ARE THE CUSTOMERS' RIGHTS PROTECTED AGAINST FRAUD IN MOBILE BANKING IN TANZANIA?

A review of the laws and practice[1]

Caroline A. Mutalemwa & Dr. John A. Ubena***

Abstract

The development of Information and Communication Technology especially digitalization, computerization and Internet has improved the banking sector in various countries including Tanzania. Customers have the potential to perform financial transactions through their Bank Accounts at any-time and anywhere. Despite that, Tanzania currently faces a challenge in the digital or cyber environment which has brought with it several cybercrimes perpetrated by unknown persons such as hackers. These crimes and notorious behaviours extend to the banking sector where unauthorized or fraudulent transactions are performed in the customers' bank accounts without their knowledge and affect their chances of being indemnified for the losses. This article analyzes the law and practices relating to mobile banking customer's rights to privacy and compensation in case of fraudulent mobile banking transactions in Tanzania. The findings have shown that the increase of fraud in mobile banking cases is contributed by ineffective compensation schemes, cumbersome procedures for investigating cybercrimes, and unfair terms and conditions of mobile banking services.

Key words: Mobile banking, fraud, right to compensation and privacy.

1 This article is based on the LL.M research work done by Ms. Caroline Mutalemwa and supervised by Ubena John. See Mutalemwa, C., Protection *of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022.

*LL.M candidate at the Faculty of Law, Mzumbe University. E-mail: carolinemutalemwa2018@gmail.com

**Judge – High Court of Tanzania. E-mail: johnubena@gmail.com

1. Introduction

Currently, Electronic banking[2] is part of the advanced and modern world of money remittance as it involves the exchange of funds in a paperless form between Banks, business entities and customers.[3] Its manifestation is seen to take place in various ways including the use of Automated Teller Machines (ATMs), internet banking and mobile banking all fostered in the field of Information and Communication Technology (ICT). With specificity to mobile banking, the system introduced to the world has simplified performance of financial activities such as cash deposit, cash withdraw and paying bills for customers among other functions.[4] A remarkable essence can be spotted during the outbreak of COVID-19 in Tanzania at the beginning of the year of 2020 where mobile banking and other forms of banking were emphasized or pushed up in order to reduce the congestion in Banks and other financial intermediaries[5] for the sole purpose of limiting the risks of contacting the virus between customers and bank officials. Another importance is that it manages to change the style of doing business[6] by allowing banking customers to perform their financial transactions for 24 hours without going to the bank tellers as normally done in the traditional model of banking.[7]

The history of mobile banking along with other forms of electronic banking can be traced at the time when the western countries such as the United States, introduced the use of message transmitters and clearing houses[8] in banking operations like Master Card Company (MCC), Visa Card Company (VCC) and Society for Worldwide Interbank Financial Telecommunication (SWIFT).[9] These companies allow and promote worldwide payment settlements that favors international customers or travelers. This international influence from western countries pioneered Tanzania to start offering electronic banking services such as payment services through credit, debit and pre-paid cards, internet banking, mobile banking and the use of ATMs in the 1990s[10] for a similar purpose of advancing in the modern world of banking industry.

In the mid-1990s, the Civil Service Department of Tanzania initiated measures with the purpose of transforming a recognized and well-developed field of ICT.[11] In 1999, Tanzania Bankers Clearing House issued paper instrument standards specifying requirements for computer printout of cheques and transactions done at a point of sale. By the year 2000, the Bank of Tanzania (BoT) issued guidelines on the introduction

2 Also referred to as Electronic Fund Transfer (EFT) or E-Finance as according to Mollel, A. and Lukumay, Z., Electronic transaction and law of evidence in Tanzania, Peramiho Printing Press, Songea, 2008, p. 285.

3 *Ibid*, p. 5.

4 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 1.

5 *platforms to shape Africa out of recession*, The East African Daily News, 2020, No. 152, p. 11.

6 Mambi, A., ICT Law Book: A Source Book for Information & Communication Technologies and Cyber-Crime, Mkuki, na Nyota Publishers, Dar es salaam, 2010, p. 120.

7 Mukama, R., *Electronic Banking and Technological Development in Tanzania: A Legal Analysis*, Ruaha Law Review, 2014, Vol.2, No. 2, p. 2.

8 'Online Banking System' <https://www.scribd.com/doc/18028736Online-Banking-System> accessed on 14th October 2020.

9 *Supra note 6,* p. 5.

10 Mollel, A. and Lukumay, Z., Electronic transaction and law of evidence in Tanzania, Peramiho Printing Press, Songea, 2008, p. 5.

11 *Ibid.*

and operation of audible card based electronic money scheme to address on key strategies and operational issues essential for any institution that is dealing with electronic money products.[12] Institutional frameworks like the Bank of Tanzania Electronic Clearing House (BOTECH) in 2000 became legally established and operative, facilitating normal inter-bank electronic debit clearing and it has connectivity with clearing houses in cities such as Mwanza, Mbeya and Arusha.[13]

Policies were also made in 2003 like the National Information and Communications Technologies Policy which carries the vision and mission towards facilitating the application of ICT in improving living standards of Tanzanians.[14] In the same year, Tanzania Inter-bank Settlement System (TISS) was implemented and became operative in 2004 as an online system that facilitates Real Time and Gross Settlement (RTGS) of payment instructions between Banks in Tanzania.[15] This made Banks to become members of the TISS and SWIFT as a way to engage in the process of interbank electronic clearing.[16]

Regulations also came into place for example Anti- Money Laundering (Amendment) Regulations of 2019, Bank of Tanzania (Financial Consumer Protection) Regulations, GN 884 of 2019 and Electronic and Postal Communications (Online Content) Regulations, GN 538 of 2020. They monitor and improve electronic banking transactions by ensuring a safe environment for the protection of its consumers.[17] Over the years, Tanzania has made noteworthy progress in deploying ICT in the banking industry by allowing Banks like CRDB, NMB and NBC to invest significantly in the system through introducing several forms of electronic banking services such as internet and mobile banking.[18]

However, mobile banking has embarked challenges in protection of customers' rights in the aspect of privacy and compensation against fraudulent transactions. For example the enactment of the Banking and Financial Institutions Act of 1991, did not point out anything concerning protection of customers rights in electronic banking services due to the low embracement of the system by most of the financial institutions in the Country even though developed countries like The United States and United Kingdom felt its impacts.[19] In 2011, the BoT Report acknowledged the legal framework in Tanzania guiding the banking sector to be outdated, ineffective and incomprehensive in dealing with the emerging problems like cybercrimes such as fraud and unauthorized transactions in electronic banking services.[20] For example The Cyber Crimes Act[21]

12 Mukama, R., *Electronic Banking and Technological Development in Tanzania: A Legal Analysis*, Ruaha Law Review, 2014, Vol.2, No. 2, p. 6.
13 *Supra note 9*, p. 6.
14 *Ibid.*
15 *Ibid.*
16 Currently Tanzania has a total of 29 Commercial Banks of which about 20 banks are members of TISS and SWIFT.
17 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 4.
18 Abdallah, A., *The Impact of ICT Revolution in Tanzania Legal System: A Critical Analysis of Cybercrimes and Computer Forensic Evidence*. A Thesis submitted to the Open University of Tanzania, 2011, pp. 28-29.
19 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania*, PSU Research Review, 2019, Vol. 3, Issue. 2, p. 102.
20 *Ibid*, p. 105.
21 No. 14 of 2015.

and Electronic Transactions Act[22] do not address in details the issues of electronic banking services, Bank of Tanzania Act[23] and Banking and Financial Institutions Act[24] have given limited coverage on the electronic banking[25] while other Laws are silent on various aspects like allocation of loss in cases of mobile banking fraud.[26]

Reported cases concerning fraudulent are present such as the case of **Vodacom (T) Limited and NMB v. Mwanswa Jonas**[27] where there was a claim for the recovery of pecuniary value (money) lost through a fraudulent transaction exercised in the mobile banking system. The Court held that VODACOM and NMB were severely and jointly liable to pay the respondent though it did not exonerate customers from their duty in taking care of their passwords.

2. Rights of mobile banking customers

Among the rights of customers in the banking sector, they include right to privacy[28] and compensation. In this section only these two rights will be examined. For example, a bank owes the duty of confidentiality to the customer with respect to his bank account. It meaning the bank is legally bound to keep confidential their financial affairs from any publicity except when ordered by the Court or law to do disclosure. In light of the traditional model of banking as reflected in *section 48 (1) of the Banking and Financial Institutions Act*[29]*,* the banks and all financial institutions are required not to divulge information relating to their customers unless the law requires them to do so. This duty forms part of the contractual relationship and breach of it can render to liability on the part of the bank as examined in the case of **Tournier v. National Provincial and Union Bank of England**[30] where Union Bank of England disclosed private financial data of Tournier to his Employer which later on led to his termination in employment. Court held the Bank had a duty of non-disclosure of its customer's account information nor transaction relating thereto.

Regarding the right to compensation, it ought to be granted in the customers' favor who is to be relieved in case of any fraudulent transactions that has occurred via their account.[31] Unless the Bank has proven that it was the customer' negligence in securing his information that allowed third persons to access the bank account, then such right can still be available. [32] The situation is sometimes influenced by banking agreements which limit the banks' liability against losses caused by the customers' own negligence. The mobile banking terms and conditions should have taken cognizance of the right of the customer to enjoy the banking services. The banks are the ones to maintain the banking systems security. It is logical that they should be liable for security

22 No. 13 of 2015.
23 No. 4 of 2006.
24 No. 5 of 2006.
25 Mukama, R., *Electronic Banking and Technological Development in Tanzania: A Legal Analysis*, Ruaha Law Review, 2014, Vol.2, No. 2, pp. 1-2.
26 *Supra note 18.*
27 Consolidated Civil Appeals No. 1 and No. 2 of 2016, High Court of Tanzania at Mbeya (Unreported).
28 Mambi, A., ICT Law Book: A Source Book for Information & Communication Technologies and Cyber-Crime, Mkuki wa Nyota Publishers, Dar es salaam, 2010, p. 123.
29 No. 5 of 2006.
30 [1924] 1 K.B. 461 (COA).
31 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 28.
32 *Ibid.*

breaches unless proved that the customers have divulged or shared their passwords or secret codes with third parties. Assurance must be given to these rights, otherwise it will continue leading to the exposure of customer's bank accounts to fraud risks.

3. Fraud In Mobile Banking

In Tanzania, cybercrimes are fourth ranking prevalent economic form of crimes at the incident rate of 23% and within the financial services it ranks even higher with 45% of consumers being affected by it hence making it the most sufferable crime among others.[33] Being one among the common cybercrimes, fraud is an act of dishonesty performed for the advantage of deliberately securing unfair or unlawful gain which mainly targets on information related to financial data and intellectual property rights products.[34] In the context of mobile money, fraudulent actions are intentional and deliberate actions undertaken by players in the mobile financial services ecosystem aimed at deriving gain or damaging the reputation of stakeholders.[35]

There are various factors that perpetuate for the occurrence of fraud and namely they include password sharing, weak transaction PIN strength and fraud on multiple access channels.[36] This cybercrime can take place in various ways such as network provider data breaching where hackers break into the system of telecom service providers for the purpose of stealing financial information of the subscribers. Secondly, call center fraud which involves fraudsters accessing the accounts of any individual from customer service representatives who perform a couple of checkups in revealing customers' details. Lastly, mobile phone theft which involves stolen mobile phones getting hacked and stored bank information becoming accessed.[37] All these ways allow for easy manipulation of the customers' data as hackers can withdraw funds from different financial accounts.

4. Are the Customers' rights protected against fraudsters in mobile banking in Tanzania?

4.1 Mobile Banking customers protection under International Instruments

4.1.1 The UNCITRAL Model Law on Electronic Commerce, 1996

Its adoption began in 12th June 1996 with additional Article 5 bis as adopted in 1998 which purposively manages electronic commercial transactions by setting out international acceptable rules and principles for the national legislations to implement with the target of removing legal obstacles and increasing legal predictability for electronic commerce.[38] Such acceptable rules include the equal treatment that is quite vital for facilitating the use of

33 PricewaterhouseCoopers, Fraud: the overlooked competitor, Global Economic Crime and Fraud Survey: Tanzania Report, 2018, p. 13.

34 Mambi, A., ICT Law Book: A Source Book for Information & Communication Technologies and Cyber-Crime, Mkuki wa Nyota Publishers, Dar es salaam, 2010, pp. 179 -180.

35 Mudiri, J., *Fraud in mobile Financial Services*, A Paper Published by Micro Save Publication, 2012, p. 14 <https://www.ifc.org/wps/wcm/connect/e6ae6dd9-ad8c-4663-9c38-832c1d46a9fO/Tool+7.1. Risk+Management.pdf?> accessed on 28th June 2021.

36 *Ibid*, 1.

37 Bennet, Coleman & Company Limited, know all about Mobile Banking Fraud and How to Prevent it, 2021 <https://www.timesnownews.com/amp/business-economy/personal-finance/planning-investing/article/know-all-about-mobile-banking-fraud-and-how-to-prevent-it/581110> accessed on 28th June 2021.

38 United Nations, United Nations Commission on International Trade Law, (n.d) <https://www.uncitral.un.org/> accessed on 29th March 2021.

paperless communication and transactions to foster efficiency in international trade.[39] The fundamental principles include non-discrimination, technological neutrality and function equivalence which have recognizance as elements of the modern electronic commerce law.[40]

The principle of non-discrimination ensures that a document is not denied according to its legal effect, validity and enforceability solely on the grounds that it is in electronic form. With the principle of technological neutrality, it mandates the adoption of provisions that are neutral with respect to the technology used and aims at accommodating any future development in the ICT field with further legislative work.[41] Also, by involving the principle of functional equivalence it lays down criteria under which electronic communications may be considered equivalent to paper-based communications.[42] It's other advantage to electronic banking services is addressing the issue of damages recovery liability both directly and consequentially[43] to aid victims of unauthorized electronic transactions. Impliedly, this means that there is no limitation or exoneration of liability of the Banks to their customers against fraud actions in mobile banking.[44]

4.2 Bank customers' protection under domestic laws

39 *Ibid.*
40 *Ibid.*
41 *Ibid.Ibid.*
42 *Ibid.*
43 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania*, PSU Research Review, 2019, Vol. 3, Issue 2.
44 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 31.

4.2.1 The Electronic Transactions Act, No. 6 of 2015

The Electronic Transactions Act, No. 6 of 2015 was enacted to provide the legal recognition of electronic transactions, electronic government services and other related matters.[45] It is also beneficial on the part of admissibility of data message, as provided under *section 18 (1)*, allowing for its acceptance as evidence that can be submitted during legal proceedings. This law has provided for the protection of consumers but it is limited to the one who uses electronic transaction for goods or services for sale, hire or for exchange electronically.[46] For example, *Part VI* covers on protection of consumers who participate in online banking by providing the duties of the suppliers to online consumers, determining the right of customers to cancellation of orders and time for execution of such orders. The setback is that this Act has not covered on protection of customers rights in case of any fraudulent acts that may occur in the form of mobile banking.[47]

4.3 The Cyber Crimes Act, No. 14 of 2015

In 2015, Cybercrimes Bill was introduced and tabled at the Tanzania government with the aim of protecting citizens against cybercrimes.[48] After its declaration a

45 See the long title of the Electronic Transactions Act, No. 6 of 2015.
46 Kangole, E., *Consumer Protection on Mobile Banking Transactions in Tanzania: A Critical Analysis of the Law*, a Dissertation submitted for the Award of Master's Degree of Laws (Commercial Law) of Mzumbe University, 2016, p. 44.
47 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 32
48 Breakthrough Attorneys, Cyber Crimes Act 2015 Tanzania: The Challenge in the Hands of both Corporates and Individuals, 2015, <https://breakthroughattorneys.co.tz/cybercrimes-act-

legislation, it has prescribed cybercrimes and their attendant punishments including those committed via computer system and information technology.[49] A good example included illegal system interference under *section 9*, computer related fraud under *section 12* and conspiracy to commit offence under *section 27*. It has also managed to confer jurisdiction to convict any Tanzanian citizen within or outside the country and even foreigners within or outside the country if the crime is against a person located in Tanzania as reflected under *section 30*.

This legislation is influenced with various challenges such as creating room for abuse of power by the Law Enforcement Officers upon the issue of an order for the disclosure of one's data as per *section 32* that is contrary to the right of data privacy.[50] Second, The Act shares the same condition with The Electronic Transaction Act[51] as they all do not address some issues of electronic banking services such as mobile banking[52] like liability of Banks in fraudulent transactions and recognition of crimes conducted from Bank Accounts through mobile phones[53]. Lastly, it does not have comparable provisions in line with the international best practices like fair and equitable treatment, as provided under the UNCITRAL Model Law on Electronic Commerce of 1996.[54]

2015-tanzania/> accessed on 27th March 2021.

49 *Ibid.*

50 Breakthrough Attorneys, Cyber Crimes Act 2015 Tanzania: The Challenge in the Hands of both Corporates and Individuals, 2015, <https://breakthroughattorneys.co.tz/cybercrimes-act-2015-tanzania/> accessed on 27th March 2021.

51 No. 6 of 2015.

52 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania*, PSU Research Review, 2019, Vol. 3, Issue 2, p. 104.

53 Kangole, E., *Consumer Protection on Mobile Banking Transactions in Tanzania: A Critical Analysis of the Law*, a Dissertation submitted for the Award of Master's Degree of Laws (Commercial Law) of Mzumbe University, 2016, p. 40.

54 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 33.

55 Kasanda, P. and Marandu, M., Tanzania: The National Payment System, 2016, <https://www.mondaq.com/financial-services/498230/the-national-payment-system> accessed on 27th March 2021.

56 *ibid.*

4.4 The National Payment Systems Act, No. 4 of 2015

In 2015, this Act came into place requiring banks and financial institutions to comply with the legislation on matters of applying for prescribed licenses and seeking approval where applicable within six months.[55] The Act also aims at regulating and supervising the payment systems, electronic payment instrument and payment system service providers.[56] According to *section 47* it determines the right of privacy to be maintained by the payment system providers who shall protect the privacy of a participant, customer information and not disclose such information unless so complied by the law. In contrary to this, liability will be imposed to the payment system providers for fine payment of not less than a hundred million shillings. Under *section 51* it provides for consumer protection requirements relevant to payment system services which are to be given by the BoT. Such requirements include transparent and fair terms and conditions, complaints handling and dispute resolution mechanisms and full disclosure of relevant information for the use of electronic payments services that are all to be given to the consumer. Also, *section 53* recognizes the cyber-crimes in the payment systems like hacking as an offence liable to a conviction of a fine of ten million shillings or three times the value of the property.

When it comes to covering the liability on the part of the Banks in mobile banking transactions, this law seems to be silent. Under *section 55* it gives immunity to any officer or employee of the bank against actions or proceedings in respect of exercising their powers in good faith. This acts as a way to exonerate their liability in fraudulent transactions especially where the Bank system has allowed for the performance of a financial transaction in a customer's account without their full authorization and verification.[57] Secondly, a customer is provided with complaints handling and dispute resolution mechanisms in respect to *section 51* but what are these mechanisms and what would be the solution in case of any dissatisfactions for customers with the way their claims were handled? Specificity of the law is vital to flooding away ambiguities in interpreting the provisions, something of which has not been displayed under this respective provision of the National Payment System Act.[58]

4.5 The Bank of Tanzania (Financial Consumer Protection) Regulations, GN. 884 of 2019

These regulations were made under *section 70 (1)* of the Bank of Tanzania Act[59] and according to *regulation 2* it applies to all financial service providers operating in mainland Tanzania and Tanzania Zanzibar unless prescribed otherwise by the bank in other regulations. These regulations require the governance of financial consumers' protection[60] and sheds responsibilities on the Board of Directors and senior management of operating banks and financial service providers[61]. Under *regulation 35 - 39* it provides for the protection of consumer's information and this is to ensure the appropriate security and control mechanisms to safeguard privacy of consumer's financial information against fraudulent practices and other possible misuse.

The setback of this law is that, it does not state that banking contracts which contain terms that limit or exclude liability of banks in fraudulent transactions, to be unfair.[62] In respect to *regulation 16 (2)* it allows for banks to limit their liability through contractual terms of bank services which is unfair. The regulation does not mention circumstance where the terms that limit the liability of financial service provider in fraud cases to be significantly imbalanced which creates open doors for Banks to use their limitation clauses in electronic banking contracts in avoiding any responsibility of compensating a customer so affected by the crime.[63] Secondly, it does not point out the liabilities of the BoT in cases of fraudulent transactions in mobile banking because it does not consider it to be a financial service provider as per *regulation 3*. The Bank of Tanzania should form part of being accountable in such matters as it is their duty to ensure the banking systems or services

57 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 35.

58 *Ibid.*

59 No. 4 of 2006.

60 *See Part II of these Regulations.*

61 *See regulation 5 and 6.*

62 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 39.

63 *Ibid.*

so offered to the customers are at their advantage and not constantly vulnerable to electronic crimes like fraud which greatly affects their customers.

4.6 The Payment Systems (Electronic Money) Regulations of 2015

These Regulations were made under *section 56 (1) and (2) (c) of the National Payment Systems Act*.[64] It has managed to impose some duties to the Banks as electronic money issuers. Under *Regulation 32*, it provides for the risk management by electronic money issuer who has been given various obligations such as preparing and implementing risk mitigation plans, comply with the risk management requirements and set up safeguard measures to protect funds from risks that may occasion loss to beneficiaries. Upon *regulation 45* it provides for consumer redress plan to be established by the payment system provider. Sub *regulation (2)* lays down the procedures to follow in handling consumer complaints but the last step seems to be unfair as the Bank is given the opportunity to file an unresolved compliant to the Bank of Tanzania, Fair Competition Commission or Tanzania Communication Regulatory Authority and not the consumer. Most complaints would be solved by referring to the terms and conditions of Banks which exempt them from liability leaving the consumers without privilege to seek for further help.[65]

64 (No. 4 of 2015).

65 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 40.

5. Analysis of the law and practice on protection of customers rights in mobile banking

5.1 Legal coverage of essential matters in mobile banking

Some important and essential issues have not been addressed under the Tanzania laws like damage recovery for the customers in mobile banking. Legislations like the Electronic Transactions Act[66] which has legally recognized electronic transactions in the country, does not provide for damage recovery in case one is affected by such electronic transactions in events of fraud. Other laws include the Cyber Crimes Act[67] have not given a clear environment when it comes to determining liabilities in event of risk loss in electronic fraud. Even though the bank-customer relationship by nature is contractual in nature but such liability of these financial institutions not being expressly provided by the law can act as a chance to deny their accountability in any complaint that a customer may bring before them. This implies that, banks are excluded from any burden of paying for the losses that their customers would encounter.[68]

In addition, The Tanzania laws are quite slow in protecting customers in mobile banking services as they have not incorporated tools of effecting electronic transactions. Even some national guidelines like the Electronic Payment Scheme Guidelines of 2007 do not cover on the important aspects such as remedies to customers in cases of

66 No. 6 of 2015.

67 No. 14 of 2015.

68 *Supra note 64*, p. 43.

mobile banking fraud but instead cover risk management for Banks and other financial institutions.[69] It is of no doubt that mobile banking offences such as hacking, cyber-vandalism and spoofing keep on taking place. Most of the existing laws facilitate paper-based transactions, which apparently are not applicable to the technological changes in the banking sector. It is claimed that in observing some of laws such as the Banking and Financial Institutions Act the features are not in tune with the electronic commerce development[70] and such poor legislation and law enforcement creates incentives for misuse (hackers) to intensify their fraudulent activities[71] in association with jeopardizing the security of the consumers[72].

Even in other jurisdictions like Zimbabwe, various laws such as the Bank Use Promotion and Suppression of Money Laundering Act[73], Prevention of Corruption Act[74] and Money Laundering and Proceeds of Crime Act[75] were introduced to purposely guard the system against financial crisis by any impudent practices, curb corruption. These legislations still remain silent in covering up on use of technologies measures like Artificial Intelligence and machine learning to curb bank fraud and other financial crimes[76] that entails how their legal framework has not exhaustively associated the key aspects in securing their banking system including mobile banking.

5.2 Stability of the security system

Cyber security has been a recent concern rated to be the most important issue as it is a dual requirement to protect customers' privacy and protect their Accounts against fraud.[77] The cyber-crimes associated in banking services are mostly referred to as organized crime syndicates which are threats posed in financial or personally identifiable information.[78] Other East African countries for instance, in Uganda have experienced cyber-attacks on their Banks that has led to the temporary suspension of electronic banking services like mobile banking as a result of the loss of over 11.9 billion Ugandan Shillings from Customers' Bank Accounts.[79]

In most cases, banks claim their banking security system to be perfect and such common line of reasoning is not to be relied upon.[80] Recently, outsiders retrieve pass codes of the customers' accounts without negligence of the customers making them available[81] by breaking through the

69 Castri, S. and Gidvani, L., Enabling Mobile Money Polices in Tanzania: A "test and learn" approach to enabling market-led digital financial services, 2014, p. 6.

70 Mambi, A., ICT Law Book: A Source Book for Information & Communication Technologies and Cyber-Crime, Mkuki wa Nyota Publishers, Dar es salaam, 2010, p. 130.

71 *Ibid*, p. 179.

72 Viswanadham, N. & Alexander, M., *Assessment of Legal Challenges Relating to E- Banking in Financial Institutions,* International Journal of Finance and Banking Research, 2019, Vol. 5, No. 3, p. 50.

73 [Chapter 24:24] 2 of 2004.

74 [Chapter 9:16] 27 of 2004.

75 [Chapter 9:24] 4 of 2013.

76 Chitimira, H. & Ncube, M., *Towards Ingenious Technology and the Robust Enforcement of Financial Markets Laws to Curb Money Laundering in Zimbabwe,* Pioneer in Peer Reviewed Journal, 2021, Vol. 24, pp. 10-13. https://perjournal.co.za/article/view/10729

77 *Supra note 71*, p. 49.

78 PricewaterhouseCoopers, Fraud: the overlooked competitor, Global Economic Crime and Fraud Survey: Tanzania Report, 2018, p. 13.

79 The East African Daily News, Ugandan Banks face Cyberattacks every 39 seconds, *The East African Daily News*, 2020, No. 152, p. 16.

80 Mason, S., *Debit Cards, ATMs and Negligence of the Bank and customer,* Butterworths Journal of International Banking and Financial Law, 2012, p. 23.

81 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 54.

banking security system in many ways.[82] For example, the backdoor attack involves exploiting alternative methods of accessing a system that does not require the usual means of authentication. Secondly, the denial-of-service attack prevents the rightful users from accessing the system as thieves wrongfully enter a password numerously that lock a person's account. Lastly, the direct-access attack includes bugs and viruses which gain access to a system and copy its information or modify it.[83]

In legal aspects, The Tanzanian Laws do not create room for a good security system. Legislations such as the Cyber Crimes Act[84] allows police officers in police stations to issue an order to any person in possession of data that is related to a criminal investigation to disclose it. This may be done in violation to the constitutional right to privacy[85] and may subject such information to cyber-crimes related to fraudulent transactions. The power so provided to these Police Officers allows them to retrieve personal financial information from a banking customer meaning data such as pass codes are exposed to an outsider and it may not guarantee strong protection of one's account.[86] Sometimes, when there are no reliable internet services as a result of the poor network connection, it may affect the security system because it gives a chance to cyber-crimes to take place. Services that are affected by a poor network connection include mobile bank transaction and even using Automated Teller Machine (ATM). This leads to insecurities on the part of the customers meaning they will lack confidence as personal information will be known to third parties.[87]

5.3 Unilateral terms in mobile banking agreements

The relationship between the bank and customer is mostly determined to be contractual in nature whether involving the traditional or new model of banking.[88] Protection of the rights of these customers also depends on the terms and conditions so concluded between the Banks and its customers. They are standard form and one-sided favorable especially on the Bank. These agreements are influenced with terms and conditions that deny any payment for damages in connection with the customer's account.[89] For example, under the DTB Electronic Banking Services Agreement on Mobile and Internet Banking, Clause 10.1.7 provides that;

The Bank shall not be responsible or liable for any damages or losses arising from

82 *Supra note 79*, p. 17.

83 Chen, J., Mobile banking, 2020, <https://www.investopedia.com/terms/m/mobile-banking.asp> accessed on 2nd May 2021.

84 No. 14 of 2015.

85 The UN Declaration of Human Rights (especially Article 12 on right to privacy) https://www.un.org/en/universal-declaration-human-rights/ last visited on 24 May 2022; Article 16 of the United Republic of Tanzania Constitution 1977 as amended provides for right to privacy. Breakthrough Attorneys, Cyber Crimes Act 2015 Tanzania: The Challenge in the Hands of both Corporates and Individuals, 2015, <https://breakthroughattorneys.co.tz/cybercrimes-act-2015-tanzania/> accessed on 27th March 2021; see also Ubena John, Privacy-a forgotten right in Tanzania, Tanzania Lawyer, 1/2]TLS, 2012, pp.72-114; Samuel Warren & Louis Brandeis, The Right to Privacy, 4 Harvard Law Review, (1890)193-220; for case law see Jebra Kambole v The Attorney General [2017] TLS LR 322; Jamii Media Company Ltd v. AG and Another [2017] TLS LR 447.

86 *Supra note 80*, p. 55.

87 Viswanadham, N. and Alexander, M., *Assessment of Legal Challenges Relating to E- Banking in Financial Institutions,* International Journal of Finance and Banking Research, 2019, Vol. 5, No. 3, p. 53.

88 Onwudiwe, C., Legal Aspects of Electronic Banking in Nigeria: An Overview, 2017, <https://eprints.covenantuniversity.edu.ng/10272/1/Legal%20Aspects%20of%20Electronic%20Banking%202017%201.pdf> accessed on 15th March 2021.

89 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania*, PSU Research Review, 2019, Vol. 3, Issue 2, p. 105.

unauthorized access to any Electronic Banking Service by a third party using the customer's Password, PIN and/or log-in Information, unless prior notification from the customer has been received by the Bank stating that no further access to the relevant Service shall be granted to any person using such PIN and/or login-in Information which notification shall have effect either from the date receipt of such notification or such later date as may be specified in such notification

From the above clause, it excludes the bank's liability in matters of fraud that may occur to their accounts. This means, it will be the customer's duty to keep the Bank indemnified against such transactions as provided under Clause 11.3.3 of the same Agreement. Mobile banking customers greatly face problems from these terms such as not getting compensated when a third party illegally and electronically steals money from their Accounts even if it was not by their negligence. It is quite clear that Banks do not want to bear the entire loss from the transactions as to why they pin it to be a customer's fault. [90] However, in order to so, there must be proof of such negligence on the customer directly implying that the burden of proving carelessness of a customer lies on the Bank[91] in case the matter has been taken to Court. The Bank could use identification or recognition evidence to prove through Surveillance Cameras[92] that provides images of a known person to a customer performing an ATM transaction authorized by account holder who provided his or her bank card along with the PIN. Even testimony and hearsay evidence[93] is applicable as long as they relate to proving the fault of the customer that attributed to the fraudulent transaction to take place.

The constant denial of their liability by reference to the Bank agreements has caused many complaints on the damage recovery in electronic banking services stipulated by losses incurred due to unauthorized transactions.[94] That is why Courts have to interfere to safeguard the rights of these users as reflected in the case of **Ecobank Tanzania Limited v. Future Trading Company Limited**[95]**.** In the case**,** Galeba, J A stated that, a banker is a trustee to the customer because it has massive control over the depositor's funds and unfettered prerogative to use the money without consulting its owner *vis a vis* no powers remain to the customer. It was finally held that, a bank has the burden to prove it was not at fault in the disappearance of a customer's funds because it is the sole custodian of the money.

5.4 Long duration and cumbersome procedures in handling cybercrimes

One among the practical issues concerning protection of customers' rights against mobile banking fraud is the dispute mechanism. [96] In handling disputes in mobile

90 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, pp. 57-58.

91 Bank Frauds- who is responsible?, (n.d) <https://www.news18.com/amp/topics/bank-fraud> accessed on 16th September 2021.

92 Seng, D. and Mason, S., Electronic Evidence, 4th ed, Institute of Advanced Legal Studies at the University of London, London, 2017, p. 61.

93 *Ibid*, p. 39.

94 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania*, PSU Research Review, 2019, Vol. 3, Issue 2, p. 105.

95 Civil Appeal No. 82 of 2019, Court of Appeal of Tanzania at Dar-es-salaam, (Unreported).

96 Mutalemwa, C., *Protection of Customers' Rights Against*

banking, it is more of tiresome job for the complainants. Under *regulation 53 (2) of the Bank of Tanzania (Consumer Protection) Regulations of 2019*, the BoT must determine a complaint that has been filed before it from the financial service provider, for a period of 30 days as specified under the fourth schedule of the Regulations. Depending on the nature of such cases, they should not take such long time in determining rights of the customers as it amounts to unnecessary delays which can discourage customers from making follow-ups and loose hope in ever been relieved from the continuous cyber-attacks in their financial accounts.

5.5 Customers' ignorance of mobile banking systems, regulation, terms, and conditions of services

First and foremost, most people are less aware on how their rights can be violated by the mischievous behaviors of cyber hackers or fraudsters. The measures taken in this aspect are not similar like the ordinary precautions of preventing bank cards from being stolen[97] as cyber-crimes in the digital era work slightly different. For instance, a criminal can simply use a direct-access attack that includes bugs and viruses which gain access to a system and copy its information or modify it.[98] Sometimes, by the negligence of customer they can simply give away their PIN Codes to people who make their accounts vulnerable to any future fraudulent action. A customer may think that, the Bank performed the unauthorized transaction but rather it was the mind and efforts of another. In addition, their rights can also be violated by the terms and conditions of the mobile banking agreements which limit the liability of the Banks that a lot of people are unaware of such unfair clauses.[99]

The customers' unawareness on the legal implication of mobile banking is in turn also big challenge.[100] Under *regulation 19 (3) (a) of the Bank of Tanzania (Financial Consumer Protection) Regulations of 2019,* banks are allowed to develop financial education programs that deal with public awareness campaigns in self-protection against fraud and also highlight the public on the Legal instruments in matters of mobile banking. While conducting the study, questionnaires were issued to five (5) Bankers (CRDB, DTB, KCB and EXIM), there was no response about conducting these programmes.[101] This indicates the likelihood that, some users of mobile banking are less aware of the nature of the system especially on its vulnerability. It was further found out that, the ignorance of customers on how to deal with cybercrimes and how to pursue their rights drives them away from getting legal protection they deserve. This also

Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania, a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 50.

97 Mason, S., *Debit Cards, ATMs and Negligence of the Bank and customer,* Butterworths Journal of International Banking and Financial Law, 2012, p. 2.

98 Chen, J., Mobile banking, 2020, <https://www.investopedia.com/terms/m/mobile-banking.asp> accessed on 2nd May 2021.

99 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 61.

100 Viswanadham, N. and Alexander, M., *Assessment of Legal Challenges Relating to E- Banking in Financial Institutions,* International Journal of Finance and Banking Research, 2019, Vol. 5, No. 3, p. 48.

101 Questionnaires were issued to Bankers in Mwanza where the study was conducted and such responses were received on. See Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, pp. 61-62.

explain their low use of mobile banking due to fear of becoming victim of fraud and not knowing the remedies. Such lack of knowledge of the users has adversely influenced the adoption of this electronic mode of banking in Tanzania.[102]

5.6 Linkage of Tanzania legal framework with International Standards

The International Instruments, specifically the UNCITRAL Model Law on Electronic Commerce of 1996 was the first legislative text to set forth international standards like fundamental principles of non-discrimination, technological neutrality and function equivalence that have been widely recognized as elements of the modern electronic commerce law.[103] Since Mobile Banking is derived from electronic commerce then, these elements apply simultaneously.

Some of the Tanzania national laws do not have an interconnection with the international best practices in banking business. For example, the Cyber-Crimes Act[104] does not have any provisions which provide or cover the international best practices especially on technological neutrality and functional equivalence. It shows a non-adoption and non-compliance with these international elements that each country must have in their laws since The UNCITRAL Model Law on Electronic Commerce of 1996 acts as a guide for other states to use in forming their laws on electronic banking services. At the same time, it shows non reliance by citizens to such National law in favoring the interests of the banking customers as it fails to hold the important principles that could help in protecting the rights in mobile banking. Though some Legislations like The Bank of Tanzania (Financial Consumer Protection) Regulations of 2019 have managed to reflect on some of the international standards, this should be the case for all the laws regulating mobile banking in the country.[105]

5.1 Increase in number of internet users

It was once reported in 2012 that internet users have risen to 5.63 million users in Tanzania and the trend increases at the rate of 416.98% yearly.[106] Such an increase implies to the increasing opportunity of cybercrimes for users who could simply enrich themselves by manipulating the cyber security system of Banks and illegal transfer money from banking customers' Accounts. Some of these fraudsters are considered to be from the internal and external sources including persons such as bank employees and contractor.[107]

6.0 Conclusion and suggestions for improvement

The impact of mobile banking in Tanzania has open up for fraudulent transactions

102 Rumanyika, J., *Obstacles towards adoption of mobile banking in Tanzania: A review*, International Journal of Information Technology and Business Management, 2015, Vol. 35, No. 1, pp. 1 and 13.

103 United Nations, United Nations Commission on International Trade Law, (n.d), <https://www.uncitral.un.org/> accessed on 29th March 2021.

104 No. 14 of 2015.

105 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 62.

106 Mshangi, M., et al. *The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania?*, International Journal of Information Security Science, Vol. 3, Issue 2, p. 4.

107 Sanusi, Z., et al, Fraud schemes in the Banking Institutions: Prevention measures to avoid severe financial loss, 7th International Conference on Financial Criminology, 2015, p. 1.

to easily take place leaving the customers of the services troubled with no surety in safe guarding of their right to privacy and claiming their right to compensation. It is noteworthy that, ICT has made a tremendous impact in banking services as *"anywhere, anytime banking"* has become a reality[108] but the services are rigged with complexities and difficulties in view of the fact that the risks of the modern technology are unforeseeable and some are unavoidable.[109] Though, Tanzania has managed to make some efforts in the recent years to properly regulate mobile banking yet the system is still in vain. Even with the laws available, controlling the risks in mobile banking has become an everlasting process.[110] Inevitably, the banking customers in the context of Tanzania are left at the mercy of the Banks[111] which continuously deny their duties and liabilities in matters of fraud with the aid of the unilateral agreements, that customers are affected by even when they try to prove their non-negligence.

6.1 Suggestions for improvement

Once, his Lordship Nsekela gave an obiter dictum in the case of *Trust Bank (T) Limited v. Le-Marsh Enterprises Limited and Two others*[112] that, the law must be kept abreast of technological changes as they affect the way of doing business. This view is relevant even in mobile banking services. In lieu of what has been discussed herein above, the Tanzania legislature should amend several laws and align them with the rights mobile banking customers. Some of these laws are the Cyber Crimes Act and National Payments System Act which ought to cover clearly and transparently issues of liability of banks in fraudulent cases in line with the International Standards of electronic banking services. Regulations also require some modification like the Payment Systems (Licensing and Approval) Regulations of 2015 which indicate a need to provide remedy or redress plan for customers who are victims of mobile banking fraud.

Firstly, having a legal framework that addresses associated challenges in mobile banking is a good way to build a safe digital environment to protect users' interests. Secondly, having an improved legal framework will help Tanzania to keep up with the global digital economy in combating cybercrimes. This is widely acknowledged in the facilitation of international trade and investment and as a nation in solving various risks in electronic commerce.[113] Thirdly, the legal framework will show consistency with the UNCITRAL Model Law on Electronic Commerce of 1996 as an international instrument to assist states in reforming and enhancing their legislations. Including the UNCITRAL international standards in the Tanzanian laws of mobile banking will ensure uniformity, a regulatory approach

108 Viswanadham, N. and Alexander, M., *Assessment of Legal Challenges Relating to E- Banking in Financial Institutions*, International Journal of Finance and Banking Research, 2019, Vol. 5, No. 3, p. 53.

109 Onwudiwe, C., Legal Aspects of Electronic Banking in Nigeria: An Overview, 2017, <https://eprints.covenantuniversity.edu.ng/10272/1/Legal%20Aspects%20of%20Electronic%20Banking%202017%201.pdf> accessed on 15th March 2021.

110 Mukama, R., *Electronic Banking and Technological Development in Tanzania: A Legal Analysis*, Ruaha Law Review, 2014, Vol. 2, No. 2, p. 9.

111 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania*, PSU Research Review, 2019, Vol. 3, Issue 2, p. 108.

112 [2002] TLR 144.

113 United Nations, United Nations Commission on International Trade Law, (n.d), <https://www.uncitral.un.org/> accessed on 30th March 2021.

in improving the governance of electronic commerce.[114]Also, the framework shows international cooperation in combating cyber-crimes in electronic banking that is a cross cutting issue.[115] Lastly, it will act as a better approach in handling the matter rather than depending on judiciary, whose interpretation alone is not enough to facilitate electronic banking transactions.[116]

6.1.1 Improvement of mobile banking security system

Firstly, and foremost, the development and implementation of adequate security policies and measures for Banks like encryption, passwords, and firewall, and for communication between the bank and external parties would be an aid towards stabilizing the security used in mobile banking services. Second, Banks need to consider having digital signatures as a precautionary measure to prevent malpractices with electronic information. Third, focusing on multi-player protection approach is the best alternative for system security because it includes shielding the authentication process from malicious activities and providing user-to-site authentication strategies.[117] Fourth, detecting thieves or sending a notification to the customer, via messaging alert on a particular transaction requested or about to be done. This is part of the 'Know Your Consumer/Customer' (KYC) protocols employed to identify and verify a customer prior to making an engagement with them and successfully avert or detect fraud.[118] With these measures, data would not be subjected to misuse by third or unknown persons, customers' fund would be secured from illegal transfers and customers would be won back for the favor of the banks in mobile banking service.[119] It is the duty of the Banks to guarantee safety of its' business or services[120] so as to ensure a trustworthy banking environment that will build a better lasting relationship with their clients.[121]

6.1.2 Fair terms and conditions of mobile banking services

The terms and conditions of banking agreements must be favorable to both parties and most especially the customers. The mobile banking agreements should provide for accountability of Banks and Financial Institutions in fraud cases especially where there is no absolute proof on the negligence of the customers in securing their PIN Codes.[122]

114 Bwana, J., *Governance Challenges Facing Regulation of Electronic Commerce in Least Developed Countries with Reference to Tanzania,* a Dissertation submitted in partial fulfillment of the requirements for the Degree of Masters of Laws at the University of Warwick, 2002, p. 57.

115 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania,* PSU Research Review, 2019, Vol. 3, Issue 2, p. 108.

116 Mukama, R., *Electronic Banking and Technological Development in Tanzania: A Legal Analysis,* Ruaha Law Review, 2014, Vol. 2, No. 2, p. 9.

117 Viswanadham, N. and Alexander, M., *Assessment of Legal Challenges Relating to E- Banking in Financial Institutions*, International Journal of Finance and Banking Research, 2019, Vol. 5, No. 3, p. 49.

118 PricewaterhouseCoopers, Fraud: the overlooked competitor, Global Economic Crime and Fraud Survey: Tanzania Report, 2018, p. 18.

119 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, pp. 66-67.

120 Mason, S., *Electronic Banking and how Courts approach the evidence,* Computer Law and Security Review 144, 2013, p. 12.

121 Lugano, L., *The Impact of Electronic Banking on Operational Performance of Commercial Banks in Dar-es-Salaam – Tanzania: A Case of Commercial Banks in Dar-es-Salaam Region – Tanzania*, a Dissertation submitted for the partial fulfllment of the Degree in Master of Business Administration (MBA-CM) of Mzumbe University, Morogoro of Tanzania, 2016, p. 19.

122 It is a trite principle in the law of evidence that he who alleges must prove (see Section 110 of the Evidence Act [Cap 6 R.E. 2019]). Disputes involving banking transactions provide for the onus to the Banks in proving that they acted within their mandates and any financial transaction at dispute was authorized by the Account Holder. See Mason, S., *Electronic Banking and how Courts approach the evidence,* Computer Law and Security Review 144, 2013, p. 3.

Recognition of the rights of customers should be embraced which will act as a sign of the responsibility that the Banks takes in case cyber hackers manipulate financial accounts in the face of their customers. It will also show banks efforts in securing the rights of customers especially the right to compensation. After all, it is their duty to do so since they are ones who offer the system to the customers.[123]

6.1.3 Benchmarking legal frameworks from other jurisdictions

Benchmarking is one way of learning protection of rights of mobile banking customers best practices from other jurisdictions. For instance, the Mauritius Guidelines on Consumer Protection on Electronic Fund Transfer[124] requires the Bank or financial institution to enter contracts with their customers which provide for the sharing of risks. This makes customers to not be solely liable or at all for any loss they did not contribute to and with such guidelines, they deny privilege of Banks or any financial institutions to escape accountability by simply refereeing to their standard form contracts. Considerations can also be placed in England and Wales where most of judges have reached decisions in determining negligence of a customer in this aspect by proof of the PIN in a customer's account being carelessly kept like in written notes[125] otherwise financial institutions cannot swiftly deny their liabilities. The Government could formulate new laws that would be in line with the objects of various foreign laws in the field of mobile banking. In addition, Tanzania can employ the advanced methods of machine learning and Artificial Intelligence in combating with bank fraud used by Singapore, Italy and United States[126] as part of bench marking with other states by viewing it's their strength and weaknesses. This would help in adapting new strategies or plans to improve their ways of securing rights against mobile banking fraud.[127]

6.1.4 Reduction of red tapes

There should be a change in the way and time interval of handling matters of mobile banking fraud for complainants. The findings for this study established that, procedures to be followed in solving cases of mobile banking fraud are cumbersome. For example, according to the Head of Cyber Crime Unit at the Central Police Station in Mwanza the procedures include customers reporting to the Police Station, investigators being appointed and waiting for cooperation from bodies like TCRA, Banks and Mobile Network Companies of which consume a lot of time for them to respond back.[128] EXIM Bank staff also elaborated their procedures which include customers reporting their claims at the offices, sending such claims

123 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 67.

124 1998 (BNM/GP 11).

125 Mason, S., *Debit Cards, ATMs and Negligence of the Bank and customer,* Butterworths Journal of International Banking and Financial Law, 2012, p. 7.

126 Chitimira, H. & Ncube, M., *Towards Ingenious Technology and the Robust Enforcement of Financial Markets Laws to Curb Money Laundering in Zimbabwe,* Pioneer in Peer Reviewed Journal, 2021, Vol. 24, pp. 21 and 22 https://perjournal.co.za/article/view/10729

127 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, pp. 67-68.

128 Questionnaires were issued to the Head of Cyber Crime Unit at the Central Police Station in Mwanza where the study was conducted, and such responses were received. See, Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, pp. 52.

to the Head Quarters in Dar-es-Salaam and that matter will be handled in 40 days upon its receipt. KCB Bank officer further stated that the procedures of handling fraud cases included communicating with the mobile network operators to retrieve information on the claims, advising a client to file a compensation form and wait for confirmation from the Head Quarters, for an uncertain number of days to allow the customer to proceed with the claim process for his or her compensation. [129]

When such steps to follow are many and time consuming, they tend to make customers unable to continue seeking for their respective rights. The procedures need to be convenient, in order to make it easier for the customers to claim for their rights without bottlenecks.

6.1.5 Creation of effective and customer supportive policies

Fraud is not only a product of the poor regulation by the Laws but also by the financial regulators who need to take various action in managing the cyber environment.[130] The Central Bank (BoT), as a financial regulator, should create policies which must be in line with the essential elements in mobile banking for example, fair and reasonable compensation with the main objective of establishing a system of relieving their customers for any direct financial loss that might have been incurred due to the deficiency in the services offered by the bank or commission solely or directly attributable to the bank.

These policies need not be with harsh conditions when it comes to compensating the vulnerable party who has faced cyber-attacks.[131] Apart from compensation policies, the BoT can implement electronic banking policies that allow for proper management and regulation of such an advanced model of banking. Comprehensive policies will ensure better control over the system including strong security measures and management of disputes which is likely to occur. Secondly, there would be no more unilaterally dictating terms and conditions in agreements and contracts[132] on mobile banking services as they would simply play as guidelines when bank agreements or contracts are being made.

6.1.6 Creation of Comprehensive fraud control programmes

These include non-other than cost effective automated transaction monitoring and sanctions screening system so as enable early detection and prevention of fraud and other suspicious activity.[133] The purpose of such programs must be properly strengthened to enable the good compliance with the procedures and reduce fraud risks of any sort. Possible risks must be addressed and adequately mitigated with appropriate controls such as consumer sensitization

129 Questionnaires were issued to some of Bankers working at EXIM and KCB Bank in Mwanza where the study was conducted, and such responses were received. See, Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 52.

130 Mudiri, J., *Fraud in mobile Financial Services*, A Paper Published by Micro Save Publication, 2012, p. 1 <https://www.ifc.org/wps/wcm/connect/e6ae6dd9-ad8c-4663-9c38-832c1d46a9fO/Tool+7.1._Risk+Management.pdf?> accessed on 28th June 2021

131 Mutalemwa, C., *Protection of Customers' Rights Against Fraudulent Transactions in Mobile Banking: Analysis of the Law and Practices in Tanzania,* a Dissertation submitted for the partial fulfillment of the Degree in Masters of Commercial Law at Mzumbe University, Morogoro of Tanzania, 2022, p. 68.

132 Kato, I., *Legal Framework Challenges to E-Banking in Tanzania,* PSU Research Review, 2019, Vol. 3, Issue 2, p. 105.

133 Buku, M. and Mazer, R., Fraud in Mobile Financial services: Protecting Consumers, Providers and the system, CGAP Publications, Washington, 2017, p 3.