LEGAL CHALLENGES POSED BY ELECTRONIC BANKING IN NIGERIA

Abstract

Electronic banking has come to stay in Nigeria. Is the Nigerian legal system, especially the law of banking, properly structured to address the legal challenges that arise from the use of electronic banking? Thankfully, the recently passed Cybercrimes (Prohibition, Prevention, etc) Act 2015 has covered some of the criminal aspect of electronic banking by its penal provisions. However, in bank/customer relationship, the ability for any aggrieved party to seek redress for a civil wrong inn a court of law must be met by adequate legal provisions in the area of civil law that deal with such dispute.

This article looks at the evolvement of banking business in Nigeria, from the hitherto customer-bank teller relationship to the prevalence of platforms for electronic banking, outside banking halls and note that the Banking and Other Financial Institutions Act (BOFIA) is outdated in regards to electronic banking. This work also examines the several legal challenges that arise from electronic banking, especially in the area of inadequacy of substantive law, criminal law, money laundering/terrorism, electronic signature and consumer protection.

What is Electronic Banking?

Electronic banking (e-banking) is also known as Electronic Funds Transfer (EFT),[1]

---

[*] S. T. James (Mrs), Lecturer Nigerian Law School Lagos Campus & Monyei Chukwuemeka, Legal Practitioner, Lagos.

[1] Federal Trade Commission, Consumer information, electronic banking at www.consumer.ftc.gov/articles/0218-electronic-banking. Last assessed 17 October 2015.

It is difficult to define what constitutes e-banking, or electronic funds transfer, as there is no e-banking specific legislation in Nigeria just as there is the Payment Services Directive (PSD) in the EU and the Electronic Fund Transfer Act in the United States.
The Central Bank of Nigeria Guidelines on Electronic Banking in Nigeria[2] does not define the term 'electronic banking' anywhere in its provisions. However, in the Report of the Technical Committee (of the Central bank of Nigeria) on Electronic Banking[3], Electronic Banking was defined as a means whereby banking business is transacted using automated processes and electronic devices such as personal computers, telephones, fax machines, internet, card payments and other electronic channels."[4]

The Cybercrimes (Prohibition, Prevention, etc) Act which was signed into law in May, 2015 does not have electronic banking as its main objective[5] but it has provisions that touch on the electronic systems of financial houses. Electronic Transfer of fund is defined under the Act as *any transfer of funds which is initiated by a person by way of instruction, authorization or order to a bank to debit or credit an account maintained with that bank through electronic means and includes point of sales transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfer initiated by telephone, internet and card payment*".[6]

Central to the concept of electronic banking or electronic funds transfer are:

a) That instructions are issued by electronic means,
b) That the electronically issued instruction is directed to an intermediary, usually a financial institution, and
c) That the electronically issued instruction instructs the intermediary to credit or debit an account.[7]

Electronic banking therefore, did not change the core of banking business in Nigeria[8] but it revolutionized the modes by which deposits, transfer of

2 The Report of the Technical Committee" .Available at www.cenbank.org/out/publications/bsd/2003/e-banking.pdf. Last accessed 17 October 2015.
3 Available at www.cenbank.org/out/publications/bsd/2003/e-banking/pt4.pdf. Last accessed 17 October 2015.
4 See par. 1.2, pg 6 of the Report of the Technical Committee.
5 See sec. 1 of the Cybercrimes (Prohibition, Prevention, etc) 2015 - "The Cybercrimes Act", for its three objectives.
6 Sec. 58 ibid.
7 Legal and Regulatory Framework in E-payment Environment, par. 23, pg2; Paper prepared by Prof. 'Konyin Ajayi, SAN (with Muyiwa Balogun, Deji Arowolo & Godswill Iwajokuw) of Olaniwun Ajayi LP for the International Payments Systems Conference 2013 organized by the Central bank of Nigeria.
8 'Banking business' is defined under section 66 of the Banking And Other Financial Institutions Act 1991 to mean "the business of receiving deposits on current account, savings account or other similar account, paying or collecting cheques, drawn by or paid in by customers; provision of finance or such other business as the Governor may, by order published in the Gazette, designate as banking business"

funds/third party payments, and drawing up of cheques are conducted, from the hitherto paper based techniques (involving the use of passbooks, deposit slips, cheques) to electronic means.

The definition of *electronic fund transfer* in the Cybercrimes[9] lists these electronic means to include point of sales transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfer initiated by telephone, internet and card payment but it in reality, electronic means employed in e-banking are not limited to these.

From early times up till now, the crux of banking has not changed, as much as the essential essence of business-buying and selling- has not changed. For varied reasons, including safety and security, individuals have always kept currency or precious article other than money with themselves and this involves the deposit of the cash/article with another trusted party, with some commission often accruing to that 'other' party. That money will at some point be withdrawn by the individual that deposited same. Such an individual may also need some capital for a project and the person who holds currency/cash deposited may loan to the individual some of the cash belonging to those who have deposited money with it, with interest to be paid on the loan sum. This is essentially what commercial banking entails.

The means of doing the above have become more regulated over time as responsibilities, roles and rights had to be properly defined. The banking industry in Nigeria has been said to have evolved in four stages viz; the unguided laisses-faire phase (1930-1959), during which several poorly capitalized and unsupervised indigenous banks failed before their tenth anniversary; the controlled regime (1960-1985), during which the Central Bank of Nigeria (CBN) ensured that only "fit and proper" persons were granted banking license, subject to a minimum paid-up capital; the post-Structural Adjustment Programme (SAP) or decontrolled regime (1986-2004), during which the banking licenses were freely dispensed on the basis of political patronage and the emerging forth stage which is the era of consolidation (since 2004) with major emphasis on recapitalization and proactive regulation based on prudential principles.[10]

The increased regulation of the banking industry was also necessitated because of the evolvement, over time, in the modes of conducting banking

[9] Section 58 of the Cybercrimes Act, 2014.

[10] Pg. 14, National Open University of Nigeria: Banking Laws and Regulations Course Guide. Available at www.nou.edu.ng/uploads/NOUN_OCL/pdf/SMS/BFN%20305.pdf last assessed October 17 2015.

business. Paper-based payment techniques have been employed before the advances, over the course of the last two to three decades, in information communication technology (ICT). Under the paper based system for instance, a bank customer wanting to make a deposit will be required to fill a deposit slip and hand same to bank teller who completes that deposit. A customer will be required to fill a leaf of a passbook/ withdrawal slip or draw up a cheque to effect withdrawal or transfer of a sum from his account. This often took place in banking halls.

Today, a bank customer can withdraw, deposit or transfer money to another account without having to step into a banking hall. This has been made possible through the advances in ICT that have made banking business possible over the telephone, by an Automated Teller Machine, over the internet, among others. With advances in ICT, particularly the internet, the traditional conception of markets as fixed places where buyers and sellers physically converge for the conduct of commerce has long been thrown out of the window.[11]

History of E-Banking in Nigeria

The introduction of electronic means of banking has been traced to the Structural Adjustment Programme (SAP) initiated in 1986 by the Babangida Administration.[12] The SAP changed not only the structure but also the content of banking business. Just as the number of banks grew tremendously from 40 in 1985 to 125 in 1991, the SAP made possible the licensing of more banks which poised more threat to existing ones and the more aggressive the marketing techniques adopted by them.[13] In the process of the intense competition, adoption of electronic banking was seen as a necessity to maintaining a good competitive position and the journey started in November, 1990 when Societe General Bank launched the first Automated Teller Machine.[14]

In the Report of the Technical Committee on Electronic Banking, it was stated that a survey was conducted in September 2002 to determine the level and types of e-banking activities carried out by banks. The survey showed that; seventeen (17) banks were offering internet banking; twenty-

---

[11] See R. Azam, "Global Taxation of Cross-Border e-Commerce Income" (2012), 31 *Virginia Tax Review*, 639-693, at 647-648. See also, T. Thierer *et al*, "The Commerce and Trust in Electronic Payments" (2005), 24, *Computer and Security*, 10-15 as cited in Legal and Regulatory Framework in E-payment Environment, par. 23, pg2; Paper prepared by Prof. 'Konyin Ajayi, SAN (with Muyiwa Balogun, Deji Arowolo & Godswill Iwajokuw) of Olaniwun Ajayi LP

[12] Pg 2-3, *International Journal of Economic Development Research and Investment*, Vol. 2, No 1; April 2011, Electronic Banking in Nigeria: Challenges of the Regulatory Authorities and the Way Forward. Adewuyi, I.D.

[13] Ibid.

[14] Ibid.

four (24) were offering basic telephone banking; seven (7) had ATM services, while 13 of the banks indicated that they were offering other forms of e-banking. Twelve (12) of the banks indicated that their websites were hoisted in Nigeria while 22 were hoisted overseas. Fourteen (14) of the websites were information only, eleven (11) were information transfer system while 22 were transactional.[15] The Report went on to list some of the electronic services that had been introduced by the banks to include: Personal Computer (PC) Banking; Telephone Banking; Automated Teller Machines (ATM); Internet Banking and Cards. It was found that the number of ATMs had increased from 3 in 2000 to 68 in 2002. The Report also found that mobile phones were increasingly being used for financial services.[16]

In relation to electronic payments, it was found that the most common channel of electronic payments delivery in Nigeria was the smart card and that the full range of electronic transactional banking, such as funds transfer via the internet, had experienced limited growth, as there was very limited operational online (web based) payment systems in country.[17]

Just as there was a sharp rise in the use of electronic banking in Nigeria, between the time of the setting up of the first ATM in 1990 and September 2002 when the survey was conducted, sharp increase was also noticed, in the spread and employment of electronic banking in Nigeria between 2002 and 2014. According to the Central Bank of Nigeria Financial Stability Report 2014,[18] as of December 2014 there were 15,935 ATM terminals; 34,561 PoS terminals; and the volume of transactions over ATM, POS, Mobile, and Internet (web) combined rose to 255,820,046 valued at N2,446.00 billion.[19] The above statistics indicate that electronic banking has become entrenched in Nigeria as a means of banking business.

Legal Challenges Associated with Electronic Banking

The instrument of Law is employed by all states to define relationships and indeed, several laws are enacted in Nigeria to regulate different human relationships[20]. Case law has also defined several relationships not expressly defined in statutes. Section 258 of the Evidence Act 2011 defines

[15] Page 6 of the Report of the Technical Committee on Electronic Banking

[16] ibid.

[17] ibid.

[18] Table 4.1. pg. 77, ibid.

[19] Pg. 77, ibid.

[20] First of all, the Constitution of the Federal Republic of Nigeria 1999 (as amended) sets down provisions that establish and regulate the relationship between individuals living in Nigeria, the government of Nigeria and the people of Nigeria, Nigeria and other countries etc. The Matrimonial Causes Act (MCA) and the Marriage Act regulate marital relationships; the Companies and allied Matters Act (CAMA) regulates the relationships between individuals who come together to form a business or non-business organization; and many other enactments.

bank/banker to mean a bank licensed under the Banks and Other Financial Institutions Act Cap. B3LFN, 2004 and includes anybody authorised under an enactment to carry on banking business. The Court in *NDIC v Okem Enterprises Limited*[21] defined a customer of a bank as any person having an account with a bank or for whom the bank has agreed to collect items and includes a bank owning an account with another bank.

In the English case of **N. Joachimson v. Swiss Bank Corporation**[22], Lord Atkin stated thus; *The relation of banker and customer is that of debtor and creditor with the super added obligation to honour the customer's cheque to the amount of the moneys standing to his credit in his current account*. The Banks and Other Financial Institutions Act encapsulates what this relationship entails in its definition of banking business. It is defined under section 66 as *the business of receiving deposits on current account, savings account or other similar account, paying or collecting cheques, drawn by or paid in by customers; provision of finance or such other business as the Governor may, by order published in the Gazette, designate as banking business*. It is trite that banking business is contractual in nature and benefits and obligations arise from same.

It has been stated and explained earlier in this work how electronic banking has altered the modes by which banking business is now conducted in Nigeria.[23] However, electronic banking also has its challenges. These challenges are not just legal but also affect other areas-regulatory, economic, social etc). As it is with technological advances, electronic banking would naturally lead to the reduction in bank employees as banking business shifts from the hitherto banking hall transactions to transactions over electronic means. This work is however concerned with the legal challenges of electronic banking. By legal challenges, what are contemplated are the challenges arising from electronic banking, affecting the state, customers, banks and third parties, for which there are inadequate legal provisions or no provisions at all. In examining these challenges, it is needful to first examine the major laws regulating banking in Nigeria and how the laws provide for electronic banking, if at all.

---

[21] (2004) 10 NWLR (Pt. 880).

[22] [1919] 707, 1289.

[23] See pg. 2 of this work.

1. INADEQUACY OF THE LEGAL FRAMEWORK CONTROLLING ELECTRONIC BANKING IN NIGERIA

i. Central Bank of Nigeria (Establishment) Act 2007

This Act repealed the Central Bank of Nigeria Act 1991 and established the Central Bank of Nigeria (CBN). One of the principal objects of the Act is the promotion of a sound financial system in Nigeria[24] and in furtherance of this object, section 47(2) provides that the Bank shall continue to promote and facilitate the development of efficient and effective systems for the settlement of transactions (*including the development of electronic payment systems*). Thus, by this provision, the CBN was now obligated, statutorily, to co-ordinate the development of electronic banking in Nigeria.

However, prior to the 2007 Act, the CBN had already laid down guidelines for electronic banking in Nigeria. The Bankers' Bank[25] had in August 2003 issued Guidelines on Electronic Banking in Nigeria.[26] This followed the Report of the Technical Committee on E-banking set up by the bank.

These guidelines were laid down in line with the three major roles of the CBN in the area of monetary policy, financial system stability and payments systems oversight[27]. They touch on technology and security standards; standards on security and privacy; monetary policy; legal issues; regulatory and supervisory issues; Reporting requirements; and penalties.

One of the major challenges with the Guidelines is that it does not serve as a proper regulation of e-banking in Nigeria. Even the penalties imposed by the Guidelines are merely on banks that fail to seek CBN approval before launching, implementing or enhancing electronic banking services/products[28] and for failing to submit, within the prescribed deadline, the required information/documents.[29]

---

[24] Section 2d of the Central Bank of Nigeria (Establishment) Act 2007.
[25] As the CBN is also referred to.
[26] "The Guidelines" . Available at www.cenbank.org/out/publications/bsd/2003/e-banking.pdf.
[27] See the Preamble to the Guidelines.
[28] See par. 4.4.1a of the Guidelines.
[29] See par. 4.4.2b.

Banking business is essentially between the banker and the customer and the CBN plays a supervisory role over banks and it laid down the Guidelines in line with its role. Aside these guidelines, the CBN also issued Regulatory Framework for Mobile Payment Services in Nigeria; Standards and Guidelines on Automated Teller machine (ATM) Operations in Nigeria; and Guidelines on Point of Sale (POS) Card Acceptance Services.

These guidelines and regulations are from comprehensive, and, fall short of a definitive legal and regulatory framework for e-payment-addressing only small pockets of the elements that a definitive e-payment legal framework ought to address, focusing more on operational matters and far too little on addressing and allocating legal risks unique to e-payments.[30]
As it relates to the allocation of legal risks, at any event, doubts abound as to whether given the rooting of the CBN guidelines and regulations (implied power under mandate to foster development of efficient and effective payment systems), the CBN can as between the financial institutions which it regulates, and users of e-payment services that it does not regulate, validly allocate liability. Further doubt in this regard is occasioned by the lack of clarity as to the interface between the CBN liability allocation rules and rules of general law relating to contracts, tort, etc.[31]

Therefore, any legislation on electronic banking must properly define roles, benefits and liabilities that arise in the course of electronic banking. The Payment Services Directive (PSD) which deals with the legal framework for e-payment in the European Union (EU) and the Uniform Commercial Code and Electronic Fund Transfer Act of the United States regulate, among other things, E-payment service providers[32]; payment finality rules;[33] Access to funds[34]; Revocability of e-payment[35]; liability for fraud and mistaken payments.[36]

As of 2003, the Technical Committee of the Central Bank of Nigeria noted in its Report on Electronic Banking in Nigeria, on the Nature and Types of

---

30 Par. 82(supra)
31 ibid.
32 See PSD, (n 40), Article 5; Article 4A UCC; Sections 103(a)1, 104(a)(2), ETF (n 27), Section 903(7).
33 Article 64-78 ibid; Article 4A UCC, Section 104.
34 See PSD, (n 40), Article 74(1); Article 4a UCC, Section 405(a).
35 See PSD, (n 40), Article 66; Article 4A UCC, Section 211.
36 See PSD, (n 40), Article 74; Article 4a UCC, Section 205 (b).

Risks Associated With Electronic Banking[37] that there were legal risks associated with electronic banking. The Report stated thus:

> Legal risk result from violation of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established in the course of delivery of banking services and products via electronic channels.[38]

Despite the phenomenal increase in e-banking activities in Nigeria today, it is unfortunate that this trend has not been matched with commensurate development in the legal framework for the practice of e-banking. In Nigeria, reliance is being placed on existing legislations, regulations, rules and codes of professional ethics evolved in relation to paper-based transactions to deal with electronic banking issues.[39] Not very much has been done to address the legal challenges associated with electronic banking.

Banking and other Financial Institutions Act

The Act was enacted in 1991 but it has undergone several amendments since then.[40] However, these amendments have not regulated electronic banking and this is understandable as the Act was originally enacted for the regulation of banking and other financial institutions and other matters connected therewith[41]. Its sixty-seven sections do not even cover the full scope of banking business.

Fraud

Fraud is a serious challenge to electronic banking. Nearly every system employed in electronic banking has been bedeviled by fraudulent activities. The end the fraudsters seek are not far from-obtaining things capable of being stolen or inducing any other person to deliver to any

[37] Par. 2.2
[38] Par. 2.2.5
[39] Par. 5.1 page 34.
[40] The Act was amended in 1997, 1998, 1999 and 2002.
[41] See the Long title of the Banking and Other Financial Institutions Act.

person anything capable of being stolen.[42] Armed robbery was, and still is,[43] a serious threat to money stored by banks in their vaults. Aside banks, customers have also been victims of armed robbery attacks especially when these armed robbers had gotten wind that their victims had cash on them. The Nigerian economy has not gone totally cashless (and this is not the purport of the CBN's Cashless Policy[44]) but it is the future of the Nigerian economy.

Criminally minded individuals have gone after Automated Teller Machines (ATM), Bank mobile payment applications, online accounts of bank customers; etc and have hacked these systems. The email accounts of Nigerians are often inundated with emails requesting them to update their bank account details by sending certain confidential information to certain email accounts that are coined to look like the official email accounts of banks[45] and the result is that when a customer sends such confidential account detail to these accounts, the fraudsters can now easily access the accounts and transfer money from the accounts to their own accounts or accounts of their syndicates. It is also very possible for a worker at a financial services company to compromise a customer's account from the confidential information of the customer's details, which the worker is privy to.[46]

Indeed, as much as the signature of a customer will have to be proper on a cheque alleged to have been drawn by such a customer, in electronic banking, digital/electronic signatures are employed. They often take the form of PINs or passwords which only the customer handling an account is expected to be privy to. However, in terms of the usage of ATMs, it would be thought that even if a customer's PIN or password were compromised, the customer's account cannot be accessed via an ATM because the fraudster does not have the ATM card of the customer. However, this is not always so as these cards can also be 'cloned'[47] and the implication is that a fraudster can now have a copy of the bank

---

[42] See section 419 of the Criminal Code Act.

[43] See pg 11 of the cashless economy presentation (now repealed by the Administration of Criminal Justice Act, 2015.

[44] The purpose of the Cash policy of the CBN is to "Reduce (NOT ELIMINATE) the amount of physical cash (coins and notes) circulating in the economy. See slide 13 of the Presentation of the Central Bank of Nigeria, Towards a Cash-less Nigeria: Tools and Strategies, at the NCS 24th National Conference. July 2012.

[45] See HOW TO AVOID ONLINE BANKING FRAUD. Available at www.nairaland.com/1485454/how-avoid-online-banking-fraud. last accessed on 17 October 2015.

[46] See news report of such an occurrence at news2.onlinenigeria.com/headlines/43226-busted-diamond-bank-worker-nabbed-for-defrauding-customers.html. Last accessed on 17 October 2015.

[47] See report at www.scam-detector.com/face-to-face-scams/pin-pad-cloned-debit-cards. Last accessed on 17 October 2015.

customer's ATM card and PIN. Aside electronic banking modes that need electronic cards to operate (such as ATM machines and Point of Sales), several other electronic banking/electronic fund transfer/e-payment means merely require certain details on the electronic card plus the secret PIN of the customer that is possession of such card. The downside of this is that if these details are gleaned from the online platform where these details were entered, (like it has been reported to have happened severally in the West in recent years[48]), the customer's details would have been compromised. And this can often lead to financial loss for the customer.

The Cybercrimes Act 2015 has done a lot to criminalize several unlawful acts in relation to accessing computer systems to defraud. The Act criminalizes:

i. Unlawful access to computer systems/networks for fraudulent purposes[49];

ii. Willful misdirection of electronic messages[50];

iii. Unlawful interceptions of computer data, content, traffic data etc[51];

iv. Computer related forgery[52];

v. computer related fraud[53];

vi. theft of electronic devices[54];

v. Unauthorized modification of computer systems, network data and system interference[55];

vi. Fraudulent issuance of e-instructions[56]

vii. Identity theft and impersonation[57];

[48] In 2012, bank account information from 79 banks in the United States and the United Kingdom was hacked and posted on the internet, exposing financial information for 1,700 accounts. More recently, account information for up to 76 million customers of a financial services giant was stolen by Russian hackers in what was thought to be a coordinated attack on a number of banks. Statistics obtained from about.bgov.com/2015/02/corporate-hacking-and-the-financial-services-industry/ last accessed on 17 October 2015.

[49] Section 6(1) of the Cybercrimes Act.

[50] See section 11 of the Cybercrimes Act.

[51] See section 12 of the Cybercrimes Act.

[52] See section 13 of the Cybercrimes Act.

[53] See section 14 of the Cybercrimes Act.

[54] See section 15 of the Cybercrimes Act.

[55] See section 16 of the Cybercrimes Act.

[56] See section 20 of the Cybercrimes Act.

[57] See section 22 of the Cybercrimes Act.

viii. Cyber stalking[58];

ix. Cybersquatting[59];

x. Attempt, conspiracy, aiding and abetting[60];

xi. Manipulation of ATM/POS terminals[61];

xii. Electronic cards related fraud[62];

xiii. Dealing in card of another[63];

xiv. Purchase or sale of card of another[64];

xv. Use of fraudulent device or attached emails or websites[65]

There are several other acts penalized by the Act but those listed above have been highlighted because they relate to the interference of electronic banking for fraudulent activities.

Forgeries and Unauthorized Withdrawals

The relationship between a bank and its customer is contractual.[66] The bank undertakes to receive money and collect bills for its customer and the proceeds so received are not to be held in trust for the customer, but the bank borrows the proceeds and undertakes to repay them on demand by the customer.[67] This demand by the customer, under paper based system of banking will either be by the customer executing a withdrawal slip or drawing up a cheque. These will have to be signed by the customer. Bank tellers will often refuse to honour a cheque or withdrawal slip if the signature is irregular. Irregular, being that it is different from the signature the bank has in its records of the customer to which the money to be debited is registered.

[58] See section 24 of the Cybercrimes Act.
[59] See section 25 of the Cybercrimes Act.
[60] See section 27 of the Cybercrimes Act.
[61] See section 30 of the Cybercrimes Act.
[62] See section 33 of the Cybercrimes Act.
[63] See section 34 of the Cybercrimes Act.
[64] See section 35 of the Cybercrimes Act.
[65] See section 36 of the Cybercrimes Act.
[66] See Union Bank of Nigeria Plc v Ajabule (2011) 18 NWLR (Pt 1278) 152. Also see Afribank Nigeria Pl v Amuibunwa (2012) 4 NWLR (Pt 1291) 560.
[67] See Mai v Standard Trust Bank Ltd (2008) All FWLR (Pt. 399) 552.

Under the paper based system of banking, it is possible for bank notes to be forged. Sections 463-489 of the Criminal Code Act criminalize forgery and forgery-related offences but what is contemplated by these provisions is forgery of physical documents.

Thus, when money is withdrawn from a customer's account, without the demand coming from the customer or from a person having the customer's instruction, such instruction is said to be unauthorized.

Section 205.2(m) of Regulation E[68] defines an unauthorized electronic funds transfer as one initiated by a person other than the customer without actual authority to initiate the transfer and from which the customer receives no benefit. It would appear however that the burden which is on banks to account for customer's money fraudulently withdrawn from their possession has not shifted under electronic banking. The case of *UBA Plc v Yahuza*[69] is instructive. In this case, the Respondent was a customer of the Appellant in its Katsina Branch with a savings account. His case was that on the 13th, 14th, 15th, 16th, 17th, 18th an 19th of November 2008, the sums of N380,400.00, N340,200, N180,900.00, N201,000.00, N201,000.00, N200,000.00 and N85,500.00 respectively were illegally withdrawn from his said account. It was his case that he discovered these facts when he went to withdraw monies from his account and was informed by the staff of the Appellant that he had no funds in his account and that he sought for an explanation from the staff of the Appellant for the lack of funds and that when no reasonable explanation was forthcoming, he demanded for his financial statement of account wherein he noticed the illegal withdrawals. It was his case that his several demands made on the Appellant, both written and oral, to rectify the illegal withdrawals were not acceded to by Appellant.[70]

The appellant denied the entire case of the Respondent and its case in defence was that the alleged sums were withdrawn using the ATM card of Respondent of Respondent and that the ATM card was in possession of the Respondent and the secret pin number was known only to the Respondent and the Respondent did not report the loss of the ATM card and as such the monies were either withdrawn by the Respondent himself or by someone the vespondent authorized or permitted to have access to the ATM card and pin number. It was its case that the account of the

[68] 12 C.F.R pt 205 (1996); Regulation E is part of the Electronic Funds Transfer Act.
[69] (2014) LPELR-23976 (CA).
[70] Par. E, pg 10; par. A-C, pg. 11.

Respondent was on-line and that it was the exclusive prerogative of the Respondent of where and when to use or withdraw money from the account with the ATM card without any notice to, consultation with or approval from the Appellant and that the ATM machines are automated and programmed to pay money to anyone with the correct ATM card and pin number without its direct involvement and none of its staff or officer had knowledge of the Respondent's pin number.

It was its case that the respondent was unable to make further withdrawals from the account because there was not enough credit in the account and that if the alleged withdrawals were by an authorized person, the Respondent must have willfully or carelessly or negligently exposed his ATM card and pin number to that person and that such person was not a member of its staff, officer of anyone under its control. It was its case that it shall raise the defence of "act of stranger" and that it took all necessary and proper steps to secure the funds of the Respondent and is thus not liable for the loss arising from the alleged withdrawals.[71]

The trial Court held in the favour of the Respondent. The judgment was affirmed on appeal and the Appellant was asked to refund to the Respondent the sum of N1,090,211.00 (one hundred million and Ninety Thousand, Two Hundred and Eleven Naira) being the sum proved by the Respondent to have been illegally withdrawn from his account with the Appellant. Interest was also awarded.[72] The Appeal Court in its judgment, relying on the case of *Wema Bank Plc v Osilaru* (2008) 10 NWLR (Pt 1094) 150, stated thus:

It is trite law that customer's monies in the hands of the banker are not in the custody or under the control of the customer and such monies remain the property in the custody and control of the banker, and payable to the customer when a demand is made. Thus, if anything happens to the money thereafter e.g. theft of money or unauthorized withdrawals, it is the banker and not the customer that bears the loss.

The import of the above position is that where a customer alleges that money has been withdrawn from his account, with or, without his authorization, the bank will be liable to refund the sum alleged, unless the bank can prove that the money withdrawn was with the authorization of

[71] Par. C-G, pg. 11, par. A-C pg 12.
[72] Par. G, pg., 34-par. C, pg. 35.

the customer who makes the allegation, or that the customer had been negligent with his ATM card or PIN. The CBN Guidelines on E-banking recognized this challenge. It is stated in Par. 3.0c that Banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc because of hacking/other technological failures. Banks should therefore, institute risk control measures to manage such risks.

This obligation has now been imposed on financial institutions by the Cybercrimes Act. Section 37 of the Act provides thus:

(1) A financial institution shall-

(a) Verify the identity of its customers carrying out Electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before issuance of ATM cards, credit cards, Debit cards and other related electronic devices;

(b) Apply the principle of know your customer in documentation of customers preceding execution of customers electronic transfer, payment, debit and issuance orders;

(2) Any official or organization who fails to obtain proper identity of customers before executing customer electronic instructions in whatever way, commits an offence and shall be liable on conviction to a fine of N5,000,000.00

(3) Any financial institution that makes an unauthorized debit on a customer's account shall upon written notification by the customer, provide clear legal authorization for such debit to the customer or reverse such debit within 72 hours, shall be guilty of an offence and liable on conviction to restitution of the debit and a fine of N5,000,000.00.

Thus, financial institutions now have an obligation to verify the identity of customers before executing electronic instructions that come from them. This provision re-enforces the position as stated by the court in the Wema Bank's case that a Bank is liable for customer's monies in their possession. banks now have an added responsibility to verify customer's identity before acting on electronic instructions. Is is left to be seen how this provision will be interpreted by the Court. The determination of the Courts is likely to come down to the circumstances of each case.

It is submitted that the Act does not properly balance risk of unauthorized withdrawals between financial institutions and users as the rules of liabilities are not clearly spelt out.

Electronic Signature

The issues of fraud and unauthorized withdrawals in electronic banking naturally lead to the legal challenge of electronic signatures. Electronic signature has been defined as *any electronic means that indicates that a person adopts the contents of an electronic message, or more broadly that the person who claims to have written a message is the one that wrote it (and that the message received is the one that was sent by this person)*.[73]

Courts in various jurisdictions have decided that enforceable electronic signatures can include agreements made by email, entering a personal identification number (PIN) into a bank ATM, signing a credit or debit slip with a digital pen pad device at a point of sale, installing software with a clickwrap software license agreement on the package, and signing electronic documents online.[74]
It has been held that an unsigned document is a worthless piece of paper that has no evidential value.[75]
In the light of this, it is unsurprising that signatures play a great role in banking transactions.
In paper based transactions involving cheques, persons who alter or forge a document may be charged for forgery. However in electronic banking there are no papers or written signatures that can fit into the definition of documents or writing under sections 463 or 464, of the Criminal Code especially as computer information does not exist in writing, and the customer's PIN is not a written document.[76]
At present, Electronic signature is well provided for under Nigerian law. Section 93(2) of the Evidence Act 2011 allows for electronic signature

[73] See 'Electronic Signature' at https://en.m.wikipedia.org/wiki/Electronic_signature. Last accessed 17 October 2015.
[74] ibid.
[75] See Aouizu v Nzenbe (19890 4 NWLR part 118 pg 755
[76] The Technical committee on Electronic Banking noted the challenge of electronic signatures in relation to criminal liability.

where a rule of evidence requires electronic signature or provides for certain consequences if a document is not signed.[77]

Section 17(1)a of the Cybercrimes Act makes electronic signature in respect of purchase of goods, and any other transactions binding.

Section 17(1)b provides that *whenever the geniuses or otherwise of such signature is in question, the burden of proof, that the signature does not belong to the purported originator of such electronic signature shall be on the contender*.

The Act also penalizes the forgery of signatures through electronic devices, thus covering the loophole exposed by the CBN's Technical Committee.[78]

However, the Act excludes certain transactions from the categories of contractual transactions or declarations that are valid by virtue of electronic signature.[79]

It is submitted that section 17(1) b of the Cybercrimes Act improperly places a burden on the contender (most likely the customer whose signature was forged) to show that the signature does not belong to him. This is because the issue at stake in forgery is not whether the signature belonged to the contender but whether the sign, taken as the signature, was made by the contender in the material transaction. For example, if a PIN is taken as the customer's signature, such pin can be fraudulently obtained through phishing and then used in a transaction, as if the Fraudster were actually the owner of the PIN. The issue here is not whether the PIN belonged to the owner but whether it was used by him, or with his authorization, in the said transaction.

Money Laundering and Terrorism Financing

One of the traits of electronic banking is that it can easily promote anonymity during the course of transactions; especially when such transaction is international-involving the transfer of money from an account with a financial institution outside Nigeria to an account in Nigeria, and vice versa. This can easily be exploited for the laundering of money or the sponsoring of terrorist activities. Section 11 of the Money Laundering Act 2011 prohibits the opening or maintaining of numbered or anonymous accounts by any person. However, the recent spate of electronic banking use in Nigeria has made it possible for bank accounts

[77] Furthermore, section 93(3) of the Evidence Act provides: An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

[78] See section 17(1)c of the Cybercrimes Act.

[79] See section 17(2) of the Cybercrimes Act.

to be open and run with less scrutiny than a 'normal' bank account will undergo.[80]. This, it is submitted, defeats the purport of section 11 of the Money Laundering Act.

The ease at which payments can be made electronically, and the volume of such payment that can be made also leaves e-banking susceptible to exploitation by elements that want to launder money or finance terrorist activities. This is especially so as it is left to be wondered, the ease at which financial houses can identify and report suspicious transfers of money, as is required by section 10 of the Money Laundering Act 2011 and section 14 of the Terrorism (Prevention) Act 2011.

Consumer Protection

The Consumer Protection Council Act makes no provision in respect of electronic transactions. The Act defines a Customer to mean *an individual who purchases, uses, maintains or disposes of product or services*[81]. Individual making use of electronic banking services are exposed to many risks that customers have to be protected from. Indeed many Nigerians employing the use of the internet, ATMs, PoS, Mobile payment modes etc are not literate and even many that are literate are not aware of hazards that follow electronic banking. Meanwhile, Nigerian banks are urging customers to obtain and withdraw money with ATM cards, carry out transactions over mobile banking applications or through the bank's website where an account would be opened for them, etc.

There is also not much information available as to the level of privacy enjoyed in terms of personal information that customers give to banks through electronic platforms. The right to privacy is constitutional.[82]

There is also need for rules to be laid down in terms of liability for negligence; especially where a customer is defrauded due to his own negligence or, in a situation where a bank is negligent in protecting customers' information. Risks have to be properly apportioned.

Conclusion and Recommendations

Electronic banking has come to stay in Nigeria. There are more legal issues relating to electronic banking than those addressed in this work. To deal with these challenges, electronic banking in Nigeria must be rooted in a clear legal basis and therefore, there is need for a specific

---

[80] For example, an instant account can be opened with GTBank, online. The user is prompted to fill an online form and immediately receive the account number. See https://socialbanking.gtbank.com/account, Last accessed on the 16 of October 2015.

[81] See section 32 of the Consumer Protection council Act.

[82] See section 37 of the Constitution of The Federal Republic of Nigeria 1000 (as amended).

legislation that deals with electronic banking. Such legislation will have to properly deal with e-payment transactions solely, and cover both domestic and international transactions.

The enactment will also take care of the issue of where risks should lie between the financial house providing the electronic banking service and the customer using such service.

Provisions also have to be made to take care of the apparent gaps in other legislations like the Consumer Protection Council Act and the Money Laundering Act. The Cybercrimes Act should also be amended to cover the loop hole it opened in respect of electronic signature.