# JURISDICTIONAL CHALLENGES IN ELECTRONIC BANKING FRAUD (ATM, MOBILE BANKING & INTERNET BANKING): WHO IS RESPONSIBLE UNDER INTERNATIONAL LAW?[*]

**Abstract**

*Jurisdiction is a geographical area within which political or judicial authority may be exercised. E-banking or Internet means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking functions. However, the emerging trend in Internet banking in Nigeria is of global concern. For one thing, the Nigerian economy is a strong force in Africa. The country also has a high reputation for Internet-related frauds in the world, having been regarded as the headquarters of Advance Fee Fraud (419). It is also defined for the purpose of this paper as banking activities accessed by using a computer employing modems and telephones. Challenges occur in determining or deciding who and where with this judicial authority may be exercised when fraud is perpetrated; while using internet banking. This may lead to certain questions: which country's court has jurisdiction? Who will be responsible when withdrawals are made in a customer's account via ATM? This paper is aimed at evaluating regulatory and constitutional framework to ensure successful practice of internet banking in Nigeria, Tanzania and India, pointing out jurisdictional challenges and determining who is responsible for e-banking fraud under international law. We made recommendations for technological improvement and innovative e-banking law reform.*

**Keywords**: Jurisdictional challenges, electronic banking, internet, responsible and international law

## 1. Introduction

Monetary policy of any country is directly related to economic development of the country where banks play major role. Information technology and communication networking systems have revolutionalized the working of banks and financial institutions all over the world. Banking has become more complex with the introduction of electronic banking. The convenience of e-banking has attracted the public at large all over the world. Banking services has reached rural people of India and has its working wing globalized. Thus, is the complicatory story of e-banking; where there are advantages of numerous facilities offered due to digitalization, there is also plenty obligation to be meted out by the banks. Banker has to act like a king and servant at the same time. He has to vigil and also be loyal to his customers. This dual play makes his job tough. E-banking has brought banking 24 hours and 7 days, where there is no need for the customer to visit banks personally. E-banking is a product of last century due to research conducted in the field of banking and financial services.[1] The concept of e-banking has been simultaneously evolving with the development of the World Wide Web programmers working databases came up with the idea of online banking transactions sometime during the 1980s in Europe. They called this home banking. In 1983, the Nottingham building society commonly abbreviated and referred to as the Non Banking Service launched the first internet banking service in United Kingdom. The first online banking service in United States was introduced in 1994. There are advantages and disadvantages of introduction of technology in banking system. The work of the law starts where there are disadvantages to the public in general and individual in particular. There are certain challenges the banking is facing which are due to obligations imposed by law on the one hand and the invention of new technology and its adoption at the other. This necessitates introduction of new guidelines at the RBI.[2]

## 2. Clarification of Terms

E-banking is being used in India for some time now in the form of digital data in computers, credit and debit cards, Automated Teller Machines, Mobile Banking, net banking and internet banking.[3] Internet or e-banking means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking functions. E-banking has been defined in law lexicon as banking activities accessed by using a computer, employing modems and telephones.[4] In e-banking, 'e' stands for electronic and the banking has been defined 'an acceptance of money from the public, for purpose of lending or investment of money, which is withdrawable by

[*] **Livinus I. NWOKIKE**, **OND, HND, PGD, MBA, FNIM. LLB (Hons), BL, LLM, PhD Candidate,** Justice of Peace; Notary Public; Lecturer, Department of International Law and Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra, Nigeria, Email: li.nwokike@unizik.edu.ng, website: www.geci.org.ng.tolerancefocus@gmail.com. Phone Numbers: 08033521034, 09073018015.

[1] S V Nadagouder and M P Chandrika, 'Law Relating to E-Banking in India – An Outreach Challenge', *International Journal of Current Research* Vol 5, Issue II, November, 2013, pp 3308 0 3512, available at http://www.journalcra.com accessed on 14th November, 2019

[2] *Ibid*, p 3508

[3] B R Sharma, *Bank Frauds Prevention & Detection*, (3rd ed. Universal Law Publishing Co, 2009) p 281

[4] P AiyarRamnath, *Advanced Law Lexicon*, (4th ed., Nagpur; Wadhwa and Co, 2013) p 1561

cheque, draft or otherwise[5] and banking by using electronic devices is e-banking. Hackers who enter systems and donating more than look around, or even copy files, do not profit from their crimes generally do not do anything harmful or malicious, and do not cause any loss to the companies, organizations or businesses that they intrude upon. Most often what hackers are accused of land prosecuted for is 'trespassing' and 'possession of unauthorized access devices. That is, they are prosecuted for their presence, virtual though it may be. The judicial system is protecting us not from the actions of hackers, but from the presence, or the possibility of the presence, of hackers.[6] URL is an acronym for universal resource locator. It includes information about the-machine the page is stored on the path name of the file that contains it, along with other technical points. World Wide Web or WWW or W3 is an organised reservoir of information. It is composed of thousands of computers on internet which contain varying degrees of information which can be accessed by internet account holders. The access to this information is mostly free of charge in an unrestricted manner. At times the access is restricted by passwords and sometimes is allowed only on payment basis. Computers which are part of WWW are called websites. The information available on websites is called 'Documents'.[7] WWW is a collection of documents that are linked together in an almost endless manner. The links from a document terminate on other documents which have links with other documents and so on. What is more, the other documents which the links terminate may not be on the same website and may actually resident on other website that may be located several thousands of kilometres away in another country. So, links from website to website, it will create a criss-cross of lines spanning all over the globe that would look something like a spider web-covering the web. Hence, the name is World Wide Web (WWW). A computer is an electronic device designed to accept and store data, process them and produce results under the direction of detailed step-by-step instructions. Further, computer is also an electronic device which takes an input, processes the input and gives the desired output.

**3. Features of e-banking**

The main features of e-banking are:

1. In e-banking, banking functions are carried by using internet facility.
2. It removes the traditional geographical barriers as it could reach customers at different counters/jurisdictions.
3. E-banking facilitates banking transactions at all time and on the days including holidays and Sundays.
4. It provides several additional delivery channels which are more convenient and cost effective to both customer and the banker.
5. It is based on science and technology i.e. use of electronic devices which saves time and energy of banker and customer.
6. Its special features lie in ensuring security of the transaction, customer's privacy and transparency of transaction.

**Services through e-banking**

E-banking services are delivered to customers through the internet and web using Hypertext Markup Language (HTML). In order to avail e-banking facility, customer must have internet access and web browser software. Multimedia information in HTML format can be displayed through online web browsers. The heart of the e-banking application is the computer system, which includes web servers, database management systems and web application programmes that can generate dynamic html pages. Bank customers' account and transaction information is stored in a database which is a specialized software that can store and process large amounts of data in high speed. The function of the web server is to interact with online customers and deliver information to users through internet. When web server receives a request such as an account inquiry from an online customer, it requires an external web application programme to process the request. C,Visual basic, VBS script and Java are some of the languages which are used to develop web application programmes to process customer requests interact with the database and generate dynamic responses. Then the web server will forward the response to HTML files to e-banking customers. Several banks also use state of the art imaging systems allowing customers to view images of cheques and invoices over the internet.

**Services of e-banking includes**

1. Information System: General Information's like interest rates branch location, bank products and their features, loan and deposit features are provided in the bank website. There exist facilities for downloading various types of application forms exp. deposit application form, loan application form, etc. The communication is carried through e-mail, otherwise the person seeking information need not disclose his

[5]Section 6 of Banking Regulation Act, 1949

[6] K Mani, *Electronic Banking Frauds: ATM, Mobile, Banking and Internet Banking* (New Delhi: Kamal Publishers, 2018) 15

[7] *Ibid*

identity. Also, there is no possibility of any unauthorized person getting into production systems of the bank through internet.[8]

2. Electronic Information Transfer System: The system provides customer with specific information in the form of account balances, transaction details and statement of accounts. The information is still largely of the 'read only' format. Identification and authentication of the customer is through password. The information is fetched from the bank's application system either in batch mode or off-line. The application systems cannot directly access through the internet.[9]
3. Fully Electronic Transactional System: This system allows bi-dimensional capabilities. Transactions can be submitted by the customer for online update. This system requires high degree of security and control. In this environment, web server and application systems are linked to secure infrastructure. It comprises technology covering computerization, networking and security, interbank payment gateway and legal infrastructure.[10]
4. E-banking services can be availed for payment of bill, fund transfer, credit card, railway and air ticket booking, investment, recharging phones and mobiles and shopping. Generally banks do not charge customers for providing certain services.[11]

**4. Legal Provisions on E-banking in India**

India is a signatory of WTO. The basic principles of WTO are Liberalization, Globalization and Privatization. Therefore, trade and commerce in India has been liberalized. Incidentally, the financial sector has also undergone major changes. With the advent of e-banking, India is facing unprecedented competition from the World at large. If technology is not updated in financial sector, international trade would be a distant dream. The deregulation of the banking industry coupled with the emergence of new technologies has enabled new competitors to enter the financial services market quickly and efficiently. Various provisions of law, which are applicable to traditional banking activity, are also applicable to internet banking. This is does not overcome the problems, and therefore there is need for introduction more stringent rules and laws specifically to meet the problems of e-banking. The legal framework for banking in India is provided by a set of enactments, viz. The Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and Foreign Exchange Management Act, 1999 are few among many such legislations. It is mandatory on the part of all entities to obtain a license from Reserve Bank of India under Banking Regulations Act, 1949 to function as bank. Different types of activities which a bank may undertake and other prudential requirements are provided under this Act. Reserve Bank of India has regulated acceptance of deposit by Non Banking Institutions also. Under the Foreign Exchange Management Act, 1999, Non Residential Indians can lend, open a foreign currency account or borrow from a bank in India including from a Non-Resident bank, except under certain circumstances provided under the law. Besides, banking activities are also influenced by various enactments governing trade and commerce, such as, Indian Contract Act, 1872, the Negotiable Instruments Act, 1881, Indian Evidence Act, 1872, etc.[12]

**5. Obligation of Banks and the Online Banking**

There are certain obligations which the banker is supposed to fulfill. They are

1. Banks have to maintain secrecy of customers account.[13] This obligation dates back to 1924 where in a case popularly known as Tournier case,[14] in which it was held that banker should not disclose customers financial position and the nature and the details of his account to anybody, since it may affect his reputation, credit worthiness and business. Now with the advent of new technology, this obligation has become a difficult task for there are hackers who can operate other account. Bankers are not in a position to trace them. They come to know only when the customer informs them of some irregularity in their transaction. Hence, to meet out this obligation, banks have to update their technology to the requirement.
2. Banks are also under obligation (public duty), to produce documents to the court whenever called for.[15] In earlier days this was easy as the documents were either in printed or in written form and readily available with the banks. Banks keep these information's in electronic form as it is easier and cheaper to store and retrieve and also ensures speedier communication / transmission. Information Technology Act, 2000 was drafted to facilitate users of electronic communication similar to other paper based or oral testimony means. Records can be kept in electronic form. Electronic form means information generated,

[8]K C Shekar, 'Banking Theory and Practice', (20th ed., Mumbia: Vikas Publishing House Pvt Ltd, 2007) p 45
[9] Ibid at p 46
[10]http://www.iajet.org/iajet_files./vol.2/no.1/internet%20banking/20adoption%20in%20an%20emerging %20economy%20indian%perspective.pdf retrieved on 5 May, 2011
[11]R S Joga, 'Computer Contracts and Information Technology Law,' (2nd ed. Wadwa& Co., Nagpur, 2005) p 123
[12]M L Tannan, Tannan's, 'Banking Law and Practice in India, (20th ed., India Law House, 2003) p 157)
[13]Section 13 of Banking Companies (Acquisition and Transfer of Undertaking) Act, 1970
[14]*Tournier v. National Provincial & Union Bank of England*, (1924), K.B., 461
[15]Section 4 of Bankers Books Evidence Act, 1891

sent, received or stored in media, magnetic, optical, computer memory, micro film, etc. Now in the eyes of law written records means electronic records which can be produced before the court like it was produced previously.[16] But banks have to reproduce the documents and store them properly. If the software is attacked with virus it washes of all the documents. Hence, banks have to carefully handle the electronic documents or else they will be accountable to the law.

3. Obligation to verify forgery of signatures.[17] Banks have to verify the signature of the customer before paying their cheques. This obligation is on the paying banker. The law is very strict; and in case of forgery the banker is liable. This is limited to traditional banking. Introduction of new technology has helped banker in storage and retrieval of signature of customers. Each signature card is scanned using a scanner that takes images of the signature and converts it into digital form which are then stored in the hard disk. When a cheque (traditional) is received for payment, the signature can be retrieved by the user. What when the funds are transferred electronically? In case of electronic fund transfer, digital signatures are used which are in the form of code. These signatures are in electronic form attached to electronic record. The obligation of the banker to verify the signature is continuing here for digital signature. Hence, the banker should adopt technology which can identify the sender by recognizing message originator, authentication and non reputable that affixes a coded message to the document. It is used to sign the record. Banker has to maintain records of the digital signature and also educate the customer in this regard.
4. The other obligation on the banker is to provide proper service to the customer: Otherwise the bank is answerable. Not providing proper service attracts Consumer Law which amounts to deficiency in providing service. It has been held in *Vimal Chandra Grover v. Bank of India*,[18] that banking is a business transaction of a bank and customers of a bank are consumers within the meaning of Section 2(1)(d)(ii) of the Act. This obligation extends to electronic banking also.

In Nigeria, conventional banking system started in Nigeria in 1952. Since then, the industry has witnessed a lot of regulatory and institutional advances. The industry was being controlled by at most five out of the 89 banks in existence before the commencement of the ongoing banking industry reformation in the country. Multiple branch systems is also one of the notable features of Nigerian banks, with a total of 89 banks accounting for about 3017 bank branches nationwide as at 2004. As well, the industry is faced with heavy challenges, including the overbearing impact of fraud and corruption, erosion in public confidence, a poor capital base, persistent cases of distress and failure, poor asset quality, and so on. Part of the moves to resolve these lingering problems include the banking reform initiated by the Central Bank of Nigeria in June 2004, which is largely targeted at reducing the number of banks in the country and making the emerging banks much stronger and reliable.[19]

In the bid to catch up with global developments and improve the quality of their service delivery, Nigerian banks have no doubt invested much on technology; and have widely adopted electronic and telecommunication networks for delivering a wide range of value added products and services. They have in the last few years transformed from manual to automated systems. Unlike before when ledger-cards were used, today banking has been connected to computer networks, thereby facilitating the practice of inter-bank/inter-branch banking transactions. Developments at home, such as the introduction of mobile telephone in 2001 and improved access to personal computers and internet service facilities have also added to the growth of electronic banking in the country. However, whereas local banks most commonly practice real time online intranet banking, the integration of customers into the process is far from been realized. Many of the reasons are attributed to the high prevalence of internet fraud and lack of an adequate regulatory framework to protect the banks from the volatility of risks associated with Internet banking, especially at the levels of communication and transaction. In the main, Nigeria is globally regarded as the headquarters of Advance Fee Fraud which is perpetrated mostly via the Internet.[20]

**6. The Emerging Issues in Internet Banking in Nigeria**

In its survey on the extent of e-banking adoption by Nigerian banks, the Central Bank of Nigeria, in September 2002, found out that of the 89 licensed banks in the country, 17 were offering Internet banking, 24 were offering basic telephone banking, 7 had ATM services, while 13 of the banks were offering other forms of e-banking. This implies that as at then, only 19.1 percent of the banks were offering internet banking.

[16]R N Chaudhary, *Banking Laws* (1st ed., Central Law Publications, 2009) p 377
[17]Section 89 of the Negotiable Instrument Act, 1881
[18]A I R 2000 SC 2181
[19] A E Ezeoha, Regulating the internet banking in Nigeria: Problems and Challenges – Part I, *Journal of Internet Banking and Commerce*, Vol. 10, No 3, 2005, available at http://www.arraydev.com/commerce/jibc/ accessed on 14th November, 2019
[20] *Ibid*

At present, the situation does not seem to have shown any significant improvement. Whereas about 90 percent of the banks in the country offer other forms of electronic banking services like telephone banking. ATM and electronic funds transfer, internet banking is yet to take center stage. This aspect of banking is still at the basic informative stage. This is so despite the widely acclaimed benefits of internet banking against the traditional branch banking practice. Part of the reasons identified for the inability of banks in Nigeria to take full advantage of this mode of banking includes lack of adequate operational infrastructure like telecommunication and power, upon which e-banking generally relies. Due to the inability of the banks to integrate their operations into the internet development process, Internet banking can be said to have less impact in the existing banking structure in the country. Earlier articulated reasons why internet banking was having a moderate economic impact in the country include: that Nigerian bank customers are not on the average trained on for teller jobs and the workings of internet banking, a situation which makes transaction processing via internet banking prone to error; the absence of a clearly defined legal framework for internet banking, leaving banks with inadequate legal cover to provide the services; and poor telecommunication infrastructure all over the country. In addition, the fact that internet usage in the country has been abused by cyber-criminals makes its window unattractive for domestic banking operations and legitimate international operations. The inherent fear associated with patronizing internet banking services in Nigeria is again re-enforced by the growing evidences that the world over, dubious Nigerians use fake bank website to scoop funds from unsuspecting victims. In some cases, these crimes are committed using existing bank sites.

**7. Threats of Cyber-Crimes on the Nigerian Banking Premises**

The Advance Fee Scheme or 419, which is one of the most popular of all internet frauds, has its origin from Nigeria in the 1980s. Its development and spread follows the path of the developments in information technology. At inception, postal letters were used as key media for committing 419 frauds. Later in the early 1990s, it became integrated into telecommunication facilities such as the telephone and fax. From the late 1990s following the introduction of computers and internet, 419 crimes became prevalently perpetrated through the use of e-mail and other internet means. The latest dimension taken by the perpetrators of this crime is the use of fake internet bank sites, and using that to encourage victims to open accounts with them. The country is currently rated as having one of the highest records of internet frauds in the whole world. According to the National Consumers League,[21] the country is the third highest ranked in Internet 'money offer' frauds. As was reported in one of the national newspapers, frauds and forgeries in Nigerian banks as at June 2005 stood at 329 or N1.15 billion monetary equivalents, against 222 cases or N1.47 billion monetary equivalents in April this same year. There is even global suspicion that a Nigerian crime syndicate that coordinates global crimes such as money laundering, bank fraud and 419 scams exists today. These issues basically defeat the key ingredients of e-banking, which includes confidentiality, integrity and availability.

Several factors are responsible for the above situation. They include inordinate tolerance for corruption among Nigerian public and government agencies; weakness of the existing legislative/judicial institutions to make and enforce relevant laws on cyber-crimes; deteriorating quality of graduates in terms of professional values and ethics; chronic unemployment among graduates, and the widening gap between the few rich and the many poor caused mainly by bad governance. In the main, erosion of good value principles and corruption constitute the greatest cause of rising cyber-crimes among Nigerians. This, according to Transparency International, is worsened by fact that several generations of Nigerians have been raised in this norm. Hence, what is seen as a dangerous global crime, is socially acclaimed and glamorized in Nigeria. The above situation constitutes the environment upon which internet banking has emerged in Nigeria. Although the level of the adoption and practice of internet banking has remained quite insignificant, global projections still remain that the internet would continue to play a revolutionary role in the development and delivery of banking products and services all over the world. In effect, it is this projection that has raised pertinent regulatory questions concerning internet banking, especially in internet fraud-infested countries like Nigeria. One key issue here borders on how to handle the rising level of frauds and forgery prevalent in the entire banking system; and how to make internet banking fit well in the banking structure of a country so notoriously identifiable with criminal use of internet access.

**8. The Regulatory Challenges**

At the national level, the Nigerian government and the relevant regulatory agencies have strived to match the rapidly changing electronic banking environment with necessary regulations and institutional frameworks. Earlier efforts made to this effect included the enactment of the Failed Banks (Recovery of Debts) and Malpractice in Banks Decree No. 18 of 1994, and the Money Laundering Decree of 1995. However, as noted above, poor enforcement procedure rendered these instruments very inactive in checking the menace of financial crimes. By the late 1990s, following record growth in internet and computer usage in the country, almost all the regulations

[21] National Consumers League (2002), Internet Fraud Statistics, www.ncinet.org/shoppingonline

guiding the banking industry, including the Banks and Other Institutions Act of 1991, were lacking adequate provisions to accommodate the emerging trend. Not even a mention of electronic banking or any manner of its application was mentioned in any of those prevailing regulatory documents. The situation created a lot of gaps between the levels of CBN regulatory tools and the advances in information technology. This at the same time made the banks vulnerable to all kinds of risks, including transaction, strategic, reputation and foreign exchange risks. This deficiency notwithstanding, it was not until 2003 when the maiden guidelines on electronic banking came into force. The electronic banking guidelines emerged from the findings of a Technical Committee on Electronic Banking set up by the Central Bank of Nigeria in 2003 to find appropriate modalities for the operation of electronic banking in the country. It was indeed the findings and recommendations of the committee that led to the adoption of a set of guidelines on Electronic Banking in August 2003. Of the key provisions of the Guidelines, only a section deals with issues relating to Internet Banking. Section 1.3 paragraph 4 of the guidelines, exceptionally stresses that banks should put in place procedures for maintaining the bank's Website, including the various security features needed for internet banking services.

Despite its numerous technical specifications, the Guidelines have been widely criticized as not being enough to check the growing popularity of Internet banking against the backdrop of growing sophistication in technology related crimes and frauds. Closer examination of the contents of the Guidelines equally shows that the document fails to meet up with the four key areas where internet banking may have regulatory impact – changing the traditional lines upon which existing regulatory structures are laid; handling concerns about existing public policy issues; changing the nature and scope of existing risks; and rebalancing regulatory rules and industry discretion. Again, some important recommendations of the Technical Committee that gave rise to the adoption of the guidelines were completely omitted. This is especially so with paragraph 6.1 of the Committee's report, which among other recommended that all banks intending to offer transactional services on the internet/other e-banking products should obtain an approval-in-principle from CBN prior to commencing these services. Part of the criticisms is that the recent guidelines that are capable of constraining the practice and development of internet banking Nigeria. One of such areas, for instance, is the requirement on electronic banking product development. While acknowledging that the existing regulations would apply wholly on electronic banking, section 4.2 of the Guidelines emphasizes that only banks, which are licensed, supervised and with physical presence in Nigeria, are permitted to offer electronic banking services in Nigeria, and that virtual banks are not to be allowed. The Guidelines also gives indications that the products/services can only be offered to residents of Nigeria with a verifiable address within the geographic boundary of Nigeria; any person residing physically in Nigeria as a citizen, under a resident permit or other legal residency designation under the Nigerian Immigration Act; any person known herein as a 'classified person' who neither is temporarily in Nigeria. The Guidelines go further to indicate that the e-banking service should be offered in Naira only; and that where such a service is to be provided in foreign currency, it should be to only the holders of ordinary domiciliary accounts, and conform with all other foreign exchange regulations. On some other aspects, the Guidelines have also been criticized for not addressing adequately the critical issues concerning internet security. It failed to explicitly recommend a standard that allows banks to examine potential threats that may already be in existence in each individual financial institution's current network.

In addition to this array of criticisms, the workability of proper internet framework is also queried amidst the poor state of basic information technological infrastructure in the country. This is essentially necessary since e-banking generally relies on the existence of adequate operational infrastructure like telecommunications and power to function effective. Though little success has been recorded, the supply of these requisite facilities is very erratic in the Nigerian case. Where they exist, high cost of acquisition and maintenance tend to deny a greater percentage of the population access to them. The case of internet access is a glaring one – where majority of the citizens rely solely on the services of commercial cyber cafés to meet their internet needs. It is expected of the e-banking guidelines to provide procedures not only for banks' investment in internet facilities, but also in promoting customers' access to such. Unfortunately, none of such is contained in the document.

**9. Emergence of Electronic Banking in Tanzania**

The banking activities in Tanzania could be traced back to the 1900s[22]. Modern banking practices were ushered in by the colonialists who, for the purpose of facilitating their economies in Tanzania and East Africa at large, introduced banks.[23] The earliest banks were a product of the Germany regime in Tanganyika. A great deal of banking regulations, however, emerged under the British regime from 1919 in Tanganyika when it took over the colonial mandate from Germany and Tanganyika became a British Protectorate. Apart from introducing more

[22] Binamungu and Ngwilimi, 2006

[23] C I Kato, Legal Framework Challenges to E-Banking in Tanzania available at http://www.grin.com/document /47996 accessed on 14th November, 2019

banks than ones left by the Germans, the British enacted a number of laws to regulate banking activities in Tanganyika. After independence, these banks carried on the colonial banking legacies till the 1967 Arusha Declaration led to the nationalization of all the private banks.[24] In the early 1990s, a report on the Inquiry into Monetary and Banking Systems in Tanzania paved the way to the enactment of the Banking and Financial Institution Act, 1991. Despite its remarkable contribution, the Act did not point out anything on electronic banking because the information and communication technology (ICT) had not been embraced by most of the financial institutions in the country at that time though its impacts had already been felt by developed countries such as the USA and the UK.[25] In Tanzania, electronic banking (or e-banking) has remained largely in its infancy despite an overwhelming response in its applicability and reception. Apart from the banks, other financial institutions have also adopted new methods of electronic financial transactions. The adoption of the Automated Teller Machines (ATMs) by various banks and financial institutions and mobile banking by various communication companies such as Tigo, Vodacom and Airtel have encouraged the adoption of habits for deposits and quick transfers of money or payments via electronic payment services. The adoption of electronic banking by CRDB, NMB, DCB, Exim Bank and NBC, for example, confirms the development of electronic banking in the country. According to the bank of Tazania (BoT)[26] to some extent, there are significant developments in country's electronic banking. The report shows that many banks use electronic banking delivery channels. These channels include ATMs, internet banking and electronic fund transfer at point-of-sale and mobile banking. However, the cyber environment comprising people, technology and applications creates a sophisticated environment for cyber threats to thrive in electronic banking. The environment consists of a learning information society (internal and external) with knowledge, skills and technologies and opportunities for cyber threats in electronic banking in Tanzania. As such, Tanzania cannot ignore this situation as it needs to act fast by taking necessary and sustainable steps to address and contain the situation before it got out of hand. This study assessed the existing policy, legal and institutional framework of ICT in electronic banking to establish whether they are sufficient and effective enough to prevent and contain cybercrime in Tanzania.

**10. Challenges to the application of e-banking in Tanzania**

Like other countries, the emerging ICT technology is fostering electronic banking in the country in terms of electronic banking delivery channels such as ATMs, internet banking and electronic fund transfer at point of sale. Electronic banking delivery channels have made the transfer of money more efficient and effective than traditional un-automated banking as customers can now conveniently access their respective accounts at any place and at any time without standing in long files. Clients can access different services without visiting bank premises and thus be subjected to long queues as in the pre-automation banking era. On the other hand, these innovations in banking have exposed one important challenge regarding how the existing policies, legal and institutional framework can address the emerging challenges of electronic banking largely unseen in the established pieces of legislation. In its report, the BoT acknowledges that the existing policies and laws guiding the banking sector are outdated and, hence, largely ineffective in dealing with the emerging problems as a result of ICT development. These problems include rising cases of cybercrimes in e-banking such as fraud and unauthorized transactions and lack of physical infrastructure to support development such as unreliable power supply and telecommunication.[27] Indeed, these problems can be solved by having in place a comprehensive policy and law coupled with a good institutional framework for their implementation. According to the Law Reform Commission of Tanzania,[28] the country has no comprehensive policy and law regulating e-banking. The existing policies and laws leave some lacunas in aspects of e-banking because they do not adequately cover computer misuse, e-banking channels such as internet banking and mobile banking. In fact, the current policies and laws are silent on the allocation of loss in case of e-banking fraud. The Tanzania National Electronic Banking Guidelines of 2007, for example, lack legal enforceability. Even the recently enacted laws, the Cybercrimes Act, 2015, and the Electronic Transaction Act, 2015 do not address in detail issues of e-banking. Similarly, the National Payment System, 2015 has failed to address many pertinent issues, such as e-cheque and customer protection. In general, the prevailing policies, legislation and institutional framework of ICT in e-banking do not protect adequately the banks and customers involved in these e-banking transactions and services.

**National Information Communication Technology Policy**

This policy came into force in 2016 with the main objective of accelerating socio-economic development with the potential of transforming Tanzania into an ICT-driven middle-income economy and society. The policy acknowledges that there is a pressing need for a comprehensive, technologically neutral and dynamic policy, legal and regulatory framework to address issues of privacy, ICT legislation and cybercrimes. In 2005, Tanzania

[24] *Op.cit*
[25] *Ibid*
[26]The Country's Central Bank – Report (2016)
[27] See BoT Report, 2011
[28] 2005

enacted Tanzania National Payment System Vision and Strategies. One of the main aims of this policy is to establish legal and regulatory framework to guide the payment system in Tanzania. Since 2005, no sufficient efforts have been made to achieve this goal. In fact, it has taken ten years for the country to enact the Cybercrime Act, 2015, the National Payment System Act, 2015, and the Electronic Transaction Act, 2015. And yet, some of the enacted legislations do not detail issues concerning e-banking. As a result, many of electronic banks challenges remain largely unaddressed by the existing laws. If a certain technology is necessary and is available in other areas, then it is possible to outsource such a service. Thus, the Outsourcing Guidelines for Banks and Financial Institutions, 2008 were developed to guide outsourcing in Tanzania's banking industry. The main laws governing the banking industry in Tanzania are the Bank of Tanzania Act, 2006 and the Banking and Financial Institutions Act, 2006. Under the Bank of Tanzania (BoT) Act, 2006, the Minister responsible can make necessary or desirable regulations to facilitate the smooth running of the banking business. The Bank and Financial Institution Act, 2006, among others things, has been enacted to provide a supervision mechanism for banks and financial institutions. The Act also empowers the Minister to make necessary or desirable regulation. In 2015, Tanzania enacted the Cybercrimes Act,[29] which prescribes cybercrimes and their attendant punishments. These crimes include those committed via the computer system and information technology such as illegal access, illegal remaining, illegal interception, illegal data interference, data espionage, illegal system interference, illegal devices, computer-related forgery, computer-related fraud, identity related crime and conspiracy to commit offence.

**11. Fraudulent Use of Access Devices[30]**

This section deals with the fraudulent use of access devices. A credit card would fall under the definition of an access device. An access device has been defined as follows; any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, specifics or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument). Fraudulent use of, trafficking in counterfeit, unauthorized access devices, producing or possessing, with intent to defraud device-making equipment are punishable. It is an offence under this section to: (i) knowingly and with intention to defraud produce, use, or traffic in one or more counterfeit access devices; (ii) knowingly and with intent to defraud traffic in or use one or more unauthorized access devices during any one-year period, and by such conduct obtain anything of value aggregating $ 1,000 or more during that period of; (iii) knowingly and with intent to defraud possess fifteen or more devices which are counterfeit or unauthorized access devices; (iv) knowingly, and with intent to defraud, produce, traffic in, have controller custody of, or possess device-making equipment; (v) knowingly and with intent to defraud effect transactions, with one or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000; (vi) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicit a person for the purpose of offering an access device or selling information regarding or an application to obtain an access device; (vii) knowingly and with intent to defraud use, produce, traffic in, have control or custody of, prepossess a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; (viii) knowingly and with intent to defraud use, produce, traffic in, have control or custody of, or possess hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain, telecommunications service without authorization; or (ix) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud cause or arrange for another person to present to the member or its agent, for payment, one or more evidences or records of transactions made by an access device. The offence shall, if it affects interstate or foreign commerce, be punished as provided.[31]

**12. Conclusion**

The importance of electronic Banking to international business and commerce cannot be overemphasized. Information technology being an innovative discovery has made international business transactions easier, as one can stay in the comfort of his home at a town like Umuomaku in Nigeria and transact business with his customer in the far away Texas in United States of America. It is axiomatic to say that the world is now a global village. However, the perfect use of e-banking, otherwise called internet banking is not without changes. In developing countries like India, Nigeria and Tanzania, these challenges and paramount as these technologies for e-banking are now to them when compared with developed economy like United States of America. The Laws and regulatory framework for their operations are also new and not as developed as in the USA. Having pointed out areas of

[29] 2015

[30] Section 1209 of Title 18 US Code

[31] US Code. Title 15, Section 1644 (c) which provides for penalties for the fraudulent use of credit cards

strengths and weaknesses in these laws and regulatory framework, the government of India, Nigeria and Tanzania should reform their laws to match with the sophistication and implication occasioned by use of technologies for e-banking in line with international law, standards, constitutionalism and globalization.