ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

Electronic Banking and Technological Development in Tanzania: A Legal Analysis

Rosemary Mukama*

Abstract

This paper reviews banking laws in Tanzania in relation to electronic banking and technological development. It is more than a decade now, since Tanzania engaged in the use of electronic banking. Since electronic banking has higher risks and much used by banks, communication companies and their customers, it is just reasonable to have the law adequately address and protects the electronic banking transactions. Unfortunately, banking laws currently in force are inadequately provide for electronic banking. For example the Bank of Tanzania Act (BoT Act) gives power to the Bank of Tanzania to: establish payment clearing and settlement system; and; make rules and regulations to govern the payment system, but the clearing and settlement system referred designed to save inter-bank transactions and therefore other types of electronic banking are not covered. Furthermore, the rules and regulations bind only participants or members of such payment clearing and settlement system. The BoT Act also gives power to the minister responsible for financial affairs of the United Republic of Tanzania to make regulations so as to give effect to the objectives of the BoT Act. However, regulation on electronic banking has not been made.

In 2000 the BoT issued guidelines on payment card to regulate payment through Automated Teller Machine (ATM) and Point of Sale (POS), but the guidelines have no legal force. This situation definitely create some practical legal issues that need attention. It is in this spirit that the author embark on analysing the Tanzania legal regime on electronic banking. The author employed library research used to acquire primary data by surveying the laws of Tanzania relating to banking and also for obtaining secondary data through reading of books, journals, articles and websites. Furthermore, the author have also employed interview banking personnel to enrich primary data. This study shows that, due to inadequancy of the

* Assistant Lecturer in Law, University of Iringa, P.O BOX 200, Iringa, Tanzania.

law regulating electronic banking, the undertakings emanate some practical issues which calls for an amendment of the Tanzania legal framework or the enactment of specific legislation to not only electronic banking, but also other cyber laws which will facilitate and protect electronic banking and the banking system in general.

Introduction

Electronic banking is an exchange of funds in a paperless form between banks, business entities and customers.[1] It may also be referred to as electronic fund transfer (EFT), e-banking or e-finance.[2] In electronic banking, funds are transferred via electronic means such as telephones, telexes, facsimiles, telegraphic transfer[3] mobile phones and computers.[4] It includes fund transfer through automated teller machines (ATMs), cheque truncation, and point of sale transactions etc.[5] It involves an application of the Information and Communication Technology (ICT) in transferring fund.[6] Generally, electronic banking comprises with four primary channels namely; EFT, electronic data interchange (EDI), electronic benefits transfers (EBTS) and electronic trade confirmation (ETC).[7]

It has been evidenced that electronic banking changes the way of doing business.[8] For example; banking working hours has now changed. The customers can bank twenty four hours a day and seven days a week, a bank customer can deposit or withdrawal cash from his or her account without facing the bank teller and banks. Banks are now sharing customers as

---

[1]A. Mollel and Z. Lukumay, *Electronic Transactions and Law of Evidence in Tanzania*, Peramiho Printing Press, Peramiho 2008[2], 5.

[2]Mollel & Lukumay, *supra*, note 1*;* M. Hapgood QC, *Paget's Law of Banking*, Lexisnexis, Butterworths 2004[12], 285.

[3]Telegraphic transfers mainly used in wholesale payment and it is also involves money orders and GIRO which used in retail payments. However, banks utilize intra-bank communication networks using VSAT leased lines and dial up telecommunication systems to transfer inter branch payments electronically. (Bank of Tanzania, "Payment System in the Southern African Development Community – Tanzania Chapter", 9. Available at "http://www.bot-tz.org" accessed 16 December 2014).

[4] B. A. Bakar, *International Finance: An Arena of Level Playing Field*, Thrust Publications, Dar es Salaam 2009, 4.

[5] Basle Committee on Banking Supervision (BCBS), "Risk Management for Electronic Banking and Electronic Money Activities" 1998, 3.

[6] "http://www.bis.org/publ/bcbs98.htm" (accessed 30 March 2011); Mollel & Lukumay, *supra*, note 1, 3.

[7] T. Glaessner *et al*, "Electronic Security: Risk Mitigation in Financial Transactions – Public Policy Issues" the World Bank Financial Sector Strategy and Policy Department, July 2002, 4. Available at "http://www1.worldbank.org/finance/" (accessed 16 July 2011).

[8] D. Palfreman, *Banking: The Legal Environment*, Pitman, London 1990, 258; A. J. Mambi, *ICT Law Book: A Source Book for Information & Communication Technologies and Cyber Law*, Mkuki na Nyota, Dar es Salaam 2010, 120.

ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

for instance a Barclays bank customer with a visa card may transact through National Bank of Commerce (NBC), CRDB Bank PLC or any other bank's ATM. It is also involves more parties in transaction as compared to traditional banking. For example parties to electronic banking includes bank, customer, electronic system provider, electronic clearing house etc.

However, it should be noted that, "electronic banking does not open up to new risk categories rather it modifies existing risks and create new risk management and prevention challenges".[9] Furthermore, banking sector is very crucial input to the monetary intermediation for the economy of any country and due to the fact that, the banking business at large extent done electronically, the law has a role to play as part of functioning infrastructure.[10] Yet, to date there is no adequate law regulating electronic banking in Tanzania as the banking laws currently in force that are applicable to the traditional banking also extend its application to the electronic banking. These laws are; the Bank of Tanzania Act, Act No. 4 of 2006 and the Banking and Financial Institutions Act, Act No. 5 of 2006. The only place where these legislation making reference to electronic banking, is in expression of the powers and functions of the BoT. The law provides;

> "The Bank shall regulate, monitor, and supervise the payment, clearing and settlement system including all products and services thereof; and conduct oversight functions on the payment, clearing and settlement systems in any bank, financial institution or infrastructure service provider or company. The Bank may participate in any such payment, clearing and settlement systems; establish and operate any system for payment, clearing or settlement purposes; and perform the functions assigned by or under any other written law for the regulation of payment, clearing and settlement systems".[11]

It is in the spirit of this provision, that the Bank of Tanzania has from time to time make circulars, guidelines and directives to regulate electronic banking in Tanzania. It has also made rules and regulations for the same objectives and it has even participated as a host of electronic clearance houses. The two pieces of legislation are complemented by other

---

[9] Central Bank of Netherlands, "Provision and Guidelines for Safe and Sound Electronic Banking", December 2007, 8; Basle Committee on Banking Supervision, "Management and Supervision of Cross-Border E-banking Activities, 2003, 6. Available at "http://www.bis.org/publ/bcbs98.htm" (accessed 17 July 2011).

[10] G. Heinrich, "Operational Risk, Payments, Payment Systems, and Implementation of Basel II in Latin America: Recent Development", 2006, 1; Heinrich is the Chief Representative, BIS Representative Office for the Americas, Mexico City.

[11] The Bank of Tanzania Act, Act No. 4 of 2006, [hereinafter "the BoT Act"], Section 6 (1) and (2).

ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

pieces of legislation in harmonization of electronic banking transactions.[12] Furthermore, the rules and regulations put in place by the electronic clearing houses and settlement systems bind only participants or members of such clearing and settlement systems;[13] generally, the law is superficially cover the aspect of electronic banking. The outcome of this legislative vacuum is the existence of practical legal issues such as: electronic cheques are not legally recognised unlike other methods of payment such as cash and paper-money; there is vagueness as to legal rights and obligations of parties in electronic banking transactions. This is because, rights and obligations conferred by the guidelines issued by the Bank of Tanzania (BoT) are uncertain with no legal force; there are some problems associated with admissibility of the electronic records and authentication of electronic signatures before the court of law; and; there is a higher possibility of cyber crimes going unpunished. These may include but not limited to; message interception, violation of data protection, financing terrorism, money laundering, interfering with computer system which may cause identity theft such as phishing, spoofing and e-fraud.[14]

In this piece of work therefore, the author embark on making a detailed legal analysis on practical issues of electronic banking which may be an obstacle to the electronic banking transactions in Tanzania; the consequences thereupon and provides the solution of the analysed practical issues while reveals the reason(s) as to why up until now Tanzania do not have adequate law governing electronic banking or any other cyber law for that matter which could adequately address and protect electronic banking transactions. To achieve the aforementioned, this paper covers the aspects of; historical background of the electronic banking, legal framework of electronic banking in Tanzania, practical issues on electronic banking in Tanzania, and finally conclusion and recommendations.

---

[12] These includes; Capital Markets and Securities Act [Cap 75 R.E 2002], The Companies Act, Act No.12 of 2002, The Evidence Act [Cap 6 R.E 2002], The Law of Contract Act [Cap 345 R.E 2002], The Electronic and Postal Communications Act, Act No. 3 of 2010, The Anti-Money Laundering Act, 2006, The Proceeds of Crime Act [Cap 254 R.E 2002] and The Bills of Exchange Act [Cap 215 R.E 2002]; and also Rules and Regulations made by the Bank of Tanzania to regulate inter-banks electronic transactions.

[13] Tanzania Inter-bank Settlement System (TISS) Rules and Regulations, 2003, Section 3. "These Rules and Regulations shall apply to all TISS participants for the transactions in the TISS and are binding to the TISS participants by the "Agreement for participating in TISS" signed by the TISS participants." Mbeya Electronic Clearing House (MBECH) Rules and Regulations, 2008, Section 1(4) (iv). "The Clearing Rules and Regulations are binding between the member banks and are designed to facilitate inter-bank cheque clearing."

[14] Mambi, *supra*, note 8, 124.

ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

1. Historical Background of Electronic Banking

The use of electronic banking can be traced back to 1950s in Western countries when electronic message transmitters and clearing houses used magnetic ink character for cheques.[15] This was possible because of the discoveries in the ICT.[16] Due to such development of technology in information and communication sector, the way of doing business around the world took another turn as Kofi Atta Annan[17] once said "information and communication technologies (ICTs) have the potential to profoundly change global trade, finance and production. By making businesses more competitive and economies more productive..."[18]

Clearing houses and electronic message transmitters adopted this technology in banking operations includes; Society for Worldwide Interbank Financial Telecommunication (SWIFT), Master Card Company (MCC), Visa Card Company (VCC), Dyna Card Company (DCC) and others. These companies facilitate payments settlement internationally.[19] For example, a customer of CRDB bank who owns a master card, when transact by using a master card at a point-of-sale in London, master card company is responsible for settling such payment from the customer account in CRDB bank.[20] However, this can only be possible if CRDB is a member of Master Card Company.

In Tanzania, electronic banking operations started in the late 1990s.[21] The banking services offered electronically includes; payment through cards i.e. credit cards, debit cards, and pre-paid cards. Other services are home banking, office banking, internet banking, cheque

---

[15]"http://www.scribd.com/doc/18028736/Online-Banking-System" (accessed 30 March 2011).
[16]The National Information and Communication Technologies Policy 2003, 1. "Information and Communications Technologies (ICT) advances since the end of the 20th Century have led to multiple convergences of content, computing, telecommunications and broadcasting. They have brought about changes in other areas, particularly in knowledge management and human resources development. Increasing capacity of ICT has further been empowered by the growth of a global network of computer networks known as the Internet. It has impacted the way business is conducted, facilitated learning and knowledge sharing, generated global information flows, empowered citizens and communities in ways that have redefined governance, and have created significant wealth and economic growth resulting in a global information society."
[17] Former Secretary-General of the United Nations served from 1 January 1997 to 31 December 2006.
[18] As quoted by Mollel & Lukumay, *supra*, note 1, 1.
[19] "http://www.bis.org/publ/bcbs98.htm" (accessed 31 March 2011).
[20]Commission of such transaction is shared between Master Card Company and CRDB as according to John Almasy, a branch manager of the CRDB Iringa branch in a seminar at Ruaha University College on 15 March 2011.
[21]"http://www.bot-tz.org" (accessed 2 April 2011).

truncation and the use of ATMs.[22] Additionally, electronic banking facilitates inter-bank monetary transfer within and outside the country.[23] In 1999, Tanzania Bankers' Clearing House issued paper instrument standards specifying requirements for computer printout of cheques and transactions done at point of sale.[24]

In 2000, BoT issued Guidelines on Introduction and Operation of Auditable Card Based Electronic Money Schemes in Tanzania for the purpose of addressing the key strategy and operational issues essential for any institution that dealing with e-money products.[25] The Bank of Tanzania Electronic Clearing House (BOTECH) became operational in 2002. BOTECH facilitates normal inter-bank electronic debit clearing and it has connectivity with clearing houses in major cities in Tanzania namely; Dar es Salaam, Arusha, Mwanza, Mbeya and Zanzibar.[26] Membership is limited to licensed commercial banks only and their main role is to facilitate the clearance of paper-based inter-bank instruments, principally cheques.[27]

Currently, interbank clearing is processed electronically at the Dar es Salaam Electronic Clearing House (DECH) which accounts for 80% in volume of the country's interbank clearing while the remaining 20% is processed manually.[28] In 2003, the National Information and Communications Technologies Policy was adopted which carries the vision and mission towards facilitation of the application of the ICT in improving the living standards of Tanzanians as it states;

> "The National ICT Policy is aligned to the following vision statement: Tanzania to become a hub of ICT Infrastructure and ICT solutions that enhance sustainable socio-economic development and accelerated poverty reduction both nationally and globally. The overall mission of this Policy is: To enhance nation-wide economic growth and social progress by encouraging beneficial ICT activities in all sectors through providing a conducive framework for investments in capacity building and in promoting

[22] "http://www.bot-tz.org" (accessed 4 April 2011).
[23]Bank of Tanzania, "Payment System in the Southern African Development Community – Tanzania Chapter" available at "http://www.bot-tz.org" (accessed on 20/05/2011); Guidelines on Introduction and Operation of Auditable Card Based Electronic Money Schemes in Tanzania 2000, Section One. [hereafter "the Guidelines"].
[24]Tanzania Bankers' Clearing House, "Paper Instrument Standards: Directorate of National Payment System", 4. Available at "http://www.bot-tz.org" (accessed 24 May 2011).
[25]"http://www.bot-tz.org" (accessed 24 May 2011). Thus, the guidelines save as a safeguard measure to consumer interests and having standardization for future system integration.
[26]"http://www.bot-tz.org" (accessed 25 May 2011).
[27]"http://www.bot-tz.org" (accessed 25 May 2011).
[28] "http://www.bot-tz.org" (accessed 20 December 2014).

> multi-layered co-operation and knowledge sharing locally as well as globally."

The banking sector makes heavy use of ICT to provide improved customer service with some banks using Very Small Aperture Terminals (VSATs) or public leased lines to interconnect their branches and cash dispensing ATMs.[29] In the same year (2003) Tanzania Interbank Settlement System (TISS) was implemented and in 2004 became operational.[30] TISS is an online system which facilitates Real Time and Gross Settlement (RTGS) of payment instructions between banks in Tanzania.[31] In order for banks in Tanzania to engage in offering electronic services to their customers or engage in interbank electronic clearing, they should be both TISS and SWIFT members.[32] Tanzania has 29 total number of commercial banks out of which 20 banks are members of TISS and SWIFT.[33]

Thus, Tanzania has five electronic houses in total whereby the Bank of Tanzania is a host of all five clearing houses.[34] Therefore, Tanzania intensively uses electronic banking as it carried out by banks and communication entities such as Vodacom with MPESA, Zantel with ZPESA, Airtel with AIRTELMONEY, and Tigo with TIGOPESA. It is recognised as one of the payment methods by the Bank of Tanzania (BoT)[35] and Tanzania Communications Regulatory Authority (TCRA).[36] In any type of business, the law assures protection of parties involved in business. As already discussed, electronic banking facilitates banking business in

---

[29]The National Information and Communications Technologies Policy 2003, 5. Available at "http://www.tanzania.go.tz/pdf/ictpolicy.pdf" (accessed 20 September 2011).

[30] "http://www.bot-tz.org" (accessed 4 April 2011).

[31] TISS functionalities include online real time account management and interbank high value or time critical funds transfers. The system has two separate options; gross settlement and liquidity optimization settlement facility (LOSF) as provided in TISS brochure available at "http://www.bot-tz.org" (accessed 20 December 2014).

[32]TISS Rules and Regulations, 2003, Section 5(1) [hereafter "TISS Rules and Regulations"]. TISS operates by using three main components i.e. SWIFT network, the participant (member) webstation and the TISS central system.

[33]Also known as Tanzania SWIFT user group. These includes CRDB, NMB, NBC, TPB, Barclays, Citi bank, Standard chartered etc. ("http://www.bot-tz.org" accessed 25 May 2011).

[34]These includes BOTECH, DECH, TBCH, MBECH and TISS which is overall. ("http://www.bot-tz.org" accessed 25 May 2011). The clearing houses hold two clearing sessions daily one for TZS instruments and another for USD cheques. Exchange of cheques takes place from 10:00am – 4:30pm on each working day. Money clearing is done once a day for TZS 9:30am – 10:00am and for USD 11:30am.

[35] The BoT Act Section 6; "http://www.bot-tz.org" (accessed 20 December 2014).

[36]TCRA is responsible in communication network in electronic banking e.g. mobile banking payments are regulated by both BoT and TCRA. The former in aspect of observing financial transactions and the latter in monitoring the mobile phone operations. The two authorities have signed a memorandum of understanding to regulate mobile money transfer services. ("The Citizen" 23 February 2011).

particular and e-commerce in general. Given the importance of banking and the risky circumstances it is involved in, the law should adequately regulate electronic banking to protect banking business which may be affected with electronic banking if it is not so adequately regulated.

2. Legal Framework of Electronic Banking in Tanzania

The legal framework does not only refer to the law but also to proper legal institutions and competent legal personnel capable to determine matters brought before them. The legal framework to accommodate electronic banking in Tanzania comprises; the Bank of Tanzania Act, 2006 and the Banking and Financial Institutions Act, 2006. The Acts continue to recognise TISS and MBECH Rules and Regulations made under the Bank of Tanzania Act, 1995. The Rules and Regulations set to govern transactions in inter-bank settlement system and at clearing houses. The Rules and Regulations[37] provide for inter-bank electronic transactions between banks within and outside Tanzania as TISS members are also required to be SWIFT members; other laws of the land are also applicable in electronic banking transactions e.g. evidence law, contract law, criminal laws etc; The High Court (T) Commercial Division established under Rule 5A of the High Court Registries (1984) Rules as amended by GN. 141 of 1999 which was later repealed and replaced by GN. 96 of 2005 adjudicates Commercial cases.[38]

The central objective for establishing the Commercial Division was to put in place a specialized court which would gratify the business community by determining Commercial disputes proficiently and effectively.[39] The Commercial Court can determine civil cases of

---

[37] These includes; Bank of Tanzania Electronic Clearing House Rules and Regulations, 2002; Dar es Salaam Electronic Clearing House Rules and Regulations, 2007; Mbeya Electronic Clearing House Rules and Regulations, 2008; Tanzania Bankers' Electronic Clearing House Rules and Regulation, 2002; Tanzania Interbank Settlement System Rules and Regulations, 2003.

[38] The High Court of Tanzania Commercial Division is one of the three Divisions of the High Court of Tanzania. It started its operation on 15 September, 1999 following a decade of legal reform process. It is now eleven (12) years old. Electronic banking cases may also fall under the jurisdiction of this court.

[39] The Judiciary of Tanzania, the High Court (T) Commercial Division Report 2010. The establishment of the commercial division therefore aimed at strengthening the private sector by encouraging both local and foreign investors.[39] The Commercial court serve as an insurance tool that can effectively, efficiently and speedily resolve commercial disputes that were to emerge in the stir of expanded business and commercial activities.[39] Generally, the call for the Commercial Court was a result of the developments in the management of the economy where privatization became an order of the day.

commercial nature under its both original and appellate jurisdiction.[40] In a number of decided cases judges endeavour to cover a wide interpretation of the document to include electronic document such as; In *Trust Bank's Case*, the Court extended the definition of banker's book to include computer printouts (this case was decided before the amendment of the Evidence Act, it has been argued that this case encouraged the amendment of the Evidence Act in 2007). In the case of *Tanzania Bena Co. Ltd v. Bentash Holdings Ltd*[41] the Court acknowledged communication conducted via email to be tendered as evidence. In the case *National Bank of Commerce v. Milo Construction Co. Ltd and Two Others*[42] the Court admitted in evidence statements stored in computer program. However, the interpretation of the judiciary alone cannot to be said to be sufficient in facilitating electronic banking transactions. A comprehensive piece of legislation is still needed to fully support and protect electronic banking undertakings.

It is undisputed fact that, the current legal framework has tried to accommodate electronic banking in Tanzania, and so far been marked as a landmark process towards effective legal framework which fits in the current technological circumstances in Tanzania. It should be noted therefore, that the current legal framework manages to partially accommodate electronic banking transactions but it can only be likened to 'a one drop of water in the ocean'. There is still a lot to be done so as the legal framework in Tanzania can fully and effectively accommodate electronic banking as well as electronic transactions in general.[43]

---

[40] The High Court Registries Amendment Rules 2005, Rule 5A (2) which states: "The Commercial Division of the High Court shall have both original and appellate jurisdiction over cases of Commercial significance." The Commercial Division did not have appellate jurisdiction from its inception as provided under Rule 2 of the High Court Registries Amendment Rules 1994. It was not until 2005 when the court was clothed with appellate jurisdiction, which allows it to hear appeals from subordinate courts i.e. the Resident Magistrates' Court and District Magistrates' courts.

[41] *Tanzania Bena Co. Ltd v. Bentash Holdings Ltd,* Commercial Case No. 71 0f 2002 (unreported).

[42] *National Bank of Commerce v. Milo Construction Co. Ltd and Two Others*, Commercial Case No. 293 of 2002 (Unreported).

[43] J. Ubena, Why Tanzania Needs Electronic Communication Legislation? Law Keeping up with Technology, 2 *Law Reformer Journal* 1, (2009), 17. "Information Communication Technology (ICT) in the name of electronic communication as an industry in *stricto sensu,* is unregulated in Tanzania. The country has therefore been running the risk of being a cyber criminals' haven. It is true for instance that, when one decides to spread computer viruses maliciously, he cannot be prosecuted in Tanzania, the reason being that we do not have a legislation in place to govern or address that problem. This is no longer a problem in some countries such as the United Kingdom which have already adopted the Convention on Cyber Crimes and have enacted the Computer Misuse Act, 1990. Other countries in the whole of European Union, member states have electronic communication legislation."

ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

3. Practical Legal Issues on Electronic Banking in Tanzania

This part explores practical legal issues posed to electronic banking given that for there is no specific law catering for the same and the existing banking laws are superficially cover aspects of electronic banking. Emphasis is drawn on the following insurmountable legal issues; legality of electronic cheques, legality of electronic banking agreements, legal rights and obligations of parties in electronic banking transactions, admissibility of electronic records and authentication of electronic signatures and prosecution of cyber crimes. The exploration of these issues are presented as hereunder;

3.1 Non-Legal Recognition of the Electronic Cheques

Methods of payment currently used in Tanzania, are cash, paper-money and electronc money. The third method comprised with it electronic cheques. The first two method are fully recognized by Tanzanian banking laws. For example; payment by cash is provided by the BoT Act and it is required that payment by cash be made in the legal tender.[44] The legal tender described is bank notes and coins at their face value.[45] In case of bank notes, a shilling, or any multiple of a shilling, suffices for payment of any amount.[46] In the case of coins having a face value of fifty cents or below, payment of any amount not exceeding five hundred shillings is effected.[47] Paper-money can be paid through a bill of exchange and promissory note. A bill of exchange defined as; "[A]n unconditional order in writing, made by drawer instructing drawee to pay to the holder of an instrument against drawer's account."[48]

A cheque is a bill of exchange which is used in payment as paper-money.[49] The definition of bill of exchange seems to exclude electronic cheques as one of the payment instrument. In common law principles, the requirement of a bill of exchange to be in writing and be signed, excludes data message or electronic materials. An instrument which does not comply with the conditions stipulated in Section 3 (1) is not a bill of exchange.[50] However, an electronic cheque is carried out as a payment instrument. The side effect of electronic

[44] The BoT Act, Section 28.
[45] The BoT Act, Section 28 (1) (a) and (b).
[46] The BoT Act, Section 28 (1) (b) (i).
[47] The BoT Act, Section 28 (1) (b) (ii).
[48] The Bills of Exchange Act [Cap 215 R.E 2002], Section 3 (1). [hereafter "the BEA"].
[49] The BEA, Section 73 (1). "A cheque is a bill of exchange drawn on a banker payable on demand."
[50] The BEA, Section 3 (2).

cheque not having legal recognition is that there is uncertainty as to when it can be said that payment is effected when such payment is intended to be carried out through electronic cheques. In other jurisdictions such as United States of America, United Kingdom, and majority of European Union member states, electronic cheque is legally recognized as one of the instruments of initiating payment through EFT.[51]

3.2 Problems Associated with Legality of Electronic Banking Contracts

A contract is established when an offer has been accepted and consideration has been formed. As a consequence thereafter, both offeror and offeree are bound with such an agreement and the agreement becomes enforceable by the law.[52] Normally, in traditional banking, a contract between a bank and an individual created when an individual makes an offer to the bank to open an account and the bank accepts such offer. The consideration is the deposits paid in by the customer. Accordingly, the customer becomes a creditor and the bank becomes a debtor obligated to repay the creditor at creditor's convenience.[53] An electronic banking contract refers to a contract done via electronic means between a bank and a customer for banking purposes. The most common way of concluding an electronic contract is by exchanging email through websites.[54] It should be noted that, electronic banking contracts are not for trivial matters, rather they are for serious contracts as they involve money transfer. It could involve credit facilities whereby a person can apply for a loan online and other procedures to process will follow later after the said contract has been concluded. The important issue is as to whether electronic banking contracts are enforceable. That is the

---

[51] N. N. N. Nditi, *Banking Lecture Material*, (unpublished), 55. "in England it became necessary to amend the law in 1996 to allow cheque truncation. A new section was inserted into the Bills of Exchange Act, 1882. The amendment was effected through an order named Deregulation (Bills of Exchange) Order 1996. The law as amended by insertion of Section 74B into the BEA, 1882, now permits the presentation of the cheque by means of electronic or similar message, which set out the fundamental features of the cheque namely; serial number, the sorting code of the drawee bank, the number of the account on which the cheque is drawn and its amount."; See also, Ubena, *supra*, note 43, 17.

[52] The Law of Contract Act [Cap 345 R.E 2002], Section 2, [hereafter "the LCA"].

[53] The BoT Act and the BFIA, Section 3; *Joachimson v. Swiss Bank Corporation* [1921] 3 K.B 110; N.N.N. Nditi, Banking Law Lecture Material" (unpublished), 90.

[54] Mollel & Lukmay, *supra*, note 1, 29. "…the two most common ways of entering into contract on the world wide web are by exchanging e-mail or by what is known as web-click whereby a shopper visits the website of an e-merchant and selects the item(s) or orders the service that he or she is after. There are certain preliminary considerations that apply to both types of contracts. Such considerations include whether a valid contract can be concluded wholly electronically at all and, if it can, how such a contract can be authenticated and attested to by a legally valid signature if necessary and what the legally acceptable proof of the contract is?"

whole concept of legality because in order for a contract to be enforceable it must be legal, contrary to that, such contract cannot not be enforceable and thus is void *ab initio*[55]

The Law of Contract Act[56] do not provide for this type of contract. One may wonder why electronic contract are exceptional. These contracts are just simple contracts and are not different from the ones concluded manually. The only difference is that they are concluded electronically. Given the position of the law, an electronic contract cannot be similar to traditional contract.[57] One simple example is that electronic contracts do not adhere to the rules of communication, acceptance and revocation of proposals as laid down by the Act. The communication of a proposal is complete when it comes to the knowledge of a person to whom it is made.[58] The communication of an acceptance is complete as against the proposer, when it is put in a course of transmission to him, so as to be out of the power of the acceptor,[59] as against the acceptor, when it comes to the knowledge of the proposer.[60] The communication of a revocation is complete as against the person who makes it, when it is put into a course of transmission to a person to whom it is made, so as to be out of the power of a person who makes it,[61] as against the person to whom it is made, when it comes to his knowledge.[62]

The fact that, electronic material gets to a receiver at the very same moment after being sent, there is no room for revocation. In other words when a proposal has been accepted a promise cannot be revoked. Since the law of contract do not provide for electronic contracts, that makes electronic banking agreements invalid simply because they do not meet legal requirements of the law. According to the cited provisions, the law affords parties reasonable time in formulation of a contract, different between the offeror and the acceptor in

---

[55] The LCA , Section 2, "an agreement not enforceable by law is said to be void".
[56] [Cap R.E 2002].
[57] C. Riefa & J. Hornle, " The Changing Face of Electronic Consumer Contracts in the Twenty-First Century: Fit for Purpose?" in L. Edwards & C. Waelde, (Eds), *Law and the Internet*, Oxford and Portland, Oregon 2009[3], 93; Mambi, *Supra,* note 8, 22. "Normally under English Law or Common Law the formation of a contract requires four main elements namely offer, acceptance, consideration and intention to create legal relations. These elements might be affected by the development and use of e-commerce. Common Law countries like Tanzania have historically relied heavily on the transfer of written, signed and authenticated documents. Some statutory rules require that some contracts be made or evidenced in particular way namely by deed, under seal and writing. They also have to be signed manually before a witness and be evidenced with original documents.
[58] The LCA, Section 4 (1).
[59] The LCA, Section 4 (2) (a).
[60] The LCA, Section 4 (2) (b).
[61] The LCA, Section 4 (3) (a).
[62] The LCA, Section 4 (3) (b).

communication, acceptance and revocation of the proposal. The *rationale* of this is to give parties enough time to decide on and submit themselves to a legal relation created as against one another[63] unfortunately electronic contract as the law stands, do not afford the parties such an opportunity.

The argument put forward under this aspect is that, Tanzanian law of contract is inadequately providing for electronic contracts because it is impossible for electronic contracts to meet the requirement of the law currently in force from its formation stage.[64] Meaning, it does not afford parties opportunity to reconsider their intention of formulating a contract before final conclusion of such contract. Additionally, it is based on traditional way of forming a contract such as by writing, orally or by conduct and under seal.[65] The fact that, common law tradition regard writing as tangible document that excludes electronic contract simply because the latter is in intangible form.[66]

Thus, electronic banking agreements need to comply with law in order to be valid and enforceable. This can only be possible if the law in force affords such an opportunity. Although UNCITRAL Model Law provides that, a contract shall not be denied validity or enforceability on the sole ground that it is in a form of electronic communication,[67] but an agreement which is contrary to the law, is *prima facie* not valid and thus cannot be enforceable. It is not enough only considering technological developments and forget about

---

[63] Mambi, *supra*, note 8, 23. "It is cardinal principle of contract laws under common law that the revocation of an offer or acceptance is said to be effective only if it is communicated. In this way, the communication of revocation is complete at different times for the person who makes it, and also for the person to whom it is made. In other words, for the person who makes the revocation, the communication of revocation is complete when it is put into course of transmission to the to whom it is made. And for the person to whom revocation is made, the communication of revocation is complete when it comes to his knowledge"

[64] Mambi, *supra*, note 8, 29. "the other criterion for validity of an online contract is the ability to reject. Assent now- terms later contracts were not enforceable because they eliminate the user's necessary ability to reject the agreement."

[65] Mambi, *supra*, note 8, 26. "there are considerable number of traditional staruroty rules in countries that apply common law principles like Tanzania about particular types of contracts requiring them to be made or evidenced in particular way. These requirements which are contrary to electronic contracts can be categorized as follows: the contract must be under seal. This is a legal requirement for a valid contract; the contract must be in writing and the contract must be evidenced in writing and signed before a witness. The definition of writing and signature under the current laws does not involve data message. In addition to that it is impossible for both parties entering into contract to use other parties to witness their transactions under cyberspace. "

[66] Mollel & Lukumay, *supra*, note 1, 30. "under pre-internet era traditional law, such contract would not normally satisfy the requirement of writing because that would require visible representation in tangible form whereas computer data is strictly speaking intangible."

[67] United Nations Convention on the Use of Electronic Communications in International Contracts, 2005, Article 8 (1).

the law which can go hand to hand with such development.[68] The fact that Tanzanian contract law inadequately provide for electronic contract, it creates legal challenge to the electronic banking because the side effect of this is that, banks cannot conclude electronic contract even if does, the said contract is void. Accordingly, one cannot be more wrong to assert that, generally, Tanzania contract law neither facilitate nor protecting electronic banking.

As one of the payment system, electronic banking should be facilitated and gain strength from the law for its very purpose of conducting banking business. And due to its nature, it is wise to strengthen the same because this will even help on acquiring new customers without the customers having physical contact with the bank of his or her choice. It is important to note that banks are very crucial in economic activities of any country.[69] Thus by having strong legal framework in place providing for electronic banking contracts, will act as an incentive to the pontential customers and banks. On a more positive note banks would have a wide involvement in other types of banking business electronically as well rather than concentrating in EFT only.

3.3 Uncertainty in Legal Rights and Obligations of the Parties in Electronic Banking Transactions

In traditional banking, parties to a contract, are the banker and the customer. In electronic banking, normally a contractual relationship involves more parties than usual. For example a single electronic fund transfer at point of sale (EFTPOS) transaction involves five contractual relationships. These are; between a bank customer and a seller, between a bank and a customer, between a seller and a seller's acquirer, between a seller's acquirer and a bank, and between a seller's acquirer and a seller's bank.[70] All of these contractual relationships make electronic banking more complex and thus requires harmonization. In traditional banking, parties to a banking contract were debtor and creditor.[71] Rights of one

[68]J. Ubena, Why Tanzania Needs Electronic Communication Legislation? Law Keeping up with Technology, 2 *Law Reformer Journal* 1, (2009), 22. "The pace of ICT development turns legislation obsolete. The law ought not only to be flexible but also be proactive to see to it that it neither leaves people unprotected against new technologies nor hamper the development of technologies themselves."

[69] MBECH Rules and Regulations, Section 22 (1) "A payment system covers the complete process from initiating a payment transaction, processing of the transaction through to settlement finality. The NPS.

[70]Chartered Institute of Bankers, *Law Relating to Banking Services: Bankers Workbook Series*, Sheffield Hallam University, London 1994, 150.

[71] *Foley v. Hill* (1818) 2 H.L 28.

party are the obligations of another party and *vice versa*. The following are some of the rights and obligations of parties in traditional banking contract; a bank has an obligation to repay a customer on demand according to the customer's instructions,[72] the customer has a right to withdraw cash at his or her convenience. Both a bank and a customer have a duty to disclose forgeries.[73] If the customer knows about the forgery and choose not to disclose and the bank pay against such forgery, the bank will be released from the liability and *vice versa*.[74]

The same position was given in the case of *Tai Hing Cotton Mill Ltd v. Liu Chong Hing Bank Ltd and Others* [1985] 2 All E.R 947, when the court observed that, in the absence of an express agreement to a contrary, a duty of care owed by a customer to his bank in the operation of his account, is limited to a duty to refrain from drawing a cheque in such a manner as to facilitate fraud or forgery. Also a customer has an obligation to inform the bank of any unauthorized cheque purportedly drawn on the account as soon as he, the customer, becomes aware of it. And in the case of *Silayo v. CRDB (1996) Ltd* [2002] 1 EA 288, the court stated that, the bank has the duty to detect fraud when a bogus cheque is presented for payment. Customer has a duty when drawing and handling cheque to exercise duty of care and diligence,[75] the bank has a right not to be deceived by the customer.

The bank has the duty of secrecy over customer's account;[76] the customer has the right to privacy of his or her account. In the case of *Tournier v. National Provincial and*

---

[72] The common Section 3 of both The BoT Act, and The Banking and Financial Institutions Act, Act No. 5 of 2006 [hereinafter "the BFIA"]; Nditi, *supra*, note 31, 89; *Joachmson v. Swiss Bank Corporation* [1921] ALL E.R 92.

[73] *Greenwood v. Martins Bank Ltd* [1932] All E.R 318.

[74] *Greenwood v. Martins Bank Ltd* [1932] All ER 318. "the plaintiff, who kept his account with the defendant bank, entrusted his wife the custody of the cheque book and pass book. In October 1929, when he asked her for a cheque to draw pounds 20 she confessed to him that she had drawn out all the money in the account saying that it was needed to help her sister in legal proceedings. Out of consideration for his wife the plaintiff refrained from advising the bank of the forgeries for eight months. However, in June 1930, when she told him that she wanted a further pounds 60 for the legal proceedings, he made an inquiries and, discovering that there was no such litigation, he told her he was going to inform the bank, whereupon she shot herself. The plaintiff brought an action against the bank for pound 4106s., the amount paid against forged signatures. The plaintiff was stopped from denying the authenticity of his wife's signatures as his because the plaintiff was under duty to inform the bank about his wife withdrawals as soon as he was aware of them so as to put on guard…had the plaintiff informed the bank as required, the bank would have been held liable for paying against forged authorizations" as quoted in N. N. N. Nditi, *Banking Law Materials*, (unpublished), 84.

[75] *London Joint Stock Bank v. McMillan & Arthur* [1918] A.C 777.

[76] The BFIA, Section 48. "Every bank or financial institution shall observe, except as otherwise required by law, the practices and usages customary among bankers, and in particular, shall not divulge any information relating to its customers or their affairs except in circumstances in which, in accordance with the law or practices and usages customary among bankers, it is necessary or appropriate for the bank or financial institution to divulge such information."

Union Bank of England Ltd, the bank was worried about an overdraft of its customer. As a result it disclosed to the customer's employer that his account was overdrawn and that the customer was thought to be gambling. The court held that, the disclosure of information by the bank to the customer's employer was breach of the bank's contractual duty of secrecy owed to the customer.[77]

In electronic banking, there are high possibilities of fraud and forgeries. In cheque truncation for example, there is no physical contact between a bank and a customer, a computer hacker may forge the cheque and send to a paying bank. Under this situation, it is over and out of the bank's and customer's hand, so who is to take the responsibility? Is it a bank, customer or a network provider? Again in electronic banking more than one contractual relationship is involved. This makes difficult to ascertain the rights and duties of each party. For example, when an ATM fails to dispense cash to the customer due to a power cut, who is to blame, is it the bank or power provider? Does the right of the customer to receive cash in his or her demand and the duty of the bank to repay the customer on demand still stand? Due to the fact that, there is no specific electronic banking laws or banking laws currently in force to address electronic banking, answering these questions is difficult because the legal rights and obligations are not well established.

Although guidelines for payment cards emphasize that, parties to electronic payment cards must enter into legal binding agreement so as to guide the electronic transactions via ATM, POS, automated call distributor (ACD) and bank computer terminals, yet the legal rights and obligations of each party are uncertain. The agreement often referred to as service level agreement (SLA).[78] The rights and obligations of each party must be well defined, disclosed and enforceable.[79] According to these guidelines, a bank and a customer must conclude a legal agreement in the use of an ATM card or payment card that will be used only in approved POS and ATMs or ACDs and bank terminals. The agreement must be

---

[77] *Tourneir v. National Provincial and Union Bank of England Ltd* [1923] All E.R 550. See also *Intercom Services Ltd and Others v. Standard Chartered Bank Ltd* [2002] 2 EA 391.

[78] The Guidelines on Introduction and Operations of Auditable Card Based Electronic Money Schemes in Tanzania, 2000, [hereinafter "the Guidelines"], Guidelines 10 (2) (xi) and 11 (5) (ii). "legally binding, enforceable and transparent service level agreements (SLAs) shall be in place and agreed between all relevant participants to a scheme. Such SLAs will reflect the levels that are commonly accepted on an international basis."

[79] The Guidelines, Guideline 10 (2) (xi) and 11 (5) (ii).

ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

guided by the law currently in force. This means, the law of contract will apply in this type of agreement for electronic banking.

Thus, in case of any breach, parties will sue on the Law of Contract Act[80] provided that their agreement was concluded accordingly. This probably answers the questions posed earlier that, which law can parties can apply in suing one another. But then, how can anyone sue another if he or she is not sure about the legal rights and obligations he or she has against such a person.

According to the Guidelines on Introduction and Operations of Auditable Card Based Electronic Money Schemes in Tanzania, 2000 which is basically for payment cards, parties themselves has to determine their rights and obligations[81] this can only mean the rights and obligations will vary from one parties to the other save only to those rights and obligations the guidelines propose that they must be included.[82] However, it should be noted that, the guidelines are mere guiding principles and do not solely confer a legal obligation on the parties on which terms of such contract should be put in place. Meaning, parties have the liberty to choose on which rights or obligation they should have. Considering the fact that, electronic banking is a very crucial aspect for financial intermediary, it would have been better if rights and obligations of the parties are well certainly established.

Uncertainty in legal rights and obligations of the parties to electronic banking is a legal challenge to electronic banking undertakings because banks may be in a difficult situation in abiding with the law. For example, banks must not divulge customer's information to the third party as the provision of the law provides;

> "Every bank or financial institution shall observe, except as otherwise required by law, the practices and usages customary among bankers, and in particular, shall not divulge any information relating to its customers or their affairs except in circumstances in which, in accordance with the law or practices and usages customary among bankers, it is necessary or appropriate for the bank or financial institution to divulge such information."[83]

[80] [Cap 345 R.E 2002].
[81] The Guidelines, Guideline 11 (5) (ii).
[82] *Idem.*
[83] The BFIA, Section 48 (1).

However, the provision gives an exception as to such disclosure of information. The phrase "except as otherwise required by law" gives a bank room to depart from the doctrine of confidentiality. Accordingly, banks normally disclose customers information empowered by different pieces of legislation such as; the Law of Evidence Act,[84] the Prevention of Terrorism Act,[85] the Prevention and Combating of Corruption Act,[86] the Mutual Assistance in Criminal Matters Act, the Proceeds of Crime Act,[87] the Drugs and Prevention of Illicit Traffic in Drugs Act, the Public Leadership Code of Ethics Act, and the Anti-Money Laundering Act.[88] Looking at the aforementioned provisions, banks can do that, when a customer is involved in criminal issues. This means therefore, when a bank gives information of their customer's account through electronic banking transactions is actually violating the provision of the law as laid down by Section 48 (1) of the Banking and Financial Institutions Act. For example in EFTPOS when a bank dishonours EFTPOS transaction for non-payment will have to disclose the reasons for such an act. This violates the law because electronic banking transactions are not covered under the exception phrase "except as otherwise required by law, the practices and usages customary among bankers." Additionaly, the doctrine of confidentiality or secrecy is violated due to the fact that, electronic message passes through a

[84] [Cap 6 R.E 2002], Section 77 "subject to this Act, a copy of any entry in a banker's book shall in all legal proceedings be received as *prima facie* evidence of such entry and of the matters, transactions and accounts therein recorded."

[85] The Prevention of Terrorism Act, Act No. 21 of 2002, Section 41 (2) and (3). (2) "every financial institution shall report, every three months, to police officer and any body authorized by law to supervise and regulate its activities (a) that it is not in possession or control of any property owned or controlled by or on behalf of a terrorist group; (b) that it is in possession or control of such property, and the particulars relating to the persons, accounts, and transactions involved and the total value of the property. (3) In addition to the requirement of subsection (2), every financial institution shall report, to the police officer, every transaction which occurs within the course of its activities, and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission of a terrorist act.

[86] The Prevention and Combating of Corruption Act, Act No. 11 of 2007, Section 12 (1). "the director general may by writing authorize any officer to search any person, if it is reasonably suspected that such person is in possession of property corruptly or illicitly acquired or to search any premises …in or upon which there is reasonable cause to believe that any property corruptly or illicitly acquired has been placed, deposited or concealed."

[87]The Proceeds of Crimes Act, [Cap 254 R.E 2002], "Where a financial institution has reasonable grounds for believing that information about an account held with it may be relevant to an investigation of, or the prosecution of a person for, an offence, the institution may give the information to a police officer."

[88] The Anti-Money Laundering Act, Act No. 12 of 2006, Section 15 (3). "where an applicant requests a bank, financial institution or any other reporting person to enter into a continuing business relationship; in the absence of such a relationship, any transaction, a bank, financial institution or any other reporting person shall take reasonable measures to establish whether the person is acting on behalf of another person."

number of transmission points; more people can have access to it and this contravenes the provision of the law.[89]

Furthermore, in electronic banking banks are exposed to another legal challenge through money laundering laws. For example, the Anti Money Laundering Act[90] banks are required to report any suspicious transaction of their customers from any type of transaction, be it electronic or traditional transaction.[91] Failure to report, banks are subject to punishment of a fine not exceeding one billion shillings and not less than five hundred million shillings or an amount equivalent to three times the market value of the property, whichever amount is greater.[92] The Anti Money Laundering Circular No. 8 of 2000 requires banks to restrict the withdrawal amount from electronic payment card. This is why; in ATM for example a normal customer cannot exceed TZS 1,000,000/= per day withdrawal for both domestic and international transaction while a corporate customer cannot exceed TZS 3,000,000/=.[93] This is done in order to prevent money laundering through electronic banking transactions.

This is a legal challenge for banks because they must comply with what the law provides but at the same time they have to satify demands and instructions of their customers. It should be noted that, customers differ in terms of financial capabilities. Probably it easier for a normal person to use TZS 1,000,000/= or 3,000,000/= per day rather than a successful businessman who is engaged in widespread use of money. It is a legal challenge because if banks dare to act to the contrary, they will absolutely have problem with the authorities. Additionally, due to the nature of electronic banking which engages a multiplicity of parties compared to traditional banking, it would be reasonable if the doctrine of privity to contract would be considered inapplicable. The doctrine of privity to contract, simply establishes that, strangers in a contract cannot sue or be sued on such contract. In the case of *Tweedle v.*

---

[89] The BFIA, Section 48. "Every bank or financial institution shall observe, except as otherwise required by law, the practices and usages customary among bankers, and in particular, shall not divulge any information relating to its customers or their affairs except in circumstances in which, in accordance with the law or practices and usages customary among bankers, it is necessary or appropriate for the bank or financial institution to divulge such information."

[90] Act No. 12 of 2006; "http://www.bot-tz.org" (accessed 20 December 2014).

[91] The Anti Money Laundering Act, Section 3.

[92] *Ibid*, Section 13 (b).

[93] Mr. Ngassa Maganga, CRDB bank teller – Iringa branch when respond to the question posed by the author on 8 December 2014. He adds even corporate customers vary. There are those who holds visa cards and those hold visa card premier. The two cards have similarity on limitation of withdraws but differ in other more privileges.

Atiknson,[94] the court observed that, any person who is not a party to a contract has neither rights nor obligations arising from the said contract.[95] In other words, a third party cannot enforce a contract. The same position was stressed up in the case of *Dunlop Pneumatic Tyre Co. Ltd v. Selfridge*[96] where the court demonstrated that, rights and obligations arising from a contract cannot be shared between the parties to a contract and the strangers.[97]

In electronic banking, as already seen, more than two parties are involved. Normally, banks tend to exempt themselves from liabilities. For example; in payment card transactions, the terms may exempt the bank from liability when the machine fails to dispense cash to customers. Due to the doctrine of privity to contract, this means that, the customer cannot complain against the network provider if such failure caused by the network provider. Because, the one in contract with the network provider is the bank and not the bank customer. Thus, it is the bank to complain on behalf of the customer. In case of *Beswick v. Beswick*[98] the court demonstrated that, the general rule in any contract is that, the contract binds parties to such a contract, however when such a contract is made for the benefits of third party who has a legitimate interest to enforce it, it can be enforced by such a third party in the name of contracting party or jointly with him or her.[99] Meaning, if a bank customer fails to receive cash from an ATM due to the network failure, he can actually complain against the network provider since the bank contracted with the network provider for the benefit of its customers.

However, the law of contract does not support this expanded doctrine (to allow bank customers as third parties to sue on the contract) even though it allows third parties to furnish consideration to the the promisee, they cannot sue on the contract.[100] Despite the presence of exceptions to the doctrine such as; in negotiable instruments a holder of a cheque on any unpleasant event can sue on any immediate parties; and when an agent acting within the instructions of the principal, customer can complain against such an agent,[101] yet,

---

[94] *Tweedle v. Atkinson* [1861] 123 ER 762.
[95] *Idem.*
[96] *Dunlop Pneumatic Tyre Co. Ltd v. Selfridge* [1915] AC 847
[97] *Idem.*
[98] *Beswick v. Beswick* [1966] 3 All ER 1.
[99] *Idem*.
[100] The LCA, Section 2 (1) (d). "when, at the desire of the promisor, the promisee or any other person has done or abstained from doing, or does or abstains from doing, or promises to do or to abstain from doing, something, such act or abstinence or promise is called a consideration for the promise."
[101] N.N.N. Nditi, *General Principles of Contract Law in East Africa*, Dar es Salaam University Press, Dar es Salaam 2009[1], 231.

according to the nature of the electronic banking, if it remain as it is, will depend only on the interpretation of the courts to determine whether the doctrine can or cannot apply. Again until the decision is reached, the current position place parties concerned at uncertainty.

3.4 Problems Associated with the Admissibility of Electronic Banking Records and Authentication of Electronic Signatures in Evidence

Electronic banking deals with electronic records which inevitably carry electronic signatures. The issue is whether the same can be admissible in the court of law to prove or disapprove allegations or matters in dispute relating to electronic banking. UNCITRAL is of the view that electronic records should not be denied legal effect, validity, enforceability, or admissibility on the sole ground that it is electronic record or data message.[102] In the absence of the law on either specific matter or provisions in various laws, this cannot be possible. Proving matters in dispute in electronic banking cases is a matter of evidence. Evidence as defined by the Evidence Act is to;

> "[D]enote the means by which an alleged matter of fact, the truth of which if submitted to investigation, is proved or disproved; and without prejudice to the preceding generality, includes statements and admissions by accused persons."[103]

The term 'means' refers to an accomplishment by which an outcome is brought about or a method(s) used to present facts in court for the aim of either proving or disproving an alleged matter.[104] "In other words, evidence is any matter of fact, the effect, tendency or design of which is to produce in the mind a persuasion, affirmative or negative, of the existence of some other matter of fact."[105] The landmark statute to this area is the Evidence Act.[106] The Act offers two forms of presenting evidence in the court of law. These are oral evidence and documentary evidence.[107] The best rule of evidence requires authenticity of the

---

[102] UNCITRAL Model Law on E-Commerce 1996, Articles 5 and 9 (1) and (2).
[103] The Evidence Act, [Cap 6 R.E 2002] hereinafter "TEA", Section 3 (1).
[104] A.S Hornby, *Oxford Advanced Learner's Dictionary of Current English,* Oxford University Press, Oxford 1989[4], 772, as cited by Mollel & Lukumay, *supra*, note 1, 65.
[105] Mollel & Lukumay, *supra*, note 1, 53-54.
[106] [Cap 6 R.E 2002].
[107] TEA, Section 61. "All facts, except the contents of documents, may be proved by oral evidence."

evidence itself. In case of oral evidence, it must always be direct.[108] Meaning, if it refers to a fact which could be seen, it must be the evidence of a witness who says he saw it;[109] if it refers to a fact which could be heard, it must be the evidence of a witness who says he heard it;[110] if it refers to a fact which could be perceived by any other sense, or in any other manner, it must be the evidence of a witness who says he perceived it by that sense or in that manner;[111] if it refers to an opinion or to the grounds on which that opinion is held, it must be the evidence of the person who holds that opinion or, as the case may be, who holds it on those grounds.[112]

In case of documentary evidence,[113] the contents must be proved by primary or secondary evidence.[114] Primary evidence means the document itself produced for the inspection of the court. The document means any writing, handwriting, typewriting and printing, Photostat, photograph and every recording upon any tangible thing that recording is reasonably permanent and readable by sight.[115] Secondary evidence is certified copies made from the original.[116] From these definitions, neither oral nor documentary evidence feature electronic record as evidence. However, as already submitted somewhere in this work, that the Evidence Act allows admissibility of electronic record in evidence before the court of law,[117] and expanded the definition of banker's book to include data message kept on an information system such as computers and storage devices, magnetic tape, micro-film, video or computer display screen or any other form of mechanical or electronic data retrieval

[108] TEA Section 62 (1). "Oral evidence must, in all cases whatever, be direct."
[109] TEA, Section 62 (1) (a).
[110] TEA, Section 62 (1) (b).
[111] TEA, Section 62 (1) (c).
[112] TEA, Section 62 (1) (d).
[113] Documentary evidence means all documents produced as evidence before the court. (Section 3 of the Evidence Act [Cap 6 R.E 2002])
[114] TEA, Section 63.
[115] TEA, Section 3.
[116] TEA, Section 65. "Secondary evidence includes – (a) certified copies in accordance with the provisions of this Act; (b) copies made from the original by mechanical process which in themselves ensure the accuracy of the copy and copies compared with such copies; (c) copies made from or compared with the original; (d) counterparts of documents as against the parties who did not execute them; and (e) oral accounts of contents of a document given by some person who has himself seen it."
[117] TEA, Section 40A. "In any criminal proceedings – (a) an information retrieved from computer system, networks or servers; or (b) the records obtained through surveillance of means of preservation of information including facsimile machines, electronic transmission and communication facilities; (c) the audio or video recording of acts or behaviors or conversation of persons charged; shall be admissible in evidence."

ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

mechanism.[118] Such a type of banker's book is admissible as a document and as primary evidence for the inspection of the court.[119] Provided that, proof may be given by a partner or officer of the bank and may be given orally or by an affidavit sworn before any commissioner for oaths or a person authorised to take affidavits.[120] Even so, admissibility of electronic records in electronic banking cases is still challengeable.

Firstly; the admissibility referred to, only deals with criminal proceedings leaving out civil proceedings of which most of them are commercial cases[121] in which banks are involved, as the Act reads;

> "In any criminal proceedings information retrieved from computer systems, networks or servers; or the records obtained through surveillance of means of preservation of information including facsimile machines, electronic transmission and communication facilities; and the audio or video recording of acts or behaviours or conversation of persons charged shall be admissible in evidence."[122]

Secondly; the nature of electronic records is intangible[123] contrary to the best rule of evidence which requires a document to be tangible.[124] As in the case of *Shirin Rajabali*

---

[118] TEA, Section 78A (1). "A print out of any entry in the books of a bank on micro-film, computer, information system, magnetic tape or any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such print out, and when such print out is supported by a proof stipulated under subsection (2) of section 78 that it was made in the usual and ordinary course of business, and that the book is in the custody of the bank it shall be received in evidence under this Act."

[119] TEA, Section 78A (2). "Any entry in any banker's book shall be deemed to be primary evidence of such entry and any such banker's book shall be deemed to be a "document" for the purposes of subsection (1) of section 64."

[120] TEA, Section 78 (2). However, the method of proving electronic record that are; electronic may be proved orally or by an affidavit cannot not be reliable because an electronic data can be easily changed without leaving a trace. The same method as established in Section 78 (2) is also used in proving paper based document. Since the two documents are different to each other cannot be similarly proved. Thus, electronic record requires scientific method to be proved for the satisfaction of the court. (E. T. Laryea, *Paperless Trade: Opportunities, Challenges and Solutions,* Kluwer Law International, The Hague 2002, 28).

[121] J. R. Kahyoza, "The Judiciary High Court of Tanzania Commercial Division"

[122] TEA, Section 78 (2). Mambi, *supra*, note 63, 186. "The Act has not cured the problem of legal certainty and admissibility of electronic evidence. This law seems to be mainly based on electronic evidence…under criminal proceedings. It might be difficult to apply such evidence where the only available evidence to be applied in cases related to civil and other cases or proceedings is e-evidence…The question of proof of the integrity of the electronic records or e-evidence has not been considered."

[123] Mollel & Lukumay, *supra*, note 1, 77.

[124] TEA, Section 3; S. M. Giordano, Electronic Evidence and the Law, 6 *Information System Frontiers* 2, (2004). "In contemporary world documents are created in electronic form. The development creates legal challenge since rules of evidence concentrates much on tangible form of evidence. Digital form differs from paper form of evidence and thus the former demands special treatment on how it can be authenticated, ascertained and admissible."

Jessa v. Alipio Zorilla the court demonstrated that, document must be proved by primary evidence by producing the document itself for the inspection of the court and secondary evidence is admitted in the court where the original cannot be found.[125]

Thirdly; the Act does not provide for compatible procedures in which the electronic evidence may be admissible. For example, printed document which bears an electronic signature, how can it be admissible? As already discussed, for evidence to be admissible it must be authentic, shows clarity, truth and genuinely. Signature on the document plays these roles.[126] A signature is defined to be the writing, or otherwise affixing, a person's name, or a mark to represent his name, by himself or by his authority with an intention of authenticating a document as being of, or as binding on, the person whose name or mark is so written or affixed.[127] Thus, a signature meant to identify a signatory, intention to sign and an intention to be bound by the content of such document.[128]

The assertion that, electronic documents cannot be reliable simply because they can easily be manipulated and due to their nature, can easily be open to fraudulent actions thus they cannot be accepted without a challenge is false. The truth is that legal community easily accepts and trust paper-based documents without any challenge compared to electronic documents because paper-based documents are readily acceptable and trusted. But even paper-based documents can be easily manipulated and thus one can tender false evidence.[129] The argument may have its basis but even so paper-based documents and electronic documents cannot be given equal ascertainment. Because, there is a huge difference between the two, it is just fair that electronic documents receive more challenges than paper-based documents because even if ascertaining the truthfulness of paper-based documents may be difficult, the difficulty cannot be similar to ascertaining truthfulness of electronic documents.

---

[125] *Shirin Rajabali Jessa v. Alipio Zorilla* [1973] LRT 84.
[126] Mollel & Lukumay, *supra*, note 1, 61- 62; *R v. Moore, Exparte Myers* [1884] 10 VLR 322; E. T Laryea, *Paperless Trade: Opportunities, Challenges and Solutions,* Kluwer Law International, The Hague 2002, 28. "proof in evidence has three meanings which are: due execution of a document shows that it was written and signed by the person purported to have been written and signed; documents tendered is the original or where a copy is admissible, a correct copy of the original; the extent to which the contents of the documents capable to establish matters stated therein under the rules of evidence."
[127] *Stroud's Judicial Dictionary* as quoted in Mollel & Lukumay, *supra*, note 1, 61.
[128] Mollel & Lukumay, *supra*, note 1, 83.
[129] E. T. Laryea, *Paperless Trade: Opportunities, Challenges and Solutions,* Kluwer Law International, The Hague 2002, 28.

ISSN 1821 – 7524
RUAHA LAW REVIEW (RLR)
VOLUME 2, NUMBER 2, 2014
FACULTY OF LAW, RUAHA CATHOLIC UNIVERSITY
PAGES 153 - 191

Therefore, it is reasonable to argue that evidence law must establish clear procedure that will help in proving electronic documents beyond reasonable doubt.

In order for a document to be admissible as evidence against any party in a suit, such a document must belong to such person and only such person's signature can tell that. As a general rule, once a person signs a certain document, the signatory cannot deny liability. In electronic documents or record, electronic signature is the main method of authenticating such a document or record.[130] Electronic signature is defined as an electronic sound, symbol or process, attached to or logically associated to electronic document with an intention of authenticating such a document.[131] It could be a name written at the end of an email message by the sender, a scanned signature that attached to the document, PIN and a mark.[132] The Tanzania landmark case on admissibility of electronic records in evidence is the case of *Trust Bank Tanzania Ltd v. Le-Marsh Enterprises Ltd and Others*[133] where the court admitted electronic records in evidence on the basis that, the law should keep pace with technological development in banking fraternity. Admitting the same, His Lordship Judge Nsekela, J submitted that;

> "Tanzania is not an island itself. The country must move fast to integrate itself with the global banking community in terms of technological changes and the manner in which banking business is being conducted. The courts have to take due cognizance of the technological revolution that has engulfed the world. Generally speaking as of now, record keeping in our banks is to a large extent "old fashioned" but changes are taking place. The law can ill afford to shut its eyes to what is happening around the world in the banking fraternity. It is in this spirit that I am prepared to extend the definition of banker's book to include evidence emanating from computers subject of course to the same safeguards applicable to other bankers books under Section 78 and 79 of the Evidence Act. Under the circumstances I decline the invitation...that evidence produced by computers should not be considered as bankers' book. As I have stated above, in as much as I

[130] Mollel & Lukumay, *Supra*, note 1, 80.
[131] *Idem.*
[132] *Ibid*, 81; J. X. Dempsey, Creating the Legal Framework for Information and Communications Technology Development: The Example of E-Signature Legislation in Emerging Market Economies, 1 *Information Technologies and International Development* 2, (2003). "laws in e-signatures and e-records are very important in creating legal framework for e-commerce in developing and transitional countries."; A. M. Nadal & J. L. F. Gomila, Critical Comments on the European Directive on a Common Framework for Electronic Signatures and Certification Service Providers, *FC '00 Proceeding of the 4th International Conference on Financial Cryptography*, 2001. "electronic signatures creates new challenges that demands legal regulations to solve them."
[133] Commercial Case No. 4 of 2000 (unreported), 3.

> subscribe to the view that the court should not be ignorant of modern business methods and shut its eyes to the mysteries of the computer, it would, however, have been much better if the position were clarified beyond all doubt by legislation rather than by judicial intervention."[134]

Even though the case admitted electronic record as evidence in civil cases, it did not lay down procedures on how electronic records and electronic signatures can be approved or authenticated. Proving an electronic document is still a challenge due to the difficulty of how to authenticate electronic signature. The method of authenticating signature must be reliable and appropriate to serve the purpose for which the electronic record was generated, stored or communicated.[135] For example where there is a scanned signature of a certain company director kept purposely to be inserted at the end of processed document, any employee gain access to it, may insert to a document and be able to transact with the bank as if authorised by such a director. The UNCITRAL proposes 'functional equivalent approach' which is based on analysing the purpose and functions of the traditional paper-based requirements. The aim is to determine how those purposes or functions could be fulfilled through electronic records, and if such electronic records meet the requirements, be admissible.[136]

Purpose and functions served by the paper based documents includes; to provide that a document would be legible by all, to provide that a document would remain unaltered over time, to allow for the reproduction of a document to enable each party to hold a copy of the same data, to allow for the authentication of data by means of a signature, and to provide that a document would be in form of being accepted to the public authorities and courts. However, more importantly is that legal requirements should be met by electronic records. Currently, as the law stands, electronic records and signatures do not meet the requirements of the law. This position poses legal challenges to electronic banking transactions and in case of inconveniences, parties may fail to obtain legal remedies.

In order to avoid any inconveniences which may cause any party in legal proceedings fail to obtain legal remedy, other jurisdictions have tried to do away with some of the problems in admissibility of electronic evidence and authentication of electronic

---

[134] *Idem.*
[135] UNCITRAL Model Law on E-Commerce, 1996, Article 7 (1) (b).
[136] UNCITRAL, "Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce", 1996, 20.

signatures. For example: Ghanaian Evidence Decree of 1975 defines the word "writing" to include handwriting, typewriting, printing, Photostatting, photographing, or electronic recording;[137] Supreme Court of the United States of America Rules on Electronic Evidence provides that, whenever a rule of evidence refers to the term writing, document, record, instrument, memorandum, or any other form of writing, such term shall be deemed to include an electronic document;[138]

Indian Information Technology Act provides that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained is such law, such requirement shall be deemed to have satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference.[139] Accordingly, the Indian Evidence Act was amended and expanded the definition of the term "evidence" to mean all documents including electronic records produced for the inspection of the court.[140]

All of these jurisdictions tend to include electronic records to the best rule of evidence, meaning electronic documents enjoy same status as paper-based documents. This is a waiver from the mandatory requirement of the law that document admissible in evidence should be tangible. However, other problems such as proof of such electronic documents are still challenge as many jurisdictions opt for functional equivalent approach.

3.5 Problems Associated with the Prosecution of Cyber Crimes

The Tanzanian criminal laws such as the Criminal Procedure Act, the Penal Code, the Anti-Money Laundering Act, the Extradition Act, the Terrorism Act, and the Proceeds of Crime Act, etc. makes no reference to cyber crimes.[141] This may cause cyber crimes to remain unprosecuted simply because the same do not fit to the definition of crimes

[137] The Ghanaian Evidence Decree, 1975, Section 179.
[138] Supreme Court of the United States of America Rules on Evidence, 2001 as quoted in Mollel &Lukumay, *supra*, note, 99.
[139] Indian Information Technology Act, 2000, Section 4.
[140] Indian Evidence Act, 1872, Section 3; Mollel & Lukumay, *supra*, note 1, 100.
[141] Mambi, *supra*, note 8, 181. "Most crimes in Tanzania are regulated by laws such as Criminal Procedure Act, the Penal Code, the Extradition Act and other related laws. However, most of these laws are out of date and do not take into account the development of technology that is always changing very rapidly. These might hinder the development of e-commerce as some of the new offences are not addressed."

as established by criminal laws currently in force.[142] Legal principles deny prosecution of offences which are not codified because un-codified offences are *prima facie* not offences as there is no offence without law. The same position was demonstrated in the case of *R v. Lloyd* when the court dismissed the charges because the e-theft offence did not match the definition of theft as established by the UK criminal laws.[143]

The occurrence of cyber crimes is very risky in banking business because banking is very crucial institution in any country's economy. But not being able to prosecute the offence, is even riskier because offenders will be set free. Therefore, current position of the criminal law is in twofold negative effects i.e. cyber criminals cannot be prevented to commit other cyber crimes nor deter potential others to do the same. Even if the court of law wishes to punish the offenders, it cannot do so because it will be in violation of the doctrine of natural justice and go against legal principles.[144] Therefore, the laws must address cyber crimes in order to protect electronic banking.

4. Conclusion

The study shows that, banks and communication companies in Tanzania intensely use of electronic banking. The electronic banking transactions offered in Tanzania include ATM transactions, electronic cheques transactions, POS transactions, internet banking transactions, telephone and mobile banking transactions, cross-border transactions, and inter-bank electronic transactions. Yet, currently Tanzania has no adequate law regulating electronic banking as the latter is regulated through banking laws previously enacted to regulate traditional banking.

The only reference banking Acts make to electronic banking, is when the BoT empowered to make guidelines, orders, circulars, rules and regulations to regulate national payment system under which electronic banking falls. Accordingly, the Guidelines on

---

[142] Mambi, *supra,* note 8, 181. "There is a great likelihood for culprits or criminals to evade their criminal responsibility under the current law provisions. The first concern might be on the whole question of the definition of theft under current law. For example Section 258(1) of the Penal Code [Cap 16 R.E 2002] provides; "A person who fraudulently and without claim of right takes anything capable of being stolen, or fraudulently converts to the use of any person other than the general or special owner thereof anything capable of being stolen, steals that thing." The main issue here is whether a data message or information which is intangible by nature can be stolen, and if yes, whether the offence can fall under this definition of theft."

[143] *R v. Llyod* [1985] 2 ALL ER 661.

[144] *Nullum crimen sine lege*; *nulla poena sine lege*, prohibition of retrospectivity, etc.

Introduction and Operations of Auditable Card Based Electronic Money Schemes in Tanzania and TISS and Electronic Clearing Houses Rules and Regulations were made to regulate the electronic banking in Tanzania. However, the guidelines do not carry any legal force rather they are mere guidelines to facilitate and regulate conducts of players in electronic banking transactions. Similarly, the Rules and Regulations made refer only to inter-bank transactions.

Although some of the bankers seem to agree with the BoT in sense that when players of electronic banking follows the BoT instructions documented in guidelines, circulars, orders, directives, rules and regulations, the risks surrounding the same are cleared or reduced. However, some of them argue that, due to inadequacy of the law, new electronic banking products are subjected to multiple checking which delays market opportunities and leave legal challenges unsolved. The banking Acts also gives mandate to the minister responsible for financial matters in Tanzania to make regulations to fulfil the objectives of the BoT Act. Through this mandate, the minister is capable to make by-laws to regulate electronic banking. However, regulation guiding electronic banking has not been documented. This is probably because the minister complies with the national payment system policy in which has the vision and mission that the system should be self regulated; or the minister agrees to the view that, law reduces business opportunities.

The Evidence Act provides for the admissibility of electronic records in evidence only with reference to criminal proceedings but do not establish how such records should be admissible. The Act also has loopholes as the admissibility of electronic records is not permissible in civil proceedings and makes no reference to electronic signatures. This area is very crucial because if electronic records in relation to civil proceedings and electronic signatures cannot be admissible in evidence, cases from electronic banking transactions which may rely only in electronic evidence cannot be resolved. Seeing the gravity, the UNCITRAL proposes that, the courts should use functional equivalent approach to admit the same. However, the UNCITRAL model laws in their essence designed to facilitate e-commerce and not to regulate the same. In whatever the case, the admissibility of electronic records and authentication of electronic signatures would be served better by the law rather than opting for functional equivalent approach.

The Bills of Exchange Act requires physical presentment of the cheque contrary to that, the cheque will be dishonoured due to violation of the law. However, the Act gives an

option to parties involved to waive such requirements. Yet, it cannot be said that, the Act authorises electronic cheques whereby physical presentment cannot be effected. The study also shows that our criminal law regime lags behind technological development since cyber crimes are not covered. Reference has been made to the Criminal Procedure Act, the Penal Code, the Terrorism Act, the Proceeds of Crimes Act and the Anti-Money Laundering Act.

The Law of Contract Act do not provide for cyber or electronic contracts. This hinders some electronic banking undertakings because electronic contracts do not meet legal requirements as provided by the Law of Contract Act. Therefore, the Tanzania legal framework lags behind technological development as it is inadequately provide protection for the electronic banking transactions.

The author found out that, the main reason as to why up until now there is no specific law regulating electronic banking despite the fact that banks in Tanzania engage in the same to the maximum, is that responsible authorities are of the view tha, over regulation hinders technological development, so it is better to leave the electronic banking self regulated. In disagreement with the reasoning, some law experts asserted that, it is not good at all for electronic banking or e-commerce in general to lack adequate protection of the law. It is better for the basic aspects of it to be regulated by the law even if some aspects remain self regulated. The author agrees with the latter stand for the reason that, it is only from the law, that the legality of anything is driven. Therefore, it is not safe to conduct electronic banking transactions relying only on BoT documents.

Therefore, it is an undeniable fact that lack of adequate legislation regulating electronic banking, poses legal challenges to banks and the electronic banking undertakings.

5 Recommendations

In the line with the observations and findings of this paper, the author is of the view that, it all comes down to one important thing in an alternative with the other. That, the Tanzania legal regime has to change so as to adequately accommodate technological development in electronic banking. The change can be affected by the enactment of a new legislation or by an amendment of the existing laws. The amendment preferred should be made to the following laws; (i) the Banking Acts; new part to be inserted in these Acts which reads Electronic Banking. Under this part following matters to be provided; various electronic

banking products; players in electronic banking to be named, rules of confidentiality in electronic banking different from those applicable to traditional banking; (ii) the Law of Evidence Act; new part to be inserted that reads Electronic Evidence which provides for following matters; admissibility of electronic evidence in both criminal and civil trials, electronic signature, and proof of electronic signatures; (iii) the Law of Contract Act; new part to be inserted that reads Electronic Contracts which provide for; formation of electronic contracts, rules of communication to be different from that of traditional contract, applicability of the privity to contract rule, and legal rights and obligation of the parties; (iv) Bills of Exchange Act; new part to be inserted that reads Electronic Cheques whereby non physical presement is allowed; (v) Penal Code; new part to be inserted that reads Cyber Crimes which provides for the cyber offences and their punishments; and (vi) the Electronic and Postal Communication Act; new part to be inserted that reads Mobile Electronic Fund Transfer where fund transfers through mobile phones are covered.

In the alternative, the enactment of new legislation can also be of merit. New legislation may be only two namely: Electronic Transactions and Electronic Signarures Act and also Cyber Crimes Act. The former is to provide for electronic contracts, electronic banking transactions, and electronic signatures; and the latter to provide for cyber offences.