to the internet is the consideration needed to cement a web-based contract. The use of digital cash in exchange for goods or services raises issues not of consideration but of performance of a contract in a web-wrap contract which is an agreement at the front of a website which purports to bind the browsers to a contract should they proceed to browse the site. Promises to pay over the internet are enough to form the consideration to create a contract; in the same way as such promises would lead to enforceable contracts in normal commercial

---

43 C. Gringas and N. Nabarro, *the Laws of the Internet* (London: Butterworths, 1977), p. 15.

44 It has been held that a justification for not holding shops as making offers is to ensure that if the shop's stock is depleted, a willing consumer cannot sue the shop owner for damages: See *Esso Petroleum v Customs and Excise Commissioners* [1976] 1WLR 1, 11. The argument has also been made that a website is not offering physical goods for sale, and as such it is difficult to accept that supplies can be exhausted, because digital products supplied on the internet are infinite in supply. See Gringas and Nabarro, *ibid.,* at p. 16.

45 *Ibid.*

46 See *Chanco Leasing SPA v Rediffusion* [1987] 1 FTLR 207. See also, *Quenerdine v Cole* (1883) 32 WL 185.

transactions.[47]Contractual intention is also essential to entering into internet or web-based contracts.

The presence of a contractual intention is even more important in e-commerce, because more often than not only one human being is involved in the communication, with programmed computers or machines at the other side. It is settled that contracts can be made with machines, and it is of no legal consequence that a machine physically completed the contract.[48] However, in most cases the courts look objectively into the circumstances of each case to determine whether a contract has been made or not. Thus, in determining the requisite intention the court applies an objective test as against a subjective one.[49]

4.3 Payment in E-commerce

Making payment for goods and services bought through the internet poses unique problems because of the fact that the parties may be thousands of kilometres apart. Goods and services bought or supplied through the internet can be paid for through the internet in the same way that the internet can be used to make offers and accept offers.[50] Vendors or sellers often insist on receiving and validating payments before providing services or releasing goods to customers, and it is therefore suggested that terms to this effect should be incorporated as part of the standard form agreements in e-commerce.[51]

Popular methods of effecting payments for goods bought through the internet include the use of credit cards, smart cards, digital or electronic cheques or cash, and debit cards. The use of credit cards is still not very popular in developing countries including

---

47 See *Bradesh v Arthur* (unreported), reviewed in Reporter 1999 *IBAQ* 18. See also *Specht v Netscape* [2002] (unreported), as reviewed by Bali *Information Technology and the Law*.

48 See *Thornton v Shoe Lane Parking* [1971] 2 QB 163, *Edwards v Skyview* [1964] 1 WLR 399, *Smith v Hughes* (1871) LR 6 QB 597.

49 See *Smith v Hughes* (1871) LR 6 QB 597 and *Shaktas On-line Services v Burrough* [1999] (unreported), reviewed in Reporter 1999 *SBJ* 6.

50 D. C. Lynch and L. Lundquist, Digital *Money* (New York: Wiley, 1996), p. 38.

51 Akomolede, *loc. cit.*, note 33 above.

Nigeria,[52] and the common practice is therefore for the sellers to obtain bank guarantees in such transactions. If the goods are supplied and payment is not forthcoming through the bank's guarantee, the seller has a right of action against the issuing bank that has guaranteed payments.[53]

4.4 Jurisdiction and Choice of Law Issues

The issue of jurisdiction is a crucial one in e-commerce. The question has always been which court assumes jurisdiction in resolving a dispute arising from a contract between the parties, in view of the fact that the parties may be residing in different countries with different legal systems. The issue basically is one of Private International Law, and the relevant Convention is the Brussels Convention on Jurisdiction and Enforcement of Judgment in Civil and Commercial Matters[54] applicable to those countries that have ratified it and incorporated its provisions into their municipal laws. It is doubtful if Nigeria has ratified the Convention, as the writers could not find any evidence of its ratification.

In relation to internet contracts, the general rule is that jurisdiction is determined by reference to the place or country where the contract is performed.[55] Where there are many jurisdictions where the contract is performed, the relevant jurisdiction is the jurisdiction where the dispute arises. The place of domicile may also determine the court that will have jurisdiction. Where the parties are domiciled

---

52 See, F. O. Ukwueze: "Protection of Consumers of Financial Services in Nigeria: A Review" in F. N. Monye (ed.), *Consumer Journal,* Vol. 2 No. 1 (Enugu: Consumer Awareness Organization, 2006) pp. 108 – 144.

53 Y. Dinakin: "Forms and Procedure of Import Export Trade in Nigeria"1982 *Law and Practice of International Trade,* pp. 30-42. See also C. Hofacker, *Internet Marketing* (New York: Wiley, 2001) p. 81.

54 *Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters* 1958.

55 O. Davies: "Contract Formation on the Internet: Shattering a Few Myths" in L. Edwards and C. Waelde (ed), *Law and the Internet* (Oxford: Hart Publishing, 1997) p. 100.

in a contracting state under the Brussels Convention, the rules of the Convention are applicable, while the rules of common law are applicable where the parties are not domiciled within a contracting state. There is a reversal of the general rule above in relation to consumer products, in that consumers are allowed to sue and be sued in their home states.[56] The implication therefore is that there will be a frequent reversal of the general rule in favour of consumers, namely that litigation will take place only where the consumers reside, since most website owners are either suppliers of goods and services or professionals.

The trend in e-commerce has therefore been to paste on the website that an agreement resulting from viewing a website is not a contract for the sale of goods or supply of services. This is obviously done to avoid the rule in favour of consumers. It has, however, been held that classification of a contract as a contract of sale of goods or supply of services should be determined by examining the terms of the contracts to discover the substances. The courts have the powers to look at the content and substance of a transaction in the event of a dispute, to determine whether it is contract of sale of goods or supply of services.[57]

A corollary of the vexed issue of jurisdiction in e-commerce is the choice of law to be applicable in disputes arising from consumer contracts concluded over the internet. The complexity involved in the choice of applicable law has been described as follows:

> The question of choice of law… is particularly difficult in the case of International computer networks where, because of dispersed location and rapid movement of data and geographically dispersed processing activities, several

---

56 See art 13 and 14 of the Brussels Convention. Also, s. 44, *Civil Jurisdiction and Judgement Act* 1982 (UK).

57 See the case of *Robinson v Graves* [1935] 1 KB 579 particularly p. 587; see generally the obiter dictum of Sir Iain Glidewell in *St Alban's City and District Council v International Computers* [1996] 4 All ER 481 at p. 493, where he opined that a transfer of a programme to a computer by a third party did not constitute a transfer of goods, as there was no title passed between them.

> connecting factors could occur in a computer manner involving elements of legal novelty.[58]

Edwards has also observed as that:

> There are still more difficulties with regulation of cyberspace by the laws of a single jurisdiction. It is not just that national law is difficult to apply and enforce given the inherently transnational nature of the internet. It is also sometimes impossible to discern what country's laws would be most appropriately applied.[59]

Where parties to the internet contract are citizens of countries that have ratified the Rome Convention,[60] then the provisions of the Convention would be applicable to determine which law to apply in disputes between the parties. The Convention allows the parties to agree *ab initio* on the law that will be applicable to whatever dispute may arise from the transaction, and where no provisions are made then the provisions of the Convention are applicable.

Freedom of contract is an established principle and that the parties to an internet contract can therefore agree on the terms and conditions of the contract including the choice of laws to govern the transactions.[61] However, this is easier in contracts that are not standard form contracts. Where the parties have contracted outside the provisions of the Convention by agreeing on the applicable law to

---

58 See OECD Explanatory Memorandum and Guidelines on the Protection of Privacy and Transborder Flows of Personal data, 1980 quoted in Gringas and Nabarro, *op. cit.,* note 43 at p. 45.

59 L. Edwards and C. Waelde: "Introduction to the Law and Internet" in Edwards and Waelde, *op. cit.,* note 55 above.

60 Convention on the Law Applicable to Contractual Obligations 1980.

61 See Nnaemeka-Agu, JSC (as he then was) in *African Petroleum v Owodunni* [1991] 8 NWLR (Pt. 210) 351. But see the provisions of s. 4 of the Supply of Goods (Implied Terms) Act 1973 (UK) where a supplier's freedom to limit terms is now completely abolished. The act provides full protection for buyers in consumer transactions and qualified protection in non-consumer transactions.

govern their transactions, the complexities of determining what should be the choice of applicable law are entirely avoided.

4.5 Evidential Issues

Transactions conducted through the internet raise fundamental evidential issues in relation to the proof. Transactions on the internet are paperless and paper records of them can only be produced from their records that first existed in electronic formats. These differ from paper-based transactions where everything from the onset are embodied in a permanent form and typically expressed in words and figures usually authenticated by signatures. Such records can only be altered by an alteration on the face of the document.[62]

In countries with common law traditions such as Nigeria it is a cardinal rule of evidence that a party must give the best evidence of facts that are in issue before the courts. And the best evidence of a fact in issue is direct evidence of the fact. Evidence of a fact in issue other than direct evidence is hearsay and generally inadmissible.[63] In consequence of this rule, one of the greatest challenges facing the courts in Nigeria is the admissibility of computer-generated evidence. In the context of e-commerce, information fed into the computer and posted on the websites of sellers and suppliers of goods and services, when retrieved from the web, would only be copies of such information and at best would be hearsay evidence. The communication between the parties would also be copies as against originals when downloaded from the internet. The peculiarity of these issues and the confusion that has also greeted their interpretation by the courts have exposed the inability of the Nigerian Law on Evidence to cope with the admissibility of the avalanche of electronically-generated evidence that is the hallmark of electronic commercial transactions.[64]

---

62 D. Bender: "Computer Evidence Law: Scope and Structure" 1979 *Computer Law Journal,* pp. 699-714.

63 This is known as "the best evidence rule" or “direct evidence rule” and is contained in s.77 (a) – (d) of the Evidence Act, Cap. E14, LFN 2004 (hereafter, the Evidence Act). See also *Subramanian v Public Prosecutor* [1956] WLR 965, 969.

64 Y. Osinbajo: "Admissibility of Computer Generated Evidence under Nigerian Law" 1990 *Jus.* pp. 11 - 20.

4.6 Cyber Crimes

Internet or cyber crime means the commission of unlawful acts using the computer either as a tool or a target, or as both. Cyber crimes may be categorised into three: the crimes of obtaining computer hardware, peripherals, and software illegally; crimes that actually target a computer network or device directly[65] and crimes committed through the use of computer networks or devices.[66] According Council of Europe, cyber-crime involves "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data..."[67] The most common internet crimes include hacking and cracking, identity theft, the sale of illegal or stolen articles on the internet, packet sniffing, and the creation of malicious codes such as viruses.

The most common form of cyber crimes in Nigeria is probably fraudulent electronic mails, referred to as 419. Apparently the number "419" refers to section 419 of the Nigerian Criminal Code Act[68] dealing with fraud. These usually take the form of e-mails, text messages and other forms of communication in which the recipient is persuaded to advance sums of money with the promise of realising a significantly larger gain.

Cyber crimes pose a very serious threat to electronic commerce and have indeed made internet transactions insecure and vulnerable to manipulation by persons who are not parties to such

---

65 These include hacking, viruses, worms, Trojan horses, logic bombs, malware, sniffers, bots, spyware, etc.

66 These do not target the computer system. They include fraud and identity theft: phishing and pharming scams; corporate espionage; embezzlement; copyright infringement with software, music and movie piracy; cyber terrorism; child pornography; trafficking, and more) See Computer Crime Law - Guide to Computer Crimes Law at http://www.hg.org/lawfirms.html; retrieved on 29/03/2011.

67 Council of Europe (COE), Convention on Cybercrime, 2001, preambular paragraph 8, http://conventions.coe.int accessed on 31/3/2011.

68 Cap. C38, LFN 2004 (hereinafter simply referred to as the Criminal Code). Section 419 forms part of Chap. 38 of the Code dealing with obtaining property by false pretences and cheating.

transactions. The extent to which internet crime has ravaged the commercial world was succinctly captured by learned authors as follows:

> It is also predictable that the proliferation of commerce on the internet will be matched by an expansion of crime on the internet. The rise in the use of digital cash and credit cards over the internet provides a greater incentive to hack than ever before.[69]

In most advanced countries these activities are crimes because of statutory regulations.[70] In Nigeria, there is no specific legislation on cyber crimes. Legislative effort in this regard in Nigeria is still at the stage of a bill which is presently pending before the National Assembly.[71] The bill addresses most of the issues that have been identified as constituting internet crimes. It contains provisions similar to the laws on this subject matter in the advanced jurisdictions; hence it is hoped that it will usher in better protection for cyber space and consumer in e-commerce when it is enacted into law.

5. Current Regulatory Framework

5.1 The Criminal Code Act and the Penal Code

Fraud generally is prohibited by the two principal penal statutes in the country: Criminal Code Act, applicable in the southern states and the Penal Code, applicable in the northern states.[72] Therefore, advance fee fraud committed on the internet may qualify as a false pretence

---

69 Gringas and Nabarro, *op. cit.,*note 43 at p. 211.

70 For example, they are crimes in the USA by virtue of the provisions of Electronic Communications Privacy Act 1988 and Computer Fraud and Abuse Act 1991. In Britain, they are crimes by virtue of the provisions of the Computer Misuse Act 1990.

71 The draft law known as "A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for Other Related Matters" has been pending since 2008.

72 See the Criminal Code: ss. 418 - 426 on cheating and obtaining property by false pretences, ss. 434 - 439 on fraud and false accounting, 463 - 483 on the offence of forgery generally and ss. 484 - 489 on personating. Also see the Penal Code: ss. 362 - 380 on forgery, s. 179 on false personating and ss. 320 - 325 on cheating.

under section 418 of the Criminal Code,[73] while a successful internet scam would amount to a felony under section 419, which 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.

Alternately such a person may be charged under section 421 of the Criminal Code of the 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...

The Criminal Code and the Penal Code predate the internet era and understandably does not specifically address cyber crimes.

---

73 Which provides that 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, is a false pretence.

However, advance fee fraud system obviously falls within the ambit of their provisions which have been used for years by the Nigerian law enforcement agencies for prosecuting alleged acquisition of property by false pretence. The provisions of the Codes on fraud are ill-suited for cyber crimes in light of a number of identifiable shortcomings.[74] First, although section 419 of the Criminal Code deems the offence of obtaining by false pretence 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 peculiarities of cyber crime. With modern mobile wireless internet modems that are readily available from GSM operators, scam e-mails can be sent from the home, internet cafes, or even while the scammer is on the move. It will be nigh impossible to police every home, office and cyber cafe in order to arrest the suspect *in flagranto delicto*.[75] There is no justification why an arrest should not be made without a warrant, given that all other felonies in the Criminal Code could be investigated without a warrant of arrest.[76] The offence of obtaining property under false pretence is capable of being committed on the internet with transnational dimension. The requirement of a warrant before a suspect can be arrested is unjustifiable; it will afford the suspect the opportunity to escape or to destroy evidence of the offence.

The second shortcoming of the provisions of the Criminal Code is the paucity of the punishments. Upon conviction, an offender under section 419 of the Criminal Code is liable only to three years imprisonment or seven years if the value of stolen property exceeds One Thousand Naira (₦1000.00). This, to say the least, is paltry relative to the enormity of the crime and unjust rewards that characteristically run into millions of dollars.

---

74 See T. A. Oriola: "Advance Fee Fraud on the Internet: Nigeria's Regulatory Response" *Computer Law & Security Report* (2005) 21, pp. 237 - 248, see particularly pp. 240 – 341.

75 In the very act of committing the offence.

76 S.3 of the Criminal Code defines a felony as ''any offence which is declared by law to be a felony, or is punishable, without proof of previous conviction, with death or with imprisonment for three years or more" while s.5 of the Act provides *inter alia* that ''Except when otherwise stated, the fact that an offence is within the definition of a felony as set forth in this code imports that the offender may be arrested without warrant."

The third drawback, under the Criminal Code, is the lack of restitution for victims of crime.[77] The victims could, no doubt, resort to civil court for remedies. However, the chances for success of the plaintiff in the typical advance fee fraud case will be extremely slim.[78] For example, 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 as the court would not hesitate to declare such a contract illegal.

5.2 The Advance Fee Fraud and other Related Offences Act 2006

Following the phenomenal growth in the menace of advance fee same in Nigeria and in view of the observed deficiencies of the principal penal statutes in relation to the matter, the Federal Government enacted the Advance Fee Fraud and other Fraud Related Offences Act.[79] The Act was intended to plug the loopholes in the Criminal Code.[80] Section 20 of the Advance Fee Fraud Act 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;

---

77 This is not the case under the Penal Code because section 78 of the Penal Code and section 365 of the Criminal Procedure Code generally empower the court that has convicted a person of an offence to make a compensation order. See the case of *Ganiyu Martins v Commissioner of Police, Kano State* [2005] 7 NWLR (Pt. 925) 614; (2005) All FWLR (Pt. 278) 1075.

78 Oriola, *loc. cit.,* note 74 at p. 241.

79 Cap. A6, LFN, 2004 (as amended in 2006, hereinafter Advance Fee Fraud Act).

80 See A. Adekunle: "Seizure of Proceeds of Criminal Activity: Trends in Recent Financial Crimes Legislation in Nigeria" *Modern Practice Journal of Finance & Investment Law* (April 1999) Vol. 3, No. 2 at 250 - 267.

As against sections 418 and 419 of the Criminal Code Act, section 1(1) (a), (b) (2) & (3) of the Advance Fee Fraud Act widens the scope of advance fee fraud victims as defined under section to include foreigners and makes fraudulent invitation of foreigners for the purpose of committing an offence an offence by itself.[81] This improvement is highly commendable because it recognises and protects potential foreign advance fee fraud victims.

The second significant improvement of the Advance Fee Fraud Act over the Criminal Code is the increase of imprisonment term from as low as five years to 20 years for obtaining property under false pretence. Under the Advance Fee Fraud Act, both actual fraud and fraudulent invitation of a person to visit Nigeria are punishable by imprisonment for a term not exceeding 20 years and not less than seven years without an option of fine.[82] This is a welcome development. A low jail term for such an offence considerably lowers the risk, and might even serve as an incentive for many fraudsters to venture into the money-making scam business.[83] Commendable also is the provision for imprisonment without option of fine for most of the offences under the Act.

Another significant provision of the Advance Fee Fraud Act is section 5(1) which provides that where a false pretence which constitutes an offence under the Act is contained in a document, it shall be sufficient in a charge of an attempt to commit an offence under the Act to prove that the document was received by the person

---

81 S. 1(1) – (3) of the Act provides follows: (1) Notwithstanding anything contained in any other enactment or law, any person who by any false pretence, and with intent to defraud (a) obtains, from any other person, in Nigeria or in any other country for himself or any other person; (b) induces any other person, in Nigeria or in any other country, to deliver to any person; or (c) obtains any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act. (2) A person who by false pretence, and with the intent to defraud, induces any other person, in Nigeria or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act. (3) A person who commits an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not more than 20 years and not less than seven years without the option of a fine.

82 See ss. 1 (3) and 4.

83 Oriola, *loc. cit.,* note 74 at p. 242.

to whom the false pretence was directed. Also a person who is in possession of a document containing a false pretence which constitutes an offence under this Act commits an offence of an attempt to commit an offence under this Act if he knows or ought to know, having regard to the circumstances of the case, the document contains the false pretence.[84] This obviously is intended to prohibit deliberate or negligent handling of fraudulent documents. Document is broadly defined to include:

> letters, maps, plans, drawings, photographs and also includes any matter expressed or described upon any substance by means of letter, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter and further includes a document *transmitted through fax or telex machine or any other electronic or electrical device, a telegram and a computer printout*.[85]

This definition of document is wide enough to cover communication by electronic means.

A further significant provision of the Advance Fee Fraud Act is the introduction of a restitutionary clause for the victims of advance fee crimes. Section 11 of the Act provides as follows:

> (1) In addition to any other penalty prescribed under this Act, the High Court shall order a person convicted of an offence under this Act to make restitution to the victim of the false pretence or fraud by directing that person - (a) where the property involved is money, to pay to the victim an amount equivalent to the loss sustained by the victim; in any other case - (i) to return the property to the victim or to a person designated by him; or (ii) to pay an amount equal to the value of the property, where the return of the property is impossible or impracticable.

---

84 S. 6, italics added.

85 S. 20.

> (2) An order of restitution may be enforced by the victim or by the prosecutor on behalf of the victim in the same manner as a judgment in a civil action.

To facilitate the implementation of the restitutionary provision, section 16(1) (a) (b) and (c) of the Act empowers the Court, if satisfied that a *prima facie* case exists against any suspects, at any stage of the proceedings, to restrain dealings in suspects' property, assets or bank account. This provision would help preserve the estates of suspects, and foreclose the possibility of disposing off valuable property that could render a restitutionary order after trial and conviction, nugatory.[86]

Section 13 (1) and (2) of the Act obligates any person or entity who in the normal course of business provides telecommunications (including GSM), internet services or is the owner or person in the management of any premises being used as a telephone or internet cafe or by whatever name called shall be registered with the Economic and Financial Crimes Commission (EFCC), keep proper records of their customers and make returns to the Commission on the use of its facilities. Such a person has a duty of care to ensure that his services and facilities are not utilized for unlawful activities. Failure to comply with the above provisions will constitute an offence punishable on conviction by imprisonment for a term of not less than three years without an option of fine and in the case of a continuing offence, a fine of N50, 000 for each day the offence persists. Also the operational license of the offender may be revoked.

The requirement of registration and returns to the EFCC will compel ISPs,[87] GSM and cyber cafe operators to mindful of the activities of their clients. By section 3 of the Act, a person who, 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 the Act commits an offence and will liable on conviction to imprisonment for a term not less more than 15 years and not less than five years without the option of a fine.

---

86 Oriola, *loc. cit.,* note 74 at p. 243.

87 Internet Service Providers.

5.3 The Economic and Financial Crimes Commission (Establishment, etc.) Act 2004

Even with the enactment of the Advance Fee Fraud Act the Nigerian government was still under international pressure do something about the menace that has not only tainted the country's image but that of its citizens abroad. This was probably due to the fact that there was no agency charged with the responsibility of investigating and prosecuting cyber crimes. It was felt that the Nigerian Police Force lacked what it takes to handle cyber crimes. The enactment of the Economic and Financial Commission (Establishment, etc.) Act[88] was in response to the call for renewed efforts in tackling the malaise. The Act establishes the Economic and Financial Crimes Commission with responsibility *inter alia* to investigate and prosecute all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.; and enforce the provisions of the following laws:

(a) Money Laundering Act 2004;[89]
(b) Advance Fee Fraud and Other Fraud Related Offences Act;
(c) Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act;[90]
(d) The Banks and other Financial Institutions Act;
(e) Miscellaneous Offences Act; and
(f) Any other law or regulations relating to economic and financial crimes, including the Criminal Code and Penal Code.[91]

The Commission's membership, which includes the Governor of the Central Bank, representatives from the Ministries of Justice, Finance,

---

88 No. 1, 2004(hereinafter EFCC Act).
89 Cap. M18, LFN 2004 (as amended)
90 Cap. F2, LFN 2004 (as amended)
91 See ss. 6, 7 and 13 (2) of the EFCC Act.

and Foreign affairs,[92] shows government's recognition of the transnational aspect of advance fee fraud, amongst other crimes, and the need to tackle it decisively.

Economic and Financial Crimes as defined in Act include all forms of fraud:

> Economic and Financial Crimes means 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.[93]

It has been argued that omission to specifically mention advance fee fraud in the definition of economic crime in the EFCC Act significantly detracts from the Act's relevance to prosecuting advance fee fraudsters in cyberspace, notwithstanding the Act's empowerment of the Commission to prosecute advance fee fraudsters in cyberspace.[94] Though the definition of economic crimes under the Act does not refer directly to electronic fraud it is unarguably subsumed under "any form of fraud" or "any form of corrupt malpractices" in the Act. Again, specific mention of cyber crime or advance fee fraud would have been superfluous and unnecessary,

---

92 Others are the Chairman of the National Drug Law Enforcement Agency, the Director General of the National Intelligence Agency, the Director General of the Department of State Security Services, the Director General Securities and Exchange Commission, the Commissioner for Insurance, the Post-Master General of the Nigerian Postal Services, the Comptroller-General Nigeria Immigration Services, an Assistant Inspector General of Police, four eminent Nigerians with cognate experience in either banking, finance or accounting and a Director General who shall be the head of Administration. See section 6 (1) of Act.

93 s. 46. Italics added.

94 Oriola, *loc. cit.,* note 74 at p. 244.

since the Commission is already charged *inter alia*, with administering the Advance Fee Fraud Act, which directly governs advance fee fraud.

An issue of concern is that the Commission has been loaded with too many responsibilities that could hamper its effectiveness. For instance, the Commission has the power to investigate all financial crimes relating to terrorism, money laundering, drug trafficking, advance fee fraud, etc. The Commission simply lacks the manpower to investigate a multitude of financial crimes, some of which are the traditional preserve of the police, immigration, and custom authorities. This calls for collaboration among all the law enforcement agents should work together in mutual co-operation rather than in rivalry. Investigations should be characterized by thoroughness, probity and integrity.

5.4 The Money Laundering (Prohibition) Act, 2004

Another relevant legislative measure in the fight against advance fee fraud on the internet is the Money Laundering (Prohibition) Act.[95] It makes comprehensive provisions to prohibit the laundering of the proceeds of crime or an illegal Act. Although proceeds of advance fee fraud are not expressly mentioned, they would appear covered under section 14 of the Act which provides *inter alia* that:

> Any person who -
>
> (a) converts or transfers resources or properties derived directly or indirectly offences form illicit traffic in narcotic drugs and psychotropic substances or any other crimes or illegal act, with the aim of either concealing or disguising the illicit origin of the resources or property or aiding any person involved in the illicit traffic in narcotic drug or psychotropic substances or any other crime or illegal act to evade the illegal consequences of his action, or
>
> (b) collaborates in concealing or disguising the genuine nature, origin, location disposition movement or ownership of the resources property or right thereto

95 Cap M18, LFN 2004.

> derived directly or indirectly from illicit traffic in narcotic drugs or psychotropic substances or any other crime or illegal act, commits an offence under this section and is liable on conviction to a term of not less than 2 years or more than 3 years

The Act punishes any person, corporate or individual, who aids or abet illicit disguise of criminal proceeds and mandates banks and financial institutions to inform the Central Bank of Nigeria or the Securities and Exchange Commission, of any transfer to or from the country, of a sum in excess of $10,000.[96] The main significance of the Money Laundering Act is that it enables authorities to monitor and detect suspicious cash transactions. This is facilitated by the statutory obligations on all financial and money transfer institutions to report any unusual or suspiciously huge financial transactions to the authorities.

5.5 The Evidence Act

In spite of the willingness of the courts to interpret the provisions of the Evidence Act liberally, various provisions of the Act have been found to be grossly inadequate for the admissibility of computer-generated evidence.[97] The problem of admissibility of evidence generated through electronic devices stems from the evidential status of storage devices, such as disks, tapes and such like materials since by virtue of section 2 of the Evidence Act they do not come within the definition of a document. Legally, the version of most electronic documents that will be tendered in legal proceedings will be copies of the original data which means that such evidence, subject to permissible exceptions, might fall foul of some of the concepts

---

96 s. 2.

97 For example, see the judgment of the Supreme Court in *Yesufu v ACB* [1976] 4 SC 1, and *Anyeabosi v RT Briscoe* [1987] 3 NWLR 84. In *Ogolo vs. IMB* (1995) 9 NWLR (part 419) 314 @ 324, the Court of Appeal per Onalaja J.C.A took judicial notice of electronic banking when it stated that "the commercial and banking operations in the keeping of account by the old system has changed to computer which makes Nigerian business to be modernised in keeping with the computer age which system is so notorious that judicial notice of it can be taken under S. 74 Evidence Act..." See also the case of *Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd* [2001] 16 NWLR (pt. 510).

underlying the admissibility of evidence in legal proceedings such as the "best evidence" rule and the rule against "hearsay". The communication between the parties would also be copies as against originals when downloaded from the internet and for it to be admitted it would have to be put in under any of the exceptions to section 91 of the Evidence Act.[98]

Much more progress has been made in the English and American jurisdictions in the admission of computer-generated evidence through specific legislation on computer evidence and judicial activism. For example, in the US case of *King v State Ex Rel Murdock Acceptance Corporation*,[99] the court admitted in evidence a computer printout tendered by the plaintiffs which showed the amount owed to them by the defendant. The clerks who accepted the payments were neither called, nor were the original records in the branch offices of the corporation produced. The court nevertheless admitted the documents and extended the exception to the hearsay evidence to cover computer records.

In the Australia, the issue of the admissibility of computer-generated evidence is now governed by legislation.[100] Thus, by the provisions of section 59 (1) of the South Australian Evidence Act, computer outputs are now admissible in both civil and criminal proceedings.

In Nigeria, the review of the Evidence Act made by the Nigerian Law Reform Commission is pending before the National Assembly. The bill makes fundamental changes to the existing rules of evidence in relation to computer-generated evidence, but only in respect of civil proceedings.[101] It is suggested that the provisions of

---

98 Y. Osinbajo: "The Law of Evidence and Information Technology" 2004 *CLE Workshop Series,* pp. 21-32.

99 [1996] 22 F2d 39.

100 See s 59(1) South Australian Evidence Act which copied s 5 of the Evidence Act 1965 (UK).

101 Bill for an Act to Amend the Evidence Act (SB291). The bill which copied the provisions of the English Civil Evidence Act 1964 provides in its s. 84 that in any civil proceedings statements contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible.

the bill should be extended to cover criminal proceedings when eventually it is enacted into law. The foregoing suggestion is very important in view of the increasing rate of cyber criminality and fraudulent practice that is threatening electronic commerce.

6. Conclusion

This chapter has identified electronic fraud as including all forms cyber crime and advance fee fraud. It was noted that strictly legally speaking fraud is a civil wrong except where the particular act has been prohibited by a penal statute. Nigerian is not totally lacking in legislation dealing with electronic fraud. In fact, one commentator stated that the proliferation of internet scams in Nigeria has more to do with a lack of effective enforcement and implementation of the existing legislation than lack of it.[102] However, an appraisal of the relevant laws has shown that they are lacking in depth and quality. This, no doubt, affects effectiveness in their implementation. The prolonged procrastinating in passing the bill to amend our over sixty-five years Evidence Act is proof to this assertion. One wonders why other extant legislation on the subject would not flounder if the Evidence Act is not amended to render easily admissible electronically generated data. As observed by Pats-Acholonu, J. C. A. (as he then was) in *Hon. Don Egbue v Justice E. O. Araka*:[103]

> It must be clearly understood that our Evidence Act is now...old and is completely out of touch and out of tune with the realities of the present scientific and technological achievements. Most of its sections are archaic and anachronistic and need thorough over haul to meet the needs of our time.

It is therefore submitted that, prosecution of cyber crime in Nigeria involving content-related offences, requiring admissibility of electronic data, will be frustrated by the present Evidence Act, and judicial activism arguably will be hard put to change the clear provisions of the statute. A complete overhaul of the Evidence Act is therefore a *sine qua non* for fighting cyber crime in Nigeria.

---

102 Oriola, *loc. cit.,* note 74 at p. 247.

103 (1996) 2 NWLR (Pt. 433) 688 at 711.

It is not only the Evidence Act that requires amendment to accord with the present technological realities. Other statutes that need to be amended include the two principal penal statutes in the country: Criminal Code and the Penal Code in relation to the definition of document to include electronic data.

Legal regulation of certain issues relating to cyberspace is totally lacking. For example, Nigeria has no legislation on data protection. The constitutional provision[104] relating to privacy is not sufficient to deal with the issue of data protection in cyber space. A more detailed statutory regulation, such as is the case in the UK and USA (as earlier cited) is not only desirable but imperative. There is also an urgent need to pass the Electronic Fraud Bill to bring our cyber space regulation up to date.[105]

Cyber crimes differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.[106] Our legislature has been slow to effect changes in existing laws that will align our statute books to the technological realities of our time. There is need to improve the machineries for enforcement of existing laws. Presently, there is a dearth of personnel required to give effectiveness to cyber crime laws. Our law

---

104 s. 37 of the 1999 Constitution (as amended) mere provides in a very terse form that: "The privacy of citizens, their homes, correspondences telephone conversation and telegraphic communications is hereby guaranteed and protected."

105 The bill seeks to enact the Nigeria's version of UK's Computer Misuse Act, 1990, Terrorism Act 2001, Copyright Designs and Patent Act 1988 (with its amendments) Protection of Children Act 1978 (as amended) Obscene Publications Act, (as amended). See J. O. Mbamalu: "Nigeria's Roadmap to Accession to Council of Europe Convention on Cyber Crime" being an unpublished paper presented in partial fulfilment of the requirement for the award of LL.M (Computer & Communication Law) to the Queen Mary University of London on 24 April, 2004.

106 McConnell International: "Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information" December 2000 at www.mcconnellinternational.com retrieved on 29/3/2011.

enforcement agents, security officers, lawyers and judges will require new training to tackle the challenges posed by electronic fraud.

Pending the adoption of the suggested legislative measures, Nigerians are advised to adopt some self-protection mechanism. Such measures include taking necessary precaution to protect their personal data such as ATM and credit card User IDs and PINs. They should also ignore obvious scam e-mails and where in doubt forward them law enforcement agencies for necessary investigation.