Legal framework challenges to e-banking in Tanzania

Charles Ishengoma Kato
Legal Department, Tanzanian President's Office: Public Service Remuneration Board, Dar es Salaam, United Republic of Tanzania

Received 22 June 2018
Revised 1 April 2019
Accepted 22 May 2019

Abstract

Purpose – This paper aims to examine the legal challenges to electronic banking and initiatives taken to address them in Tanzania. It is based on the results of a comparative analysis of policies and laws of other countries from which Tanzania can pick a leaf on how to deal with challenges brought by information and communication technology-induced innovations in the banking sector.

Design/methodology/approach – The study upon which this paper is based employed comparative analysis methods by analysing different policies and laws of Tanzania in line with attendant laws of other jurisdictions such as the USA, Malaysia, South Africa, Rwanda and Kenya and international instruments in a bid to establish the best practice pertaining to controlling and containing legal challenges brought by developments in electronic banking.

Findings – This paper confirms that, the prevailing laws guiding electronic banking in Tanzania do not adequately address the challenges the banks and customers face during electronic banking transactions. Thus, there is a need to amend the Tanzanian laws guiding this sector to put in place legislation capable of facilitating the development of electronic banking whilst addressing the associated challenges the users encounter.

Originality/value – This paper underscores the value of amending existing or enacting new laws in line with the development of technology/innovation to protect consumers in nascent electronic banking of the country. Moreover, it advocates for the development of innovation in banking sector should not be left to grow without amending/enacting laws that will promote its development and at the same time protect the users to avoid far-reaching and often unpleasant implications.

Keywords Law, Rule of law, Financial reform and regulation, E-banking legal challenges, Information and communication technology cybercrime

Paper type Research paper

1. Introduction

1.1 Emergence of electronic banking in Tanzania

The banking activities in Tanzania could be traced back to the 1900s Binamungu and Ngwilimi (2006). 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. 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 banks than ones left by the Germans, the British

PSU Research Review
Vol. 3 No. 2, 2019
pp. 101-110
Emerald Publishing Limited
2399-1747
DOI 10.1108/PRR-06-2018-0016

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 nationalisation of all the private banks Binamungu and Ngwilimi (2006).

In the early 1990s, a report on the Inquiry into Monetary and Banking Systems in Tanzania[1] 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)[2] 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[3].

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[4], NMB[5], DCB[6], Exim Bank and NBC[7], for example, confirms the development of electronic banking in the country.

According to the Bank of Tanzania (BoT) – the country's central bank – report (2016), 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 (Ally, 2016). 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.

2. 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 frameworks can address the emerging challenges of electronic banking largely unseen in the established pieces of legislation.

In its report, the BoT (2011) 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 unauthorised transactions and lack of physical infrastructure to support development such as unreliable power supply and

telecommunication. 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 (2005), 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[8], and the Electronic Transaction Act, 2015[9] do not address in detail issues of e-banking. Similarly, the National Payment System, 2015[10] 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.

3. Policy, legal and institutional framework initiatives

3.1 Policy initiatives

3.1.1 National Information Communication Technology Policy, 2016. 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[11].

3.1.2 Tanzania national payment System-Vision and strategies, 2005. In 2005, Tanzania 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[12], the National Payment System Act, 2015[13], and the Electronic Transaction Act, 2015[14]. 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.

3.1.3 Bank of Tanzania Electronic Payment Scheme Guidelines, 2007. Before the BoT Electronic Payment Scheme Guidelines came into force there was no guide regarding the electronic payment system. For quite a long time, all the transactions were performed manually. Similarly, even policies did not guide these recent modes of electronic financial transactions. The revolution of ICT in the financial sector came up with the challenges of data protection, electronic financial crimes such as unauthorised transactions and data destruction.

3.1.4 Outsourcing guidelines for banks and financial institutions, 2008. 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.

Yet, apart from lacking a legal force, these Guidelines fail to cover salient issues such as the scope of activities to be outsourced and how. In fact, the liability of the third party is not clear and there are no stipulated penalties for non-compliance. These guidelines seem to have been made in a hurry without considering all possible scenarios pertaining to the banking business.

3.2 Legislative initiatives

The main laws governing the banking industry in Tanzania are the Bank of Tanzania Act, 2006[15] and the Banking and Financial Institutions Act, 2006[16]. Under the Bank of Tanzania (BoT) Act, 2006[17], the Minister responsible can make necessary or desirable regulations to facilitate the smooth running of the banking business[18]. 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[19].

Other laws which can be used to regulate the banking sector depending on prevailing circumstances include the Foreign Exchange Act[20] which deals with *inter alia* foreign currencies, the Law of Contract Act[21] which regulates contracts, the Land Act[22] when it comes to mortgage, the Company Act[23] for bank registration and Electronic and Postal Communication Act, 2010[24], for electronic communication. However, most of these legislations were enacted basically to regulate paper-based transactions and not those occurring in the online environment. Even when these Acts were enacted during electronic era, they do not go into detail necessary to address issues of electronic banking. A good example is the Electronic and Postal Communication Act, 2010[25].

The following part discusses three legislations, namely the Cybercrimes Act, 2015[26], the Electronic Transactions Act, 2015[27] and the National Payment System, Act, 2015[28]. Moreover, it discusses in detail the provisions of these legislations in relation to e-banking in line with the objectives of the present article.

3.2.1 The Cybercrimes Act, 2015. In 2015, Tanzania enacted the Cybercrimes Act, 2015, 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[29].

The Act also provides procedures for search and seizure[30], liability of service providers[31] and general provisions regarding immunity, forfeiture of property, and offences by a body corporate, compounding of offences and spells out the power of the minister to make Regulations[32].

3.2.2 The Electronic Transaction Act, 2015. The Act recognises electronic transactions and their effects[33]. It also recognises electronic contract[34] and the admissibility of electronic evidence[35]. In fact, this Act also regulates electronic transaction in general.

3.2.3 The National Payment System Act, 2015. As its title implies, the Act aims to regulate and supervise the payment systems, regulate electronic payment instrument, e-money, payment system service providers, validity and enforceability of netting arrangements, finality and the settlement of payment instruction and other related matters.

4. Basic omissions in policies, laws and institutional framework guiding e-banking in Tanzania

Apart from the weaknesses in the current policies, laws and the institutional framework of ICT guiding electronic banking in Tanzania that have been pointed out thus far, there are basic omissions which ought to be addressed to develop even further e-banking while safeguarding the interests of the banks or financial institutions and customers by creating a conducive and safe online banking environment in the country. These following are some of the omissions that need to be addressed discussed below:

To begin with, the BoT Guidelines (2007) do not address at all the issue of liability in the event of risk/loss. For Tanzania, the situation is aggravated because banks are allowed to

unilaterally dictate terms and conditions without consulting their customers and, finally, Bank approval. Consequently, the banks make terms and conditions which absolve them from all liabilities, for example, the terms and conditions of CRDB[36]. In addition, some banks can unilaterally change terms and conditions without informing their customers, for example, terms and conditions of DCB mobile[37] and CRDB[38]. These terms and conditions of banks are unilateral as banks create them with the sole intention of protecting their interest while interests at the expense of those of the customer.

Thus, these banks should be guided in this regard to create fair and impartial terms for both the banks or financial institutions and their customers. In this regard, there is a need to formulate comprehensive policy to guide all the banks and financial institutions countrywide.

Unlike Tanzania, Mauritius Guidelines on Internet Banking, 2001 provides precisely *inter alia* that the contractual arrangements for liability should cover the sharing of risks between the institution and customers[39]. The rationale behind this provision is that customers should not be liable for loss not attributable to or occasioned by them. Including a similar provision in Tanzanian law can add value to the Tanzania BoT Guidelines of 2007.

In similar vein, Malaysia provides a good lesson. In this context, Malaysia's Guidelines on Consumer Protection on Electronic Fund Transfer, 1998 (BNM/GP 11) require the bank or financial institution to enter into contracts with their customers which provide for the sharing of risks. As such, the customers should not be made liable for any loss to which they have not contributed and the same applies to banks or financial institution. Implicitly both parties are protected against the loss caused by the other party.

Second, the BoT Electronic Banking Guidelines of 2007 do not provide damage recovery in e-banking transactions. As result, banks and financial institutions can decide unilaterally on how to pay damages without being guided. Some banks such as the NMB through its terms and conditions state that the bank shall not pay any damage to customers in connection with their account or service[40]. In other countries, guidelines address this issue to avoid such pronouncements that disadvantage customers without due regard.

Whereas the BoT Electronic Banking Guidelines of 2007 do not provide damage recovery in e-banking transaction, the United Nations Commission of International Trade Law (UNCITRAL) Model Law has comprehensively addressed the issue of damages recovery liability both directly and consequentially[41].

During interviews with NBC[42], CRDB, ECO BANK, NMB and Postal Bank customers, many of them complained about the damage recovery in e-banking as a result of the loss incurred by them due unauthorised transactions for which are caused by the banks. Some banks, normally, refund the customers the exact amounts after negotiations upon getting complaints. However, they do not consider compensating the customers for the time and other imbalances occasioned by such e-banking damages. In such cases, the UNCITRAL Model Law can serve as a sample guide in drafting guidelines aimed to address this gap in the Guidelines currently in force in the country's banking sector.

Third, the Acts do not provide the right to countermand as the law is silent on this matter and banks are normally left to decide without any due guidance. This means a customer cannot demand such rights under the Tanzanian law. As the BoT Guidelines (2007) do not provide for this right, the banks deny customers this right by imposing terms and conditions that favour respective financial institutions to the detriment of customer interests and rights. A good example to illustrate this point is the CRDB General Terms and Conditions, which denies customers such a right[43].

Whereas in Tanzania the law does not give the right of countermand, in the US the Electronic Fund Transfer Act, 1978 provides for and guarantees this right[44]. The Act states:

"(a)[. . .]A consumer may stop payment of a pre-authorised electronic fund transaction by notifying the financial institution orally or in writing at any time up to 3 business days before the scheduled date of the electronic fund transaction[...]"

The US Electronic Fund Transfer Act, 1978 defines the term "pre-authorised electronic fund transfer" as an electronic fund transfer transaction authorised in advance to recur at substantially regular intervals[45]. Thus a consumer who arranges with his/her bank a pre-authorised a credit transfer has the right under Electronic Fund Transfer Act (EFTA)[46] to instruct his bank to stop such credit transfer. A bank that fails to act on a consumer's stop payment order is liable for all damages proximately caused by such failure if such a failure was not a result of a bona fide error[47]**.** This includes intentional bank's failure to act upon such stop payment orders. In effect, the bank is still liable for actual damage notwithstanding the maintenance of procedures reasonably adapted to avoid such bona fide failure to stop the payment order[48].

However, the US Electronic Fund Transfer Act, 1978 provides that where a bank completely fails to make a credit transfer, or fails to make a timeout transfer, it is relieved from that liability if such failure was caused by an act of God or other circumstances beyond its control, or by a technical malfunction which was known to the customer at the time he/she attempted to initiate an electronic fund transfer[49].

Clearly, banks are not only liable for their failure to stop a pre-authorised credit transfer, but are also obliged to disclose to their customers in readily understandable language[50]. Their failure to do so exposes them to civil liability, under which a bank is liable to actual damages sustained, statutory damages, and the costs of the successful action together with a reasonable attorney's fee as determined by the court[51].

In the USA, the rules of stop payment in consumer-based transactions as discussed above are not only limited to pre-authorised credit transfer transactions but also extend to pre-authorised debit transfer transactions such as any debit transfer. In such cases, it is the payee who initiates the demand to transfer funds from his debtor's (the payer's) account to his account.

In Rwanda, for example, Regulation No.07/2010 of the National Bank of Rwanda on Electronic Fund Transfers and Electronic Money Transactions provides for that right that state as follows:

The standard terms and conditions to carry out an electronic fund transfer shall include:

c) the customer's right to stop payment of a preauthorized electronic fund transfer and the conditions and procedures to initiate such stop payment order[52].

In Bangladesh, the Regulations on Electronic Fund Transfer, 2014, confer this right[53], and it bears almost similar language as the provision in the Rwanda law that states as follows:

2) the standard terms and conditions to carry out an electronic fund transfer shall include;

c) the customer's right to stop payment of a preauthorized electronic fund transfer and the conditions and procedures to initiate such stop payment instruction.

On the whole, Tanzania can learn from the USA, Rwanda and Bangladesh in this area of law. It is unsafe to leave this matter simply in the hands of the banks without any form of codification. Such codification in law would enable the customer to demand for the right of countermand. As presently, there is no enabling provision, this noble right has been left up for negotiation between the bank and customers in Tanzania, and oftentimes the financial institutions take the liberty of coming up with unilateral terms and conditions to cover such voids. This happens because in most cases the customers are in a weak bargaining position during such negotiations. Thus, it is important for Tanzania to protect the weaker party by instituting robust codification of this right.

Fourth, the study found that liability in the event of erroneous e-banking transaction is common in Tanzania. Like other challenges, the policy and Act do not address this situation.

Issues such as error resolution procedure, bank's liability and customer's liability, acts constituting errors, the investigation of the alleged error, implementation of the investigation results and liability for non-compliance with error resolution procedure do lack satisfactory guidance under the present Acts.

Whereas liability in the event of erroneous and malfunctions in e-banking transaction in Tanzania is not addressed, in the USA, they have been duly addressed under[54]. The customer is required to report the error to the bank or financial institution as soon as he/she discovers the said error or mistake. When the bank or financial institution receives that notification, it has to determine whether there was error committed or not within ten working days. When it finds that there was error committed, it shall be obliged to inform the consumer about that error and correct the same in one business day including paying the interest where applicable. If the consumer has followed all the procedures, the banks may pay that consumer provisional reaccredit pending further investigation into that error within ten working plus interest where applicable. However, the investigation shall not exceed forty-five days from the date when the bank receives a notification of error. If the bank finds no error was committed, it is obliged to inform the consumer accordingly within three business days. Nevertheless, if the court is satisfied that the bank or financial institution did not pay the consumer provisional re-crediting as required, let alone get satisfied that the investigation carried out by the bank was not in good faith, under such circumstances, the bank or financial institution shall pay the consumer treble damages.

To this end, the law is comprehensive as, indeed, it encourages each party to play its respective roles. The bank or financial institution settles the customers' complaints in accordance with the set legal framework, which also stipulates the attendant penalties in case the bank ignores the provisions of the law. The law has set mandatory requirements for the bank or financial institution to operate in good faith. In fact, this is an essential general requirement that embodies all principles of equity and justice which in its present form is also covered. Under this provision, customers are sufficiently and effectively protected.

In comparison, there is significant difference between Tanzania and the US. The law in the US, has addressed this problem by spelling out all procedures under the law but in Tanzania, apart from being aware of this problem as there are many incidents of this nature occurring and recurring, no significant efforts have been made in this area by the authorities. Implicitly, all the rights of the customers are left to be administered by the banks whose commercial instincts are to safeguard their business interests first. Inevitably, the banking customer is at the mercy of the banks in the context of Tanzania.

Fifth, the laws are silent on the problem of double charge imposed by the electronic payment service provider, particularly in mobile payment through cellular phones, whereby sending and receiving money both attract charges. This situation contributes to the increase of costs of mobile money transactions. In Tanzania, there is no enabling provision to prevent double charge so as to enable the customer resort to court to seek their rights and redress. In this regard, Tanzania can learn from Australia Trade Practices (Amendment of Consumer Act) which precisely prohibits multiple pricing[55].

Sixth, the Acts do not protect minors in electronic payment. In practice, the country has evidenced the children making electronic transactions, with no efforts having been made to protect them. In Tanzania, the children are under-18 persons and the law treats them as minors, meaning any contract entered by them is null and void. Though this fact is known to many people in Tanzania and because of the nature of transaction which involves money, it is better for the law to require banks and financial institutions, especially the mobile money operators, to make an enquiry before effecting a transaction to ascertain the age of the customers. It is my considered opinion that there must be special statutory guidance to

protect the minor. In Tanzania, there is a need to protect minors in electronic transactions. In this regard, Tanzania can learn from the Organisation for Economic Co-operation and Development (OECD) on Consumer Policy Guidelines on Mobile and Online Payment, 2014. The Guidelines stipulate[56]:

To enable parents or guardians to monitor and limit children's mobile and online payments for goods and services, businesses, governments and other stakeholders should:

- *Consistent with the guidance contained in section A, issue 1, on "Accessibility and readability of payment-related information", work together to provide parents and guardians, prior to the children's purchase of or access to goods or services that are likely to generate charges incurred by children, with clear, conspicuous and easily accessible information on the costs that may be incurred in acquiring, accessing or using goods and services, and information on how to avoid those costs.*
- *Develop effective mechanisms that enable parents or guardians to ensure that payments initiated by children are subject to their authorisation.*
- *Develop tools which enable parents or guardians to exercise different types of controls over the purchases they authorise their children to make; this would include, for example, tools to prevent children from making purchases without express parental consent or tools that enable parents or guardians to establish ceilings on the amounts that could be charged to an account during defined periods.*
- *Inform parents or guardians about the availability of such tools in a clear and conspicuous manner.*

Seventh, the electronic banking laws particularly the Cybercrimes Act No. 14, 2015 do not have comparable provisions to meet international best practices and, hence, there are not only gaps in the domestic law but also international co-operation can be affected. As the nature of cybercrime in e-banking can be committed across different countries international co-operation is important and necessary to prevent such crime. Accordingly, a specific provision is necessary in this area.

Eight, as for dispute settlement, the serious regulatory concern has to do with the confusion regarding the respective mandates of the TCRA[57] and the BoT in handling disputes over mobile money services. Although the BoT has been vested with the power to regulate financial matters, the terms and conditions of the Mobile Network Operators (MNOs) in jurisdictional and dispute issues direct the matter to the TCRA. This anomaly has created a regulatory confusion between the two entities vested with diverse powers.

7. Conclusion

As observed, limited efforts have been made in Tanzania to overcome the challenges to e-banking including cybercrimes. One of the big problems that ought to be addressed sooner rather than later is avoidance of unnecessary delays in responding to cybercrimes in e-banking. After all, procrastination is the thief of time. Overall, the increasing application of new innovations not only in banking sector but also in other sectors, such applications should go *mutatis mutandis* with the enactment of relevant and pertinent policy and law without leaving loopholes unplugged to protect the users. In this endeavour, Tanzania, as outlined in this paper can learn from the robust and more client-friendly legal provisions in USA, for developed countries, and Rwanda and Bangladesh in the developing world context.

Notes

1. Nyirabu Commission (1988).
2. Information Communication Technology (ICT).

3. Bank of Tanzania (BoT) Report, 2011.
4. Co-operative Rural Development Bank (CRDB).
5. National Microfinance Bank (NMB).
6. Dar es Salaam Commercial Bank (DCB).
7. National Development Bank.
8. Act No.14 of 2015.
9. Act No.13 of 2015.
10. Act No. 4 of 2015.
11. Para. 3.6.1 of the National Information Communication Technology Policy, 2016.
12. Act No.14 of 2015.
13. Act No.4 of 2015.
14. Act No.13 of 2015.
15. Act No.5 of 2006.
16. Act No.5 of 2006.
17. Act No.5 of 2006.
18. Section 70 of the BoT Act, 2006 (Act No.5 of 2006).
19. Section 71 of the Bank and Financial Institution Act, 2006.
20. Cap.27, R.E, 2002.
21. Cap.345, R.E, 2002.
22. Cap.113. R.E, 2002.
23. Cap.212 R.E, 2002.
24. Act No.3 of 2010.
25. Act No.3 of 2010.
26. Act No.14 of 2015.
27. Act No.13 of 2015.
28. Act No.4 of 2015.
29. Sections 4,5,6,7, 8, 9, 10, 11, 12, 15 and 27 of the Cybercrimes Act, 2015.
30. Sections 31-38), of the Cybercrimes Act, 2015.
31. Sections 39-46 of the Cybercrimes Act, 2015.
32. Sections 47-51 of the Cybercrimes Act, 2015.
33. Sections 4-12 of the Electronic Transaction Act, 2015.
34. Sections 21-27 of the Electronic Transaction Act, 2015.
35. Sections 18-20 of the Electronic Transaction Act, 2015.
36. Clause 17.

37. Article 3.0.
38. Clause 15.
39. Paragraph 15 of Mauritius Guidelines on Internet Banking, 2001.
40. NMB Terms and Condition, clause 26 (b) and (c).
41. Articles 5, 14 and 18 of UNCITRAL) Model Law on International Credit Transfer, 1994.
42. National Bank of Commerce (NBC).
43. Clause 17 (i).
44. 15 USC.s.1693 (e) (1978).
45. 15 U.S.C (section 1693 (a) (10).
46. 15 U.S.C (section 1693e (a).
47. 15 U.S.C (section1693(h)(a)(3).
48. 15 U.S.C (section1693 (h) (c).
49. 15 U.S.C. (section.1693 (h) (b) (2) (c).
50. 15 U.S.C (section.1693(c) (a).
51. 15 U.S.C. (section 1693 (h).
52. Article 16 of Regulation No.07/2010 of the National Bank of Rwanda on Electronic Fund Transfers and Electronic Money Transactions.
53. Article 17 (2) (c) of the Bangladesh Regulations on Electronic Fund Transfer, 2014.
54. 15 U.SC (section 1963(f).
55. Section 47 of the Act Australia Trade Practices (Amendment of Consumer Act) No.2 of 2010.
56. Para. E of OECD on Consumer Policy Guidelines on Mobile and Online Payment, 2014.
57. Tanzania Communication Regulatory Authority (TCRA).

References

Ally, A. (2016), "Regulation of mobile money service in tanzania", PhD Thesis, Open University of Tanzania.

Binamungu, S. and Ngwilimi, S. (2006), *Revolution of Banking Business in Tanzania*, 1st ed., Mzumbe Book Project, Morogoro.

Corresponding author
Charles Ishengoma Kato can be contacted at: ckkishengoma@gmail.com