THE INTERNATIONAL JOURNAL OF HUMANITIES & SOCIAL STUDIES

An Assessment of Malpractices by Bank Customers in the Banking Industry in Nigeria

Uwem Emmanuel Udok
Senior Lecturer, Head of Department of Private Law
Faculty of Law, University of Uyo, Uyo, Akwa Ibom State, Nigeria

Abstract:
The banking industry constitutes one of the pillars on which the economy of any nation can be erected. Over the years, the banking industry has grown tremendously in terms of the network of branches and the number of staff. Coupled with these is the sophistication in the banking operations, which has helped to fast-track the services rendered by banks to customers. Regrettably, however, there has been an upsurge in the level of malpractices committed in the banking industry. These malpractices sometimes lead to the collapse or distress in the industry, being perpetrated by the bank as a corporate entity, the bank staff and the bank customers. In this paper, attempt shall be made to examine the malpractices committed by the bank customers in the banking industry and suggest measures to tackle them.

1. Introduction

In 1986, the Federal Military Government introduced the Structured Adjustment Programme (SAP) and part of the programme was the deregulation of the banking industry, which precipitated tremendous growth in the industry. Thus, the number of banks and their branches increased astronomically. There was also an upsurge in the number of total assets and total capital and reserves during that period.[1] The aftermath of this monumental growth in the banking industry was the emergence of sharp practices perpetrated by the operators in the industry. These sharp practices later metamorphosed into malpractices that resulted in the collapse of many financial institutions[2]. Banking malpractices, also commonly referred to as "bank fraud", "elite or "white collar" crimes, have permeated the very fabric of the banking industry causing monumental havoc and leading to human and financial losses.

In the words of John U. Ehodaghe

…malpractices lead to huge financial losses to banks and banks capital, their customers, the depletion of shareholders funds and banks capital base, as well as loss of confidence in he banking system. It also leads to the closure of some affected banks as witnessed in Nigeria and other parts of the world in recent times[3].

The above picture painted by the distinguished author goes to show how devastating malpractices can be to the banking industry. It is therefore intended in this paper to examine malpractices in the banking industry in Nigeria with particular reference to malpractices committed by bank customers.

2. Meaning and Nature of Malpractices

The New International Webster's Comprehensive Dictionary of English Language defines malpractice as "improper or illegal practice, "improper or immoral conduct"[4]

Furthermore, the Webster's New World Dictionary defines malpractices as follows:

"Misconduct or improper practices in any professional or official position".[5]

The Black's Law Dictionary is not left out as it defines malpractice as: "an instance of negligence or incompetence on the part of a professional".[6] One thing seems to be common to the above definitions, which is that malpractice contemplates a conduct or practice that is improper or illegal. However, the definition of malpractice contained in the Black's Law Dictionary appears to be over-inclusive as it defines malpractice to mean an act of negligence of a professional, such as a medical doctor or a legal practitioner. But

[1] Ebhodaghe, J. "Malpractices in the Banking Industry: Nature. Types. Causes and Remedies". In Safe and Sound Banking Practices in Nigeria: Selected Essays. (Lagos: Page Publishers Services Ltd, 1997) P. 160.
[2] Ibid
[3] Edhodaghe, J. op. cit, p 160
[4] Encyclopedic Edition, (Typhoon International Corporation, 2003) p. 112.
[5] New Word Dictionary, 2nd edition Siman and Scluster: p. 140
[6] Thompson West Publishing, 2004, 8th edition p. 102

banking malpractice, which is the focus herein, contemplates a manifestation of some kind of fraudulent act or intention that is against the ethics of the banking profession or against the law in general.

Ebhodaghe further elucidates: "By malpractice, we mean broadly an unpermissible practice or improper treatment of an issue. In other words, it refers to that practice that is against the rules and regulations or is forbidden by law".[7]

Prof. Adeyemi conceptualizes the term 'malpractice' as: "…Those practices which are not only just contrary to the ethics of the banking profession but also of the various banking laws and regulations".[8]

Malpractices have also been referred to as corruption and economic crimes. Hence, Joe Boldface-Irokalise states as follows: "Banking malpractice, alternatively referred to as corruption and economic crimes, constitute the genus of what is generally known as and commonly called "elite" or "white-collar" "crimes".[9]

The above is not a definition of banking malpractice but a mere description of the term. It is over-inclusive as it makes reference to corruption and economic crimes as falling within the context of banking malpractices. The description of banking malpractice as a "white-collar" crime attracts comments.

The term "white-collar crimes"[10] is all-embracing, as it "encompasses fraud against business, fraud against the government, corruption of state and federal elected and appointed officials, and the whole network of the employees in the bureaucracy…[11]. It is therefore submitted that banking malpractice is a fragment or a sub-class of white-collar crimes and it has to do with any act or practice that is against banking laws or rules and regulations.

3. Categories of Malpractices in the Banking Industry in Nigeria

Malpractices in the banking industry are categorized into those committed by the bank as a corporate body, those committed by the bank employees or staff, and those committed by non-bank employees, (customers).

4. Meaning of Bank Customer

The meaning of the word "Customer" cannot be ascribed to any known statutory enactments except judicial pronouncements. In fact, the Banks and other Financial Institutions Act otherwise known as BOFIA has not made any attempt to define the term "customer". But the term "customer" was defined in Section 2 of the Bill of Exchange Act[12]. Section 2 of the Bill of Exchange Act states as follows: A bank customer is a person, whether incorporated or not who has some sort of account.

A customer of a bank can also be described as a person who has applied to the bank to open a current or deposit account in his name and whose application has been granted by the bank[13]. There has to be a continuous banking business to make one a customer[14]. Thus, in Great Western Banking Company Ltd v London and Country Banking Company Ltd,[15] a man who had for some years been in the habit of getting a cheque exchanged for cash from the bank where he had no account was held not to be customer of that bank. Also, an isolated act of banking transaction does not make one a customer[16]. It seems that the case of Matthews v. Brown and other cases to the effect which seem to suggest that an isolated banking transaction does not make one a customer may have been over-ruled by the case of Commissioner Taxation v English, Scottish & Australian Bank, where their Lordships of the Privy criminal held that:

…a man whose only connection with the bank at the material time was payment in of a single cheque for collection of the bank[17].

It follows from the above that, it is not necessary that the account should have been opened for a minimum length of time or that it should have been operated by a customer making a certain minimum number of payments into or drawing against it[18]. A bank customer is not necessarily a person who opens an account with the bank. A person can also become a bank customer when the bank renders or gives such a person financial advice[19].

---

[7] Malpractice in the Banking Industry: Nature, Types, Causes and Remedies in Safe, Sound Banking Practice: Selected Essays, op p. 161

[8] "Malpractice in the Banking Industry". Ajibola B and Awa, U.K. (eds) in Banking and Other Financial Malpractices in Nigeria (Lagos and Oxford, Mulhouse Press, 1990) p. 14.

[9] "Eradication of Banking Malpractices in Nigeria. "Will Law Alone Succeed"? In CBN Economic and Financial Review Vol. 33, No. 1 March 1995, p. 62.

[10] The United States Bureau of Investigation, in a working definition of crimes, states of white-collar, crimes: "those illegal acts characterized by deceit, concealment, violation of trust and not force or violence. They are committed to obtain money, properly or services; or to avoid the personal or business advantage". See GAO Report Resources developed by the Department of Justice to combat white-collar crimes and punish corruption, March, 19. 1979.

[11] Idoko, A. "White-collar crimes" in Nigerian Commercial Law; Problems and Perspective. (Dept. of Commercial Law, Ahmadu Bello University, Zaria, 1984), p. 22.

[12] Bill of Exchange Act No. 20 of 1964

[13] Ibid. It is not contained in the Bill of Exchange Act Cap B8 LFN 2010

[14] Ladbroke and Company v. Todd (1914) 30 FLR 433

[15] (1901) AC 414

[16] Matthews v Brown Vol. 10 TLR

[17] (1920) AC 683

[18] Ibid

[19] Hedly Bryne and Company Ltd v Heller and Partners (1960) AC 465

Apart from account opening, anybody who deposits safe-custody items with a bank and for which charges are made are Ipso facto, customers as any breach of it can be redressed legally. Furthermore, banks can receive funds for transfer purposes from people without necessarily opening accounts for them. Banks also deal with third parties particularly in letters of credit. Example where third parties are to be paid by a bank, even where there is no account relationship.

5. Malpractices by Bank Customers (Non-Bank Employees/ Outsiders)

It is pertinent to examine malpractices perpetrated by bank customers or non-employees of the bank. Indeed, in most cases these malpractices are committed with the connivance of the insiders who happens to be bank employees.

5.1. Advanced Fee Fraud

The most notorious of Nigerian scam is the advanced fee fraud scheme known as the 419 Scheme, named after a statute in the Nigerian Criminal Code.

The indulgence by few Nigerians in advance fee fraud (419) has destroyed the reputation and creditability of the country all over the world.[20] Consequently, majority of Nigerians have found it difficult to transact business both locally and internationally. Thus "nobody trust anybody and everybody suspects everyone[21].

Thus Advance Fee Fraud involves a situation where a person approaching a bank, a company or an individual with an offer to access large funds at below market interest rates usually on long term basis. Usually, the source of such funds is not specially identified and the only way to have access to it is through the person making the offer who must receive a fee or commission "in advance". The offeror usually disappears as soon as he receives the commission or fee. A bank who is desperate for frauds may fall victim to this type of fraud. When the deal does not go through, the victim may not likely report the losses to the relevant authorities. The offence can be committed by oral communication, or in writing or even by conduct of the accused person. It is, however, to be noted that an honest belief in the truth of the statement on the part of the accused which later turns out to be false cannot found a conviction[22].

5.2. Account Opening Malpractice

This involves the deposit and subsequent cashing of fraudulent cheques. Here, a person asks to open a transaction account such as current or savings account with false identification but unknown to the bank. The account is usually opened with a small initial deposit of cash or cheque. Generally, within a few days, the person will deposit a number of dud cheques and obtain cash in return, either by cashing the fraudulent items outright or by withdrawing cash as soon as funds are available with the connivance of bank staff. In Nu-stilo Footwear v Lloyds[23] a fraudulent person opened an account in assumed name stating that he had just started business as a freelance agent. He then began to defraud his real employers by endorsing cheques payable to his employers to himself in his assumed name and paying them into the newly opened account. The cheque was £172, though large but was not enough to arouse suspicion. The second one was £550 and the subsequent one amounted to some £4,000 were paid into the account. The bank was held to be negligent. It is therefore suggested that the bank should make enquires when very large cheques are suddenly paid in for collection for a small account kept by a customer who is not actually rich.

5.3. Forgery and Counterfeiting of Negotiable Instrument

As already indicated, forgery is defined under section 465 of the criminal code[24] as knowingly making a false document or writing with the intention that a person may in the believe that it is genuine, be induced to do or refrain from doing an act whether in Nigeria or elsewhere. Negotiable instruments are instruments or documents by means of which a series of debts or criminal obligations may be discharged without the use of cash or by which payment may be deferred or postponed by the granting of credit.[25] These include bill of exchange, cheques, promissory notes, dividend warrants, banker's draft, share warrant, bearer bonds or debentures.

Modern photographic and printing equipment have greatly aided criminals in reproducing good quality forged documents. The documents may be total counterfeits or may be genuine documents that are copied, forged or altered as to amount, payout date, payee or terms of payment.

In Umaigba v New Nigerian Bank Ltd[26], a cheque was issued in the name of an officer of a government parastatal as payment for motor vehicles supplied by the plaintiff. The plaintiff deposited the cheque into his account for clearance having been endorsed to the plaintiff's trading account. The next day the plaintiff withdrew the proceeds of the cheque having been cleared by the bank. It was subsequently, discovered that the cheque was forged.

The bank alleged that the plaintiff knew the cheque was a forged one debited the plaintiff with the amount represented. The plaintiff sued the bank and the court dismissed the plaintiff's case.

---

[20] Buchanan, J. "Investigating and Prosecuting Nigerian Fraud," US Bulletin Nov. 2001, See Section 419 of the Criminal Code Cap C38 LFN 2010.

[21] Ribadu, N. "Implication of Economic and Financial Crimes on the Nation's Economics" being a Paper Presented to Defence Adviser Conference in Abuja on the 10th Sept. 2004 p. 5.

[22] Ibid p. 6

[23] Alake v The State (1991) 7 NWLR (Pt. 205) 567 Onwudiwe v FRN (2006) 49 WRN 1 at 71

[24] Cited in Penington & Hudson Commercial Bank Law (London, Macdonald & Evans, 1978) p. 248

[25] Cap C38 LFN 2004

[26] Udok, U., The Law of Sale of Goods in Nigeria (Uyo: Kan Educational Books, 2004) p. 132.

5.4. Cheque Malpractices

A cheque is a bill of Exchange drawn on a banker payable on demand[27]. However, when combined with the definition of a bill of exchange, a cheque may comprehensively be defined as unconditional order in writing drawn by the person (drawer) upon another (drawee) who must be a banker, requiring the bank, to whom it is addressed, to pay on demand, a sum certain in money to or to the order of a specified person or bearer. A cheque is therefore a very important instrument by means of which commercial transaction may be carried out without the use of cash. Common types of cheques are personal, business, government, travelers, certified, draft and counter cheques with each having its own characteristics and vulnerabilities for fraudulent use.[28] Various types of cheque malpractices are committed by bank customers sometimes through the connivance of the bank staff.

The most common types are stealing of cheque books/leaves and subsequent forging of account holders signature, cloning of cheque, alteration of payee or amount payable, etc.[29] In USA, cheque cloning is very common. Armed with a computer, scanner desktop publishing program, colour printer, and basic computer know how, a fraudster can print corporate cheques in any dollar amount with an authorizing signature that is virtually identified to the original.

In Nigeria, it appears cheque cloning is relatively new. Very few cases have been reported. One Johnson Okokon was arranged before the court on a four-count charge of conspiracy to obtain money by false pretences, forgery and alteration of documents. He was arrested while trying to withdraw the sum of ₦244,000 from a new generation bank. After subjecting the cheque that had already been cashed by someone else. The drawer of the cheque denied issuing the cheque to him. He was convicted and sentenced to 10 years imprisonment[30].

Apart from the criminal code which prescribed punishment generally for offenders against forgery, the statutory provision on this point is the Bill of Exchange Act.[31]

By Section 24 of the Bill of Exchange Act, where a signature on a bill is forged or placed thereon without the authority of the person whose signature it purports to be the forged or unauthorized signature is wholly inoperative. However, such authorized signature may be ratified by the person who originally would have given the consent and authority to sign. The weakness of the above section is that it is restricted to only forgery of signatures thus other forms of forgeries like alteration of name, figures, dates or counterfeiting or cloning of the cheque are not covered. These are covered under the criminal code provision. It is therefore suggested that the section should be broaden by way of amendment to include these other forms of forgeries of cheque.

It is to be noted that not all unauthorized signatures constitute forgery but all forged signatures are unauthorized[32]. This is because an authorized signature though wholly inoperative is capable of ratification[33]. The onus is on the plaintiff to prove that the signature on a cheque is either a forgery or unauthorized. Until this condition is met the customer can not succeed against the bank to have his account credited with the sum paid out of the account as a result of inoperative signature. In UBN Ltd v Adediran[34] there were three signatories to an account after which one of them was replaced by another person and the bank was notified. A cheque was subsequently presented containing the signature of the former who was replaced and the bank honoured the cheque. The respondent sued the bank of wrongfully debiting the account with the sum paid out and succeeded. It has been argued that the cheque was not forged in the circumstance but the signature was unauthorized since the signature of the person was inserted without authority the person having been earlier replaced by another person. He was no longer the agent of the customer. Indeed, this is a case of unauthorized signature as opposed to forged signature. If the signature of the new person was forged, then a case of forgery would have arisen. The signature was the genuine signature of the former person though he was no longer the agent of the customer and so his signature was unauthorized. To avoid rampant cases of cheque malpractices, it is suggested that the current effort by the regulatory authorities as well as financial institutions to introduce electronic payment system like ATM and credit cards to reduce the use of cheques and currency in carrying out financial transaction should be intensified and sustained. This will reduce quite a number of financial transactions carried out by means of cheque.

5.5. Money Laundering Malpractice

This is a means by which source or use of money illegally obtained are concealed by converting the cash into untraceable transactions in Banks. It is a means by which the proceeds of illegal business are put into legitimate use to conceal its illegal source. Thus, the cash is disguised to make the income appear legitimate. The true origin of funds is hidden or concealed because the funds could be moved between several institutions and across boundaries. The operations work in various forms. It could be buying securities (stocks and bonds) for cash, the securities are then placed for safe deposit in one bank and a claim on those assets used as collateral for a loan at another bank. The transaction accomplished nothing except to disguise the original source of the fund.[35]

---

[27] (1979) NCLR 472

[28] Trade Bank Plc v. Barilux (Nig) Ltd (2000) 13 NWLR Pt 685 p. 483, UBN Plc v Wokubama (2000) 14 NWLR Pt 688.

[29] Ebhodaghe, J., op. cit. p. 165

[30] Ogunleye, G. op. cit. p. 22

[31] Federal Republic of Nigeria v Johnson Okokon. Reported in EFCC Alert. A Publication of EFCC, No. 1 2 No. 2, Feb. 26, 2007 p. 6

[32] Cap B LFN 2010

[33] Chianu, E. Law of Banking: Texts: Cases: Commentaries (Benin: Enslee Books, 1995) p. 173.

[34] Ibid

[35] (1985 – 1989) 4 NBLR p. 331

5.6. E-Banking Fraud

The evolution of the internet and advances in telecommunications technology has opened up new distribution channels for financial products and services. The internet for example has opened up a number of mechanisms for commercial transactions such as e-commerce, e-banking, e-business or e-payment. Electronic banking is one of the mechanisms evolved through internet for carrying out banking transaction. Many definitions have been given in respect of Electronic banking some of which are restrictive.

Electronic Banking is defined in A-Z dictionary as "banking transactions conducted through computerized system, such as electronic funds transfer by automated teller machines to speed operation, reduce cost etc[36]. This definition appears to be restrictive as it does not take into account electronic banking by means of telephone or mobile or TV banking which are becoming popular.

Joseph Sanusi, former Governor of Central Bank of Nigeria defines Electronic banking to mean the form of banking transaction in which the bank and its customers interact electronically rather than by physical exchanges or direct physical contact.[37] This definition again appears to be restrictive as it extends electronic banking to cover only bank/ customer relationship. Of course, electronic banking could take the form of inter-bank transfer of funds. Therefore, a more acceptable definition would be that electronic banking is a means whereby banking transaction or processes are conducted through the use of electronic media.[38] While the development of e-banking has brought with it new products and ways of doing business, it has also spurned a wide variety of frauds and ways perpetrating them. The nature of perpetration is often over the network, internet or electronic card product hence the term e-banking fraud.[39] Electronic fraud deals with the use of electronic medium to commit fraud. This involves the use of electronic channels such as emails, faxes, mobile phones, credit cards, e-transact channels and other essential electronic medium to perpetrate fraud.[40] Our major concern here is e-banking fraud which is a fragment of e-fraud. Fraud was defined as something dishonest and morally wrong.[41]

In Ifegwu v FRN[42] the Court of Appeal per Aderemi, JCA stated that the word "fraud" is very weighty in the realm of criminal law. It means "deliberate deception intended to gain advantage". To say that fraud is something dishonest and morally wrong is not enough. It goes beyond that and includes any intention to gain advantage. Fraud therefore involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else.

E-banking fraud therefore means any fraudulent conduct of banking transaction or processes through the use of electronic media in order to obtain or gain some unjust advantage. Nigeria which is an English nation has high repute for internet fraud the world over. It is highly populated and has the largest market in Africa. It has the fastest growing ICT market in West Africa and its banking system has undergone the largest industry conveyance in the history of banking in Africa.[43]

The incidence of fraud and forgeries involving some Nigerian banks has assumed alarming proportion. In the year 2004, for instance, there were a total of 1,175 reported cases of attempted fraud and forgeries involving N9.6 billion, US $7.8M and Euro 18,492.00 compared with 1,036 reported cases of attempted fraud and forgeries involving N3.6 billion, US $3.5 million, DM 120 and Euro 850.00 in 2003[44]. Out of this number of incidents, 518 cases were successfully executed by the perpetrators and resulted in losses to banks amounting to N2.6 billion, US $608,721 13 and Euro 18,492.00 in 2004 compared with 369 cases of fraud perpetrated and resulted in losses to banks that amounted to US $882.0 and 895.0 in 2003.[45]

In US, it is not unusual for a Nigerian fraud perpetrator to recruit a bank insider to provide account information. Employees in a bank's customer service department usually have access to all customer accounts via computer in order to assist customers who have questions or complaints about their accounts. Once the employee finds an account with large balance, the account information is compromised and forwarded to the Nigerian armed with this account information, the Nigerian issues wire transfer order directing the bank to transfer large sums into accounts under the control of the Nigerian.[46]

At this juncture, it is pertinent to examine briefly examples of E-banking fraud.

5.6.1. Fund Transfer Fraud

This sometimes involves the interception or alteration of electronic data messages transmitted from the computers of financial institution. It may also involved releasing money transfer information to more than one beneficiary and running round to accuse the banks of paying wrongly. Also, impersonating the real beneficiary of the funds transfer to collect the money has been very rampant.

---

[36] 10th October, 2007. 3pm. A more comprehensive work will be done on this topic under Money Laundering Prohibition Act, 2011.

[37] A – Z Dictionary of Today's American English 3rd ed (New York, Butterworth, 1999) p.4

[38] "Information Technology and Banking Nigeria" Daily Times, Thursday, September 19, 2002 p. 17

[39] Such as Online Real Time Services. Electronic Smart Cards, Swift (Society Worldwide Interbank Financial Telecommunication) Electronic Clearing System, Internet Banking E-mailing Personal Computer banking, telephone banking. Internet banking, TV banking mobile banking, ATM and Repaid valve card.

[40] Nwaze, C., op cit., p. 93

[41] Ribadu, N. "E-fraud: Investigation, Prosecution and Adjudication" in Proceedings of 2005 National Seminar on Banking and Allied Matters for Judges by CIBN (Lagos: CIBN Press Ltd, 2005). P. 79

[42] Nnammi, JSC in Olutanmise v Falana (1990) 21 NSCC (Pt. 2) 97, quoted with approval by the Ajoola, JSC in W.A.B. v Savannah Ventures Ltd (2002) 10 NWLR (Pt 775) 401 at 430, See also FRN v. Ikpe (Supra)

[43] (2001) 13 NWLR (Pt 729) 103 at 132

[44] Contract NLC, 101

[45] Central Bank of Nigeria Annual Report and Statement of Accounts for the year ended 31st Dec.2004 p.17

[46] Ibid

In Nigeria, following several complaints from the public to EFCC over undelivered money sent through the Western Union Money Transfer, two staff of First Bank of Nigeria, Shodi/Mile Two Branch were arrested. They were alleged to have connived with 86 dupes outside the bank to remit money sent through western union money transfer to these dupes other than to their legitimate owners. They were allegedly found with 28 international passports, 5 National ID cards and 43 drivers' licences. These dupes allegedly used these documents to pick up money transferred to the bank.[47] There is the story of Vladimar Levin, a 27 year old Chemistry graduate of St. Pertersburg Technological University, Russia who was accused of effecting electronic transfer of about $11 million from citibanks computer data base in New York to accounts in three banks in Finland, Israel and San Francisco.[48] It is suggested that rigorous verification process should be done before any payment is made in respect of funds transfer.

5.6.2. Identity Theft Fraud

This involves stealing people's password to enter networks to which they do not have authorization and this may create enormous opportunities for fraud to occur. Information may be obtained from insiders (such as dishonest bank or government employees) by fraudulent offers for emplacement or investment. In US, groups of Nigerians using computer programmes have routinely been able to obtain list of credit card companies operating in international commerce. The card numbers are issued through foreign banks to customers who are residents of Great Britain, Germany of other European countries. Nigerians use these stolen credit card numbers to place order for expensive items like computers or automobiles. The buyer provides the stolen credit card number in payment of the purchase.[49] Rasaq Usman who hails from Ilorin, Kwara State was arrested by EFCC in June 2006. He was alleged to have been in possession of a software which he used to generate credit cards that he, in turn uses to order for goods from the United States of America. He generated a credit card belonging to an American lady and used same to order for multi-vitamins valued at $7,500 from a pharmaceutical company in US. The goods were shipped to him through a courier company which he sold to buyers. Luck ran out of him when he was arrested by EFCC men following a tipp-off[50]. It is suggested that sensitive information should be protected from unauthorized disclosure while it is in passage over communication network.

5.6.3. Phishing

Phishing operates by sending forged e-mail, impersonating on-line bank, auction or payment site. The e-mails purport to be official bank request. They ask customers to confirm their online banking details either by e-mail or by entering them into a website. The information thus stolen is used to perpetrate all sort of fraud.

Last year customers of a Swedish bank were duped to the tune of $1.1 million by internet fraudsters. Over 250 customers of the banks were duped into downloading the programme known as "Troyan" after receiving an e-mail purporting to come from the bank encouraging them to do so. The Troyan subsequently monitors the online transaction of the customers picking details and account numbers. Having obtained the account numbers of the customers the fraudsters transfer money from the account of the customers.[51] Most Nigerian banks websites are not up-dated. This makes it prone to any kind of fraudulent activities by fraudsters. It is therefore suggested that banks should constantly monitor and update their websites to avoid same being cloned by fraudsters and use it for criminal activities.

5.6.4. Payment Card Fraud

This basically involves credit card fraud and it takes many forms like stealing payment cards and uses the credit card number to commit online fraud. It may also involve duplication or skimming of card information. This takes many forms like copying credit card number for later use or misuse or copying the magnetic stripe from a payment card while a hidden camera captures the numbers on the face of card. In respect of ATM, a fraudulent card stripe reader would capture the contents of the magnetic stripe while a hidden camera reader would sneak at the users pin. The fraudulent equipment would then be removed and the data used to produce duplicate cards that could then be used to make ATM withdrawals. It is suggested that one should be careful when handling his ATM card. It should not be exposed unnecessarily. Report it immediately it is stolen or misplaced. It is further suggested that people should keep away from freestanding ATM since same is prone to fraudulent manipulations by fraudsters. ATM located in the bank premises should be patronized.

5.6.5. Hacking/Unauthorised Access

This has to do with unauthorized access to the bank's network to defraud the bank. Most times, the hackers rely on any loopholes in the bank's computer network to commit fraud.

[47] Buchanan, J. and Grant, A. "Investigating and Prosecuting Nigerian Fraud in United States Attorneys Bulletin, Nov. 2001 p. 3.
[48] Zero Tolerance, Vol. 1, No. 4 op cit. p. 42
[49] Mekunye, C. "Electronic Banking and the Banker-Customers Relationship Legal Perspectives in modus International Law and Business Quarterly, Vol.5 No. 1 March, 2000 p. 2
[50] Buchanan, J. and Grant A, op cit. p. 3
[51] EFCC Alert, Vol. 2, No. 1 op cit p. 13

6. Some Legal Problems in E-Banking Fraud

The major legal problems associated with E-banking fraud will be discussed here. First, is the problem of proof in electronic banking fraud. The existing legal framework is inadequate to deal with these cases especially quite a number of economic and financial crimes these days are carried out through the use of computers, word processors, telex machines, internet and fax machines.

The evidence status and admissibility of computer and other electronically generated statement of account or print out, emails, telegraphic transfers, telefax etc have been issues of controversy in the courts, law institutions, workshops, bar conferences and similar.[52] We shall briefly look at the opinion of one of the legal luminaries and that of courts.

Prof. Taiwo Osipitan has brilliantly argued for admissibility of computer-generated evidence as primary evidence in proof of bank related cases. He stated thus:

The issue which is of immediate importance, is the status of technology generated documents document like telexes, telegrams, telefaxes and computer print-outs under the best evidence rule. Are they document? If they are documents, are they primary or secondary documents?

…if technology generated evidence are not documents, then they are not admissible as documentary evidence. If however, they are documents, it is still pertinent to investigate their status as primary or secondary documents. If they are primary documents, they are admissible as of right under the best evidence rules otherwise necessary foundation will have to be laid for their admissibility.[53]

The learned author went further on to cite some cases[54] to buttress his point. He contended therefore that telexes, telegrams, facsimiles and computer print-outs are documents, hence they could appropriately be admitted as primary documents under the evidence Act[55]. In form of business records[56] or public documents.[57]

The courts have not been left out in giving support to the argument that technological generated evidence is admissible. As far back as 1969, the Supreme Court in the case of Esso West Africa Inc. v T. Oyegbola[58] had envisaged the need to expand the horizon of the section to include or cover computer which was virtually not in existence or at a very rudimentary stage at that time.

In Ogolo v IMB Ltd,[59] the court adopted a flexible approach. The court of Appeal took judicial notice of modern impact of computer in Banking Business. Also, in the case of R v Daye[60], the court warned as follows:

I should guard myself against being supposed to assent to the argument that anything is not a document unless it be a paper writing.

In the case of Anyeabosi v R.T Biscoe Ltd[61], the Supreme Court confirmed the documentary status of a computerized statement of account. The court had on the basis of the arguments canvassed by both counsel endorsed the admissibility of the computerized statement of account as secondary evidence.

The courts have in their wisdom given good judgment based on their interpretation of the existing laws and the need to apply them to modern practices but the problem still remains that as of today there is no concrete law of evidence as it relates to e-banking in Nigeria.[62] For electronic banking transaction, the evidence for the most part will be computer or electronically generated. The academic view on the point in Nigeria is that as in UK, the evidence Act must be amended before the computer generated evidence can be established.[63]

However, the law reform efforts produced the proposed "Evidence Decree 1998" (Now Act) which is yet to be passed into law. The decree (Now Act) specifically incorporated computer evidence into the law instead of reliance on judicial notice. It also widened the meaning of document, to include documents generated from any electronic device, but it is yet to be passed. It is therefore suggested that the National Assembly should take steps to pass the proposed Act into law so as to update law of evidence.[64]

Besides, in a case involving identity theft through phishing and other modern methods of bank fraud, absolute reliability on computer evidence would be suspect and unrealistic. This is because several examples abound at the US Federal Trade Commission Website of unsuccessful attempts by enforcement agents to locate phishers or spam originators. In order to punish fraud perpetrators, one must locate them. The current state of internet technology makes this difficult. Finding the wrong doer is an important aspect of all law enforcement agents. In view of the mechanism existing in internet processes it allows for anonymous communications that are virtually impossible to trace.[65] Any law on electronic banking fraud must make provision to deal with this type of problem.

---

[52] Charles Isiwe "Nigerian Banks and Internet Fraud" Daily Times, Monday, Feb, 12, 2007 p. 8

[53] Arise, A. "The Legal Framework for E-banking and E-Commerce in Nigeria: Issues, challenges and the way forward" in Proceedings of 2005 National Seminar on Banking and Allied Matters for Judges (Lagos: CIBN Press Ltd, 2006) p. 44.

[54] Legal impact of Technology on Rules of Evidence in Banking and Commercial Litigation in MJFIL Vol. 2. No. 4. 1998 pp 78 – 79 at p. 10

[55] Senior v Holdsworth (1975) 2 All ER 1009: R v Robiason (1992) All ER 699, R. v Day (1906) 2 KB 333

[56] Cap E LFN 2004

[57] Section 57 of Evidence Act, 2011

[58] Section 58 of Evidence Act, 2011

[59] (1969) NMLR 194 at 198

[60] (1995) 9 NWLR (Pt 419) at p. 324

[61] (Supra)

[62] (1987) 3 NWLR (Pt 59) p. 84

[63] Arise, A., op. cit p. 45

[64] Mekwunye, C. op. cit p. 85

[65] Oyewo, O. "Legal Implications of Electronic Banking in Nigeria" In Modern Practice Journal of Finance and Investment law, Jan/April, 2003. Vol. 7 Nos. 1 – 2.

Added to the above is the issue of jurisdiction. The cyberspace commerce involves a trade across national boundaries hence cybercrime can be committed across border lines. In the event that the person who commits the fraud is located, it is possible for such perpetrator to be in another country outside the legislative jurisdiction of the plaintiff.[66] This is a case across the world now. This issue came up in FRN v Jagun[67] the accused person charged before the High Court of Lagos State for issuing a fraudulent cheque in United States of America in payment of goods some of which were sent to him in Nigeria through the UPS headquarters, Lagos and some he had disposed of them in USA. The defendant/appellant brought an application to the High Court challenging the jurisdiction of the trial court on the ground that the facts of the charged disclosed that the goods in question were obtained from United States of America, a place clearly outside the jurisdiction of the honour court.

The court held, inter alia, that having received the goods in the US before disposing some of them and shipping the rest to Nigeria the offence would appear to have been completed in the United States of America and a Nigerian court is bereft of jurisdiction. Assuming a Nigerian commits fraud in US and runs back to Nigeria to avoid arrest whereas the victim resides in US, what legal remedies are available to the victim? As at 1998, fifteen foreign businessmen and who American citizens were murdered in Nigeria in connection with advance fee fraud.[68] It has been argued that a mutual legal Assistance Treaty between Nigeria and US is not yet in force and this has made extraction of fugitives from Nigeria to US difficult.[69] It is submitted that this assertion is not true in view of the fact that there are requisite legislations governing extradition between Nigeria and United States. The Court of Appeal in George Udeozor v Federal Republic of Nigeria[70] listed the various legislations governing extradition between Nigeria and US. A number of Nigerians have been extradited to US. One of the fraudsters Enginnaya Nwokeafor was on the wanted list of the United States Postal Service. He fled Holland to Nigeria. He had posed as a wealthy old man suffering from throat cancer, a terminal condition and who needed a trust worthy agent to help dispense a 55 million dollar charity fund to the less privilege in US, as he would not be able to travel from Amsterdam to USA. A victim having received a scam letter sent $38,000 through Western Union Money Transfer in Amsterdam. The victim also sent another $75,000 dollars as clearance for anti-drug/terrorist fee based on the request from Enyinnaya. The victim further paid $100,000 to clear the two boxes containing the #55,000 dollars having purportedly been seized by custom to the victim. He was arraigned in absentia before United States District Court in New York upon indictment of conspiracy, Bank fraud, mail fraud and wire fraud. He was arrested in Nigeria by EFCC and upon request from US, he was extradited to the United States for trial.[71]

In relation to contracts, some presumptions have been developed by the courts for the purpose of ascertaining the proper law to apply in cross-border transactions and this applies to electronic banking transactions.[72]

i. Where there is no express choice of law which is more likely in practice, the country where the contract is made.
ii. The country where the contract is to be performed.
iii. If the contract relates to immovable, the country where they are situate.
iv. The court will also put into consideration relevant surrounding circumstances which will include matters such as the residence and domicile of the parties.

In view of the problems created by electronic banking fraud and other cyber crime, there have been local and international initiations to tackle the problems through legislations. Some of these efforts would be highlighted here and others will be discussed in the subsequent chapters.

In 2003, the Central Bank of Nigeria released the guidelines on Electronic Banking in Nigeria. The main intent of the guidelines was to define technical requirements and the permissible scope of electronic banking for Nigerian Banks.[73] However, the Guidelines are not without some short-comings. For instance, all banks intending to offer transactional services on internet and other e-banking products should obtain approval in principle from the Central Bank of Nigeria prior to commencing these services.[74]

Furthermore, the standard for security and privacy are not specifically outlined in the Guidelines. It lacks the procedures for promoting customer's access to e-banking service. The Guidelines are only meant for banks offering e-banking products but not extended to operators of cybercafé who are more likely to be involved in cyber crime. Lastly, it lacks legal backing and therefore enforcement becomes difficult.

The Nigeria Cybercrime Working Group (NCWG) was established in 2003 under the chairmanship of Attorney General of the Federation and Minister of Justice. The new body has since 2004 been working in a project titled "National Cyber Security Initiative" which is aimed at developing cyber crime and cyber security regulations in the country. These efforts have culminated into a draft proposal the "Computer Security and Critical Infrastructure Protection Act" which is currently waiting to be passed to law by the National Assembly. Some of the intents of the proposed law are to create a central institution, (National Cybercrime Working Group) that will be responsible for the enforcement of its provision, and to seek to regulate the security of computer systems and networks and

---

[66] Arise, A., op. cit p. 45209
[67] Ibid
[68] (2006) 1 EFCCR p.
[69] Burchanam, J. and Grant, A. op. cit. p. 47
[70] Ibid
[71] (2007) 15 NWLR (Pt. 1058) at 67, These include the Extradition (United States of America) order of 1967 published in the special Gazette No. 23 Vol. 54 of 13th April, 1967, Extradition Act Cap E 25 LFN 2004. Evidence Act, Cap E 14 LFN 2004, CPA, Legal Notice No. 33 of 1967 and the 1999 Constitution.
[72] Zero Tolerance Vol. No. 4 op. cit. p. 27
[73] Mekwunye, C. *op. cit*. p. 54
[74] Ezeoha, A. *op cit*

protect sensitive ICT infrastructure[75]. The new law when promulgated seeks to prohibit three main classes of conduct, namely: (1) conduct against computer systems, with offence in this category made up of activities like unauthorized access to computer systems, access exceeding authorization, computer systems and Network interference, system intrusion, data interception, denial of service, computer trespass, e-mail bombing (2) conducts utilizing ICT system to commit unlawful acts or crimes, covering such offences as computer containing illegal communication, computer vandalism, cyber-squatting, cyber-pornography, online intellectual property theft and (3) Unlawful conduct against critical ICT infrastructures in Nigeria.[76] The above proposed computer security and critical Infrastructure Protection Act appears to prohibit only conduct relating to unauthorized access or tempering with computer systems. It does not cover conduct relating to wire and other electronic communication. These include fraud relating to tempering with telegram, telex, telefacsmile, electronic and mobile telecommunication (GSM).

In USA, there is a Wire Fraud Act, a legal concept in the United States code which provides for enhanced penalty of any criminally fraudulent activity if it is determined that the activity involved electronic communications of any sort at any phase of the event. It is a crime codified at 81USC & 1343 and states as follows:

Whoever, having devised or intending to devise any scheme, artifice to defraud, or for obtaining money or property by means of false or fraudulent practices, representations, or promises transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings signs, signals, pictures or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned for more than 30 years or both.

The above code makes specific provision for punishment where the violation affects a financial institution and even provides tough penalty. Also, the Electronic Communication Act of 1986 made the private, unauthorized interception of electronic communication illegal and punishable as a felony with a fine and up to five years imprisonment. On the Global scene, there is the Nigerian Crime Initiative launched in US in 1995 which was aimed at combating international organized crime. It developed the Anti-Drug Network (ADNET) computer system for collecting and tracking data relating to Nigerian crime. Since Nigeria does not have a specific Nigerian legislation on Electronic banking, can the Unicitral Legal Guide on Electronic Fund Transfer apply in Nigeria? It is submitted that it cannot apply in Nigeria since they do not have the force of law in Nigeria and Nigeria has not adopted it.

It is therefore our suggestion that in the meantime that there is absence of specific Nigerian legislation on electronic banking, to deal with cases of electronic bank fraud, Nigeria should adopt the UNICITRAL Legal Guide on Electronic Fraud, losses and errors. The Advance Fee Fraud and other Fraud and other Fraud Related Offences Act, 2006 provides for electronic communication offences. We submit that this legislation is insufficient to deal with cases of e-fraud especially cyber crime as it merely scratches the surface of it.

It is submitted that the above Act only provides for obligations on the part of the operators of electronic communication or remote computing service to obtain customers' or subscribers' identity (KYC) and offences for failure to do so. It does not provide for offences relating to identify fraud and unauthorized access to ICT facility which has been sufficiently dealt with in the proposed Computer Security and Critical Infrastructure Protection Act now before the National Assembly for passage into law.

Furthermore, under the proposed Computer Security and Critical Information Act there is a provision for the creation of National Cybercrime Working Group that will be responsible for the enforcement of its provisions and to seek to regulate the security of computer systems and networks and protect sensitive ICT infrastructure. Indeed, the EFCC is not sufficiently equipped to carry out these functions.

It is suggested therefore that the National Assembly should as a matter of urgency pass the proposed computer security and critical infrastructure protection Act into law.

Furthermore, proposed computer security and critical Information Protection Act now before the National Assembly should be reviewed to incorporate provisions seeking to prohibit conduct relating to unauthorized assess or interference with electronic and other communication devices as in US code against wire fraud.

The proposed Act should also be reviewed to provide specific punishment against E-fraud in the financial institutions and the punishment should be such that will serve as a deterrent to intending violators.

Furthermore, special emphasis should be placed on identify fraud. Internet banking laws and policies no matter how efficient and comprehensive only makes sense in the presence of necessary ICT Infrastructural facilities. To further check incidences of electronic banking fraud, there is need to have a law that will bind parties together in electronic transactions. One of the most critical components of any successful market economy to the digital environment is the existence of the rule of law and enforcement of written agreements and transactions that follow pre-determined rules of notice disclosure of rights and obligations. All things being equal when parties know that the signature guarantee accountability, that they gain benefits and at the same time undertake certain obligation in Nigeria their behaviour is necessary shaped by the contract which result when parties are contractually bound.

The traditional contract law which requires certain transactions to be in writing will pose serious problem that will definitely hinder electronic commerce in Nigeria. Therefore, the passing into law of an e-signature Act will provide for digital signatures and also make electronic documents as valid as hand written ones.

[75] Section 61, Par. 21, CBN Report of the Technical Committee on Electronic Banking Feb. 203.

[76] Daily Sun Newspaper, 2004 cited in Ezeoha, A. *op cit.* p. 2

7. Conclusion

It is not in doubt that malpractices committed by bank customers have negative effects on the banking industry in Nigeria. Indeed, malpractices committed by bank customers have contributed to the collapse of many banks in the banking industry in Nigeria. The sad story is that some of these malpractices are committed by the bank customers with the active connivance of the bank employees.

Unfortunately, some of the malpractices like e-banking fraud, there is still no legal framework to deal decisively with the situation, thereby giving room for increased cases of e-banking fraud. The existing legislations do not have adequate provisions to deal with the situation. Even where there are provisions, the increased sophistication and new techniques in the way and manner the perpetrators of the crime carry out their illegal act necessitates stringent measures to be introduced in the law to make it more effective to address these challenges.

The banks, government and the regulatory institutions have a role to play to ensure sanity in the banking industry. The National Assembly should as a matter of urgency pass cybercrime Bill into law.

Banks should tighten its internal control measures and enforce sanctions against breaches by bank employees who connive with bank customers to perpetrate the illegal act.

8. References

i. Ebhodaghe, J. "Malpractices in the Banking Industry: Nature. Types. Causes and Remedies". In Safe and Sound Banking Practices in Nigeria: Selected Essays. (Lagos: Page Publishers Services Ltd, 1997) P. 160.
ii. Ibid
iii. Edhodaghe, J. op. cit, p 160
iv. Encyclopedic Edition, (Typhoon International Corporation, 2003) p. 112.
v. New Word Dictionary, 2nd edition Siman and Scluster: p. 140
vi. Thompson West Publishing, 2004, 8th edition p. 102
vii. Malpractice in the Banking Industry: Nature, Types, Causes and Remedies in Safe, Sound Banking Practice: Selected Essays, op p. 161
viii. "Malpractice in the Banking Industry". Ajibola B and Awa, U.K. (eds) in Banking and Other Financial Malpractices in Nigeria (Lagos and Oxford, Mulhouse Press, 1990) p. 14.
ix. "Eradication of Banking Malpractices in Nigeria. "Will Law Alone Succeed"? In CBN Economic and Financial Review Vol. 33, No. 1 March 1995, p. 62.
x. The United States Bureau of Investigation, in a working definition of crimes, states of white-collar, crimes: "those illegal acts characterized by deceit, concealment, violation of trust and not force or violence. They are committed to obtain money, properly or services; or to avoid the personal or business advantage". See GAO Report Resources developed by the Department of Justice to combat white-collar crimes and punish corruption, March, 19. 1979.
xi. Idoko, A. "White-collar crimes" in Nigerian Commercial Law; Problems and Perspective. (Dept. of Commercial Law, Ahmadu Bello University, Zaria, 1984), p. 22.
xii. Bill of Exchange Act No. 20 of 1964
xiii. Ibid. It is not contained in the Bill of Exchange Act Cap B8 LFN 2010
xiv. Ladbroke and Company v. Todd (1914) 30 FLR 433
xv. (1901) AC 414
xvi. Matthews v Brown Vol. 10 TLR
xvii. (1920) AC 683
xviii. Ibid
xix. HedlyBryne and Company Ltd v Heller and Partners (1960) AC 465
xx. Buchanan, J. "Investigating and Prosecuting Nigerian Fraud," US Bulletin Nov. 2001, See Section 419 of the Criminal Code Cap C38 LFN 2010.
xxi. Ribadu, N. "Implication of Economic and Financial Crimes on the Nation's Economics" being a Paper Presented to Defence Adviser Conference in Abuja on the 10th Sept. 2004 p. 5.
xxii. Ibid p. 6
xxiii. Alake v The State (1991) 7 NWLR (Pt. 205) 567 Onwudiwe v FRN (2006) 49 WRN 1 at 71
xxiv. Cited in Penington& Hudson Commercial Bank Law (London, Macdonald & Evans, 1978) p. 248
xxv. Cap C38 LFN 2004
xxvi. Udok, U., The Law of Sale of Goods in Nigeria (Uyo: Kan Educational Books, 2004) p. 132.
xxvii. (1979) NCLR 472
xxviii. Trade Bank Plc v. Barilux (Nig) Ltd (2000) 13 NWLR Pt 685 p. 483, UBN Plc v Wokubama (2000) 14 NWLR Pt 688.
xxix. Ebhodaghe, J., op. cit. p. 165
xxx. Ogunleye, G. op. cit. p. 22
xxxi. Federal Republic of Nigeria v Johnson Okokon. Reported in EFCC Alert. A Publication of EFCC, No. 1 2 No. 2, Feb. 26, 2007 p. 6
xxxii. Cap B LFN 2010
xxxiii. Chianu, E. Law of Banking: Texts: Cases: Commentaries (Benin: Enslee Books, 1995) p. 173.
xxxiv. Ibid

xxxv. (1985 – 1989) 4 NBLR p. 331
xxxvi. 10th October, 2007. 3pm. A more comprehensive work will be done on this topic under Money Laundering Prohibition Act, 2011.
xxxvii. A – Z Dictionary of Today's American English 3rded (New York, Butterworth, 1999) p.4
xxxviii. "Information Technology and Banking Nigeria" Daily Times, Thursday, September 19, 2002 p. 17
xxxix. Such as Online Real Time Services. Electronic Smart Cards, Swift (Society Worldwide Interbank Financial Telecommunication) Electronic Clearing System, Internet Banking E-mailing Personal Computer banking, telephone banking. Internet banking, TV banking mobile banking, ATM and Repaid valve card.
xl. Nwaze, C., op cit., p. 93
xli. Ribadu, N. "E-fraud: Investigation, Prosecution and Adjudication" in Proceedings of 2005 National Seminar on Banking and Allied Matters for Judges by CIBN (Lagos: CIBN Press Ltd, 2005). P. 79
xlii. Nnammi, JSC in Olutanmise v Falana (1990) 21 NSCC (Pt. 2) 97, quoted with approval by the Ajoola, JSC in W.A.B. v Savannah Ventures Ltd (2002) 10 NWLR (Pt 775) 401 at 430, See also FRN v. Ikpe (Supra)
xliii. (2001) 13 NWLR (Pt 729) 103 at 132
xliv. Contract NLC, 101
xlv. Central Bank of Nigeria Annual Report and Statement of Accounts for the year ended 31st Dec.2004 p.17
xlvi. Ibid
xlvii. Buchanan, J. and Grant, A. "Investigating and Prosecuting Nigerian Fraud in United States Attorneys Bulletin, Nov. 2001 p. 3.
xlviii. Zero Tolerance, Vol. 1, No. 4 op cit. p. 42
xlix. Mekunye, C. "Electronic Banking and the Banker-Customers Relationship Legal Perspectives in modus International Law and Business Quarterly, Vol.5 No. 1 March, 2000 p. 2
l. Buchanan, J. and Grant A, op cit. p. 3
li. EFCC Alert, Vol. 2, No. 1 op cit p. 13
lii. Charles Isiwe "Nigerian Banks and Internet Fraud" Daily Times, Monday, Feb, 12, 2007 p. 8
liii. Arise, A. "The Legal Framework for E-banking and E-Commerce in Nigeria: Issues, challenges and the way forward" in Proceedings of 2005 National Seminar on Banking and Allied Matters for Judges (Lagos: CIBN Press Ltd, 2006) p. 44.
liv. Legal impact of Technology on Rules of Evidence in Banking and Commercial Litigation in MJFIL Vol. 2. No. 4. 1998 pp 78 – 79 at p. 10
lv. Senior v Holdsworth (1975) 2 All ER 1009: R v Robiason (1992) All ER 699, R. v Day (1906) 2 KB 333
lvi. Cap E LFN 2004
lvii. Section 57 of Evidence Act, 2011
lviii. Section 58 of Evidence Act, 2011
lix. (1969) NMLR 194 at 198
lx. (1995) 9 NWLR (Pt 419) at p. 324
lxi. (Supra)
lxii. (1987) 3 NWLR (Pt 59) p. 84
lxiii. Arise, A., op. cit p. 45
lxiv. Mekwunye, C. op. cit p. 85
lxv. Oyewo, O. "Legal Implications of Electronic Banking in Nigeria" In Modern Practice Journal of Finance and Investment law, Jan/April, 2003. Vol. 7 Nos. 1 – 2.
lxvi. Arise, A., op. citp. 45209
lxvii. Ibid
lxviii. (2006) 1 EFCCR p.
lxix. Burchanam, J. and Grant, A. op. cit. p. 47
lxx. Ibid
lxxi. (2007) 15 NWLR (Pt. 1058) at 67, These include the Extradition (United States of America) order of 1967 published in the special Gazette No. 23 Vol. 54 of 13th April, 1967, Extradition Act Cap E 25 LFN 2004. Evidence Act, Cap E 14 LFN 2004, CPA, Legal Notice No. 33 of 1967 and the 1999 Constitution.
lxxii. Zero Tolerance Vol. No. 4 op. cit. p. 27
lxxiii. Mekwunye, C. op. cit. p. 54
lxxiv. Ezeoha, A. op cit
lxxv. Section 61, Par. 21, CBN Report of the Technical Committee on Electronic Banking Feb. 203.
lxxvi. Daily Sun Newspaper, 2004 cited in Ezeoha, A. op cit. p. 2