Regulatory Oversight of FinTech in the Era of Artificial Intelligence: Assessing Consumer Risks in Tanzania's FinTech Sector

Abdallah A. Mrindoko
Lecturer at the Open University of Tanzania
Abdalla.ally@out.ac.tz

Abstract

The rapid evolution of Financial Technology (FinTech) is significantly transforming the financial sector, filling gaps traditionally left by conventional banks. This transformation is expanding access to formal financial services, fostering economic growth and reducing poverty in Tanzania. Despite its substantial growth, the FinTech industry in Tanzania operates without a comprehensive legal and regulatory framework, thereby exposing consumers to unforeseen risks. This paper examines the legal and regulatory challenges stemming from the integration of Artificial Intelligence (AI) and Machine Learning (ML) in the financial industry. To address these issues, this study employs doctrinal legal methods and a comparative study approach. It draws insights from international legal instruments, policies, and laws of other jurisdictions to identify legal gaps and propose solutions. The study utilises deductive and inductive reasoning for data analysis, applying statutory interpretation rules to evaluate Tanzanian laws and identify existing gaps. Furthermore, the Ejusdem Generis rule is employed to assess the legal landscape and challenges associated with AI adoption. Key Tanzanian laws and Regulatory bodies are scrutinised to pinpoint regulatory shortcomings. This study identified deficiencies and provide recommendations to enhance FinTech security in Tanzania.

Keywords: *M-money, FinTech, Artificial Intelligence (AI), Machine Learning (ML), Risk, Tanzania*

1.0 Introduction

The financial landscape is currently experiencing an insightful metamorphosis, driven by the swift ascent of Financial Technology, commonly known as FinTech. FinTech stands as a catalyst for revolutionising the management of finances, disrupting conventional banking models, and reshaping the entirety of the financial sector.[1] With innovative technologies like mobile payments, block chain, Artificial Intelligence (AI), and data analytics, FinTech is bringing about unprecedented changes in how we bank, invest, and access financial services. FinTech represents the synthesis of advanced technologies into the fabric of

[1] E Feyen., FinTech and the digital transformation of financial services: implications for market structure and public policy, Bank for International Settlement, Papers No 117, 2021

financial services, enhancing delivery and accessibility to consumers across the globe. This combination spans a diverse array of applications and processes, propelling both respected banking institutions and agile startups into the forefront of economic transformation. The proliferation of FinTech has not only democratised financial services, facilitating access for previously unbanked populations, but it has also introduced a new level of efficiency and security in financial transactions.[1]

The use of technology in financial services is not a new phenomenon, but recent developments have increased its pace, scope, and impact. The innovation in financial technology is rapidly disrupting the financial industry and bridging the gaps left by banks.[2] While there is no single definition for FinTech, the working definition adopted by the Financial Stability Board defines it as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services".[3] In Sub-Saharan Africa, FinTech presents opportunities that have not existed before. FinTech is increasingly recognised as a key enabler for financial sectors worldwide, enabling more efficient and competitive financial markets while expanding access to finance for traditionally underserved consumers.[4] The rise of the FinTech sector has profoundly impacted individuals at the base of the economic pyramid, lifting them to higher levels. Mobile technology, particularly digital finance, is spearheading greater access to financial services and promoting digital financial inclusion. Financial inclusion is crucial for achieving sustainable development goals (SDGs). Studies suggest that expanding financial inclusion within countries can advance nine of the seventeen SDGs and potentially support two additional SDGs that have yet to be fully explored by researchers.[5] Traditional banking institutions have significantly contributed to integrating a large portion of the population into the formal financial system. However, in sub-Saharan Africa (SSA), there are notable limitations due to the insufficient number of bank branches, with most branches concentrated in urban areas, thus neglecting the rural population. Additionally, the formal financial systems' stringent Know Your Customer (KYC) requirements and high initial deposit amounts have often hindered

[1] W. Zhou, *The Transformative Impact of FinTech on Financial Services*: A Comprehensive Analysis, (2021). p. 86
[2] UNCDF. (2021). Tanzania, the FinTech start-up landscape in Tanzania, p. 3
[3] Ibid.
[4] A.K Kamara and B Yu, The Impact of FinTech Adoption on Traditional Financial Inclusion in Sub-Saharan Africa, Risks, 2024. 12: 115. https:// doi.org/10.3390/risks12070115
[5] Ibid.

ordinary people from accessing banking services.[6] Given the limitations of the traditional banking system and existing economic disparities, FinTech has emerged as a transformative force for many individuals at the bottom of the pyramid.

1.0 Overview of FinTech Technology

Financial Technology, commonly known as FinTech, denotes the utilisation of technology to deliver financial services. This sector covers technology-driven startups that compete with traditional banks and financial institutions by offering diverse services such as mobile payment solutions, crowd funding platforms, online portfolio management, and international money transfers.[7] It includes a wide range of financial services and products that intersect with technology. These include peer-to-peer (or P2P) lending, online payments and foreign exchange services, digital wallets and e-money, automated or robo investment advice, artificial intelligence (AI), big data analytics, block chain and crypto-currencies and many more.[8] The realm of FinTech comprises a wide range of activities traditionally associated with the financial sector. This includes services such as payment processing, lending, asset management, and insurance, among others.[9] The Financial Stability Institute has developed a "FinTech tree" that categorizes different FinTech activities and the underlying factors enabling them. This tree has three main components: the crown, the trunk, and the roots. The crown **r**epresents the FinTech activities themselves, such as payment mediation, lending, asset management, and insurance-related services. The Trunk**,** consists of various technologies that support these FinTech activities. Examples include distributed ledger technology (DLT), artificial intelligence (AI), and machine learning (ML). The Roots**,** comprise various policies implemented by authorities to promote the use of technology and foster innovation within the financial system. Examples include policies on digital identification methods that enable public access to digital services, open banking regulations, and initiatives to facilitate innovation. Open Banking, allows third-party developers to access client data from banks to build various financial services and functions.[10]

[6] T, Beck, et al. Banking in Africa Opportunities and Challenges in Volatile Times, World Bank Group, Policy Research Working Paper, 10632, (2023).
[7] S. Anyfantaki, The evolution of Financial Technology (FinTech), *Economic Bulletin, volume 44,* 2016. *pp. 47-62.*
[8] Ibid.
[9] H. Eklööf, An overview of FinTech and crypto assets,2022.
[10] D. Wilsby and K.Winström, Financial Technology's effect on the Swedish banking Industry, egree Project in Production Management Division for Production Management at Faculty of engineering LTH Lund University 2023.

In innovation facilitation, authorities may set up innovation centers or regulatory sandboxes where new entities can test their products or services in a controlled environment. For instance, in Sweden, Finansinspektionen (FI) has established an innovation center to guide firms on organising their operations according to persisting legislation. Similarly, in the UK, the Financial Conduct Authority (FCA) has established a regulatory sandbox. Legislators worldwide are also creating regulations to promote innovation within financial services. An example is the Payment Services Directive (PSD2) of the European Union, which requires banks to share information with other entities, such as FinTech firms. Regulatory sandboxes, introduced in 2015 by the UK FCA, have gained significant interest from regulators and innovators globally.[11] In Tanzania, the Bank of Tanzania has established the FinTech Regulatory Sandbox Regulations, 2023. These regulations aim to enable the testing and deployment of FinTech innovations in a live environment within specified parameters and timeframes.

While FinTech products and services vary widely, they all leverage new or emerging technologies to deliver traditional financial services in a more cost-effective, accessible, and consumer-friendly manner. They also facilitate the development of innovative financial products and services. Typically, these offerings are more innovative and significantly cheaper compared to those provided by traditional financial institutions. [12] The use of technology to deliver financial services is not new and in fact, the financial industry has always been at the forefront of technological adoption. Examples of this include the development of innovations such as the use of telegraphic networks to perform transactions in the XIX century, the creation of credit cards in 1950 or the Automated Teller Machines in 1967. As financial institutions started to embrace digital computing, services such as online and mobile banking started to emerge during the 1980s and 1990s, facilitating remote access of services' users and operators.[13]

One of the most noted disruption trends arising out of FinTechs is the increase of non-financial companies offering financial services. It refers to Financial Services Provides (FSPs) that are generally outside the traditional banking institutions and cater specific financial services to its customer segments. They include the Technology companies such as PayPal, Google Wallet, Apple Pay, Samsung Pay, Konga Wallet and We Chat that offer e-wallet, payment, and

[11] Ibid.
[12] Ibid.
[13] FinTech Regulatory Aspects Working Group (REG WG). Key Aspects around Financial Technologies and Regulation Policy report, 2019. p. 10.

transfer services. Also, the Mobile Network Operators (MNOs) have found application of innovative business models especially in the payments and lending space across developing and less developed economies such as in Africa.[14] These MNOs provide a range of financial services such as basic payment services or micro-loans to the unbanked population.

The other beneficiaries of Technology are the Cash networks, which are companies that are neither a bank nor a telecommunication company and that create their own network of agents. These agents are retail outlets, at which clients of the cash network can deposit or withdraw cash, or make transfers. In addition, there are E-Retailers which are companies that are focusing on creating a market place for various products and services online. These include companies such as Alibaba & Amazon who leverage their extensive customer database to offer additional financial services like e-wallets, payments as well and lending facilities.[15] These disruptions, driven by innovative value propositions, have given rise to thousands of FinTechs worldwide, marking an unprecedented startup phenomenon. Many FinTechs, leveraging their robust business models, have achieved significant success while also fostering opportunities for traditional financial institutions to explore collaboration and partnerships, enhancing their reach and efficiency. More importantly, FinTechs are now pushing the traditional players to become more creative and agile.[16] Today, FinTech affects every area of the global financial system, with perhaps the most dramatic impact in China, where such technology firms as Alibaba, Baidu, and Tencent have transformed finance. China's inefficient banking infrastructure and high technology penetration make it a fertile ground for FinTech development.[17]

Emerging markets, particularly in Asia and Africa, have begun to experience what we characterise as FinTech 3.5, an era of strong FinTech development supported by deliberate government policy choices in pursuit of economic development. FinTech development in Africa has been led by telecommunications companies on the back of two factors: the rapid uptake of mobile telephones and the underdeveloped nature of banking services. Mobile money the provision of basic transaction and savings services through e-money recorded on a mobile phone has been particularly successful in Kenya and

[14] Bhattacharjee, I et al. (2024). The Rise of FinTech: Disrupting Traditional Financial Services, Educational Administration: Theory and Practice, Vol. 30(4), pp. 89-97.
[15] Ibid.
[16] Ibid.
[17] Ibid.

Tanzania.[18] Mobile money has significantly spurred economic development by providing customers with a means to securely save and transfer funds, pay bills, and receive government payments. M-Pesa, launched in 2007, remains Africa's best-known success story.

Although FinTech is transforming the economy and financial landscape through offering wide-ranging opportunities it has also been the cause of raising potential risks. As the technology is growing it has also been captured with the inclusion of Artificial Intelligence and Machine learning in its operations.[19] The inclusion of AI, brings new risks that were not anticipated before. Although the integration of AI in the financial sector brings several advantages such as reshaping the FinTech industry, driving innovations that enhance efficiency, reduce risk, and deliver personalized customer experiences. Transforming traditional banking and financial services, automating processes, improving decision-making, and providing customized services. Machine learning algorithms continuously monitor transaction data in real-time, identifying anomalous patterns that suggest fraudulent activities, thereby reducing risks and building consumer trust in digital payment platforms. However, AI brings also various risks and regulatory challenges such as liability issues that need a careful handling process.[20]

2.0 Artificial Intelligence in the FinTech

The rapid development of FinTech is driven by innovative technologies, such as artificial intelligence and block chain, and it has gained attention from innovators, academics, and regulators. The integration of AI in the financial sector is reshaping the FinTech industry, enhance efficiency and productivity and deliver personalised customer experiences.[21] There are varying reasons for the adoption of AI /ML in the financial sector. Some uses of AI/ML include powering chatbots in customer service functions, identifying investment opportunities, executing trades, augmenting lending models or making lending decisions, and identifying and preventing fraud.[22]

The extent to which a sector or firm adopts various technologies reflects a variety of factors, including a firm's ability to fund internal development and

[18] D. W Arner, et al, FinTech and RegTech in a nutshell, and the future in a sandbox, CFA Institute Research Foundation, 2017, pp.7-8.
[19] Y. Han, et al, The Impact of Artificial Intelligence on the Financial Services Industry, *Academic Journal of Management and Social Sciences,* Vol. 2, No. 3, 2023, pp. 83-85
[20] Ibid.
[21] K.L Siau, et al., Artificial Intelligence in Financial Technology, Conference paper, 15th China Summer Workshop on Information Management (CSWIM 2022).
[22] Ibid.

regulatory requirements.[23] Artificial intelligence (AI) is the general term used to describe the process of programming computers and machines to think and operate like humans. Machine learning (ML) is a subset of AI that describes computers and programs that may be programmed to operate with minimal human intervention and can in some instances learn and/or update themselves. According to Boucher,[24] AI refers to systems that display intelligent behaviour by analysing their environment and taking action with some degree of autonomy to achieve specific goals. AI is an umbrella term including a wide range of technologies and applications that have little more in common than their apparent intelligence, a quality which remains very much open to interpretation.

Several actions over the past few years have helped raise the profile of AI/ML and its role in delivering financial services. Open AI's introduction of the large language model (LLM) ChatGPT in 2022 was a rare moment when an AI/ML technology became directly accessible by the broad public.[25] Artificial intelligence (AI) has fundamentally changed the way financial industry interact with their customers, ushering in a new era of personalised and seamless experiences. Traditionally, banking interactions were often generic and impersonal, with limited scope for customization. However, AI technologies have enabled banks to leverage vast amounts of customer data to understand individual preferences, behaviors, and needs. By analysing transaction histories, browsing patterns, and social media interactions, AI algorithms generate insights into each customer's financial goals, lifestyle choices, and risk tolerance.[26] Machine learning algorithms continuously analyse transaction data in real-time, detecting anomalous patterns indicative of fraudulent activities. This proactive approach not only mitigates risks but also instills confidence in consumers, fostering trust in digital payment platforms. Moreover, AI-powered chatbots and virtual assistants are revolutionizing customer interactions in the realm of payments.[27]

These intelligent agents leverage natural language processing algorithms to understand and respond to user queries in real-time. By offering personalised recommendations, resolving inquiries promptly, and facilitating seamless

[23] P. Tierno, Artificial Intelligence and Machine Learning in Financial Services, Congressional Research Service, R47997, 2024.
[24] P. Boucher, Artificial intelligence: How does it work, why does it matter, and what can we do about it? European Parliament, 2020.
[25] Ibid, p. 1.
[26] A. Abbas, The Role of AI in Disrupting Traditional Banking and Financial Services: Harnessing Data Analytics and Machine Learning for Competitive Advantage, 2024. DOI:10.13140/RG.2.2.32110.22087.
[27] Ibid.

transactions, AI-driven chatbots enhance the user experience and drive customer satisfaction.[28] Furthermore, the integration of AI and blockchain technology is transforming transactional processes within the supply chain through the use of smart contracts. These self-executing contracts, encoded on a blockchain ledger, automatically execute and enforce the terms of an agreement when predefined conditions are met. By automating contractual agreements, such as purchase orders, invoices, and payments, smart contracts streamline transactional processes, reduce administrative overhead, and mitigate disputes.[29]

In Tanzania, the convergence of FinTech and AI has notably bolstered the integration of mobile wallets with major digital payment networks like Visa, MasterCard, and PayPal. This synergy has introduced innovations such as virtual cards including Master Pass and M-Visa, enabling users to conduct card transactions seamlessly without the need for conventional bank accounts. Moreover, the embrace of contactless payment methods alongside the widespread accessibility of ATMs has not only streamlined domestic transactions but also enhanced the ease of conducting international card payments, thereby propelling the evolution of Tanzania's digital payment landscape.[30] However, the widespread adoption of AI in the financial industry is not without its challenges. Significant hurdles include concerns about data privacy, security, and algorithmic biases. Additionally, the autonomous capabilities of AI have sparked legal discussions regarding liability issues in both contractual and criminal contexts.[31]

3.0 Consumer Risks in Tanzania's FinTech sector

The evolution of FinTech, coupled with its integration with AI, has introduced significant risks to the financial services sector. This is primarily due to the abundance of highly sensitive and valuable data it manages. As user numbers flood, hackers increasingly target everything from credit card information to personal financial data, exploiting it by selling on the deep web or for personal gain.[32] Moreover, cybercriminals have advanced their tactics, now capable of executing sophisticated cyber-attacks such as ransomware and Distributed Denial of Service (DDoS) assaults to breach confidential systems.[33]

[28] F. Akram., Innovations in FinTech: AI-Enhanced Payments and Supply Chain Management, 2024, p.2
[29] Ibid.
[30] Bank of Tanzania, Bank of Tanzania National Payment Systems annual report, 2022.
[31] O. Owolobi et al, Ethical Implication of Artificial Intelligence (AI) Adoption in Financial Decision Making, *Computer and Information Science; Vol. 17, No. 1,* 2024, pp. 49-56.
[32] C.H Patil et al, Challenges in FinTech Security, *Grenze International Journal of Engineering and Technology, June Issue,* 2023 pp. 2100-2105.
[33] Ibid.

According to Bank for International Settlement,[34] technological advancements in banking have increased risks to bank soundness and financial stability. Digital fraud is one example, where criminals exploit digitalization to commit online fraud on a greater scale and scope than previously, enabled by the agility provided by digitalization. The cybercriminal ecosystem has become increasingly industrialized, allowing non-technical criminals to access and use cyber tools without technical expertise. Dedicated marketplaces on the dark web facilitate the sale and purchase of payment card data and online banking access. Fraudsters and attackers employ increasingly sophisticated techniques, with malicious codes adapted to many banking applications that can bypass current security measures.[35]

Risk in the financial sector represents the likelihood of undesirable events occurring unexpectedly, and risk management involves skillful handling of this possibility. While theoretically, risk can also entail potential favorable outcomes, it predominantly refers to adverse circumstances rather than beneficial ones. Risk is a fundamental aspect of banking operations, regulatory frameworks, and the occurrence of banking crises.[36] In banking, risk pertains to the potential for a reduction in economic gain due to monetary losses, expenses, or adverse outcomes associated with the transactions or activities of a bank. It can also be construed as the impact of uncertainty on objectives.[37] Technological developments in the financial sector, such as the introduction of various digital platforms like M-money services, have introduced risks impacting both bank-led and non-bank-led models. Traditional risks that previously affected conventional banks now extend to mobile banking entities. However, there are distinctions in the degree to which specific risks apply to traditional banks compared to their manifestation in mobile money operations. To mitigate security risks within the industry, it is imperative to establish a robust legal framework capable of addressing critical issues and guiding the mobile banking sector.[38]

The rapid advancements in financial services have opened new opportunities while simultaneously introducing security challenges and risks for financial providers, telecommunications carriers, and the overall financial system.[39]

[34] Bank for International Settlement, Digital fraud and banking: supervisory and financial stability implications, Discussion Paper, 2023.
[35] Ibid.
[36] A.J Hafeth, Risk definition in banks, 2017 p.78.
[37] Ibid.
[38] M. Tashtamirov, Financial Innovation and Digital Technology in the Banking System: An Institutional Perspective, SHS Web of Conferences, 2023, 172, 02004.
[39] A. Ally, *Mobile Money Regulations in Tanzania*, PhD thesis, The Open University of Tanzania, 2017. p. 99.

Efforts to regulate mobile banking services have been undertaken, including distinguishing between bank-based and non-bank-based models. However, regardless of whether a telecommunications company or a bank leads the initiative, there remains insufficient insight into the specific risks associated with individual mobile money schemes. The extensive use of electronic and mobile money causes additional risks, complicating the work of electronic money issuers (EMIs) and the functioning of payment systems.[40]

The potential "disruptive" nature of FinTech presents new risks and challenges for regulators, which could negatively impact financial stability and integrity if not properly managed. While some of these risks are new, many are simply new forms of existing risks, arising not only from the technology behind FinTech but also from new or modified business models, product features, and provider types. Additionally, consumers now have greater access to more complex or unfamiliar financial products. For instance, the rapid growth of the P2P lending market in China during the early 2010s led to significant platform collapses, fraud, and operator misconduct, resulting in substantial consumer losses.[41]

In October 2018, the World Bank Group (WBG) and the International Monetary Fund (IMF) introduced the Bali FinTech Agenda, comprising 12 policy elements aimed at leveraging the benefits of FinTech while managing associated risks.[42] Policy six underscores the need for nations to adapt regulatory frameworks and supervisory practices to ensure the orderly development and stability of the financial system. This facilitates the safe introduction of new products, activities, and intermediaries while preserving trust and confidence and addressing emerging risks. While existing regulatory frameworks may mitigate several FinTech risks, new challenges may arise from innovations lying beyond the current regulatory perimeter, necessitating regulatory adjustments. Holistic national policy responses, guided by international standards, are imperative.[43] To mitigate risks and ensure the security of mobile banking transactions, a robust legal framework is essential. As the adoption of mobile money services grows, financial regulators worldwide are addressing risks associated with mobile technology use. Policymakers and regulators are drafting regulations tailored to the mobile

[40] K.Croxson, et al. Platform-based business models and financial inclusion, BIS Working Papers 986, Bank for International Settlements, 2021.
[41] WBG, Consumer Risks in FinTech New Manifestations of Consumer Risks and Emerging Regulatory Approaches, *Policy Research Paper*, 2021 p.12.
[42] Ibid.
[43] IMF, IMF policy paper, the Bali FinTech agenda, 2018.

money era, albeit facing challenges in synchronizing financial and telecommunication regulations to enhance mobile banking services.

Furthermore, the Bali FinTech Agenda underscores the importance of safeguarding the integrity of financial systems by identifying, understanding, assessing, and mitigating the risks of criminal misuse of FinTech. Technologies that bolster compliance with anti-money laundering and combating the financing of terrorism (AML/CFT) measures are essential. While FinTech innovations generally serve legitimate purposes, some may facilitate criminal activities, posing threats to financial integrity. Country responses vary, but strengthening AML/CFT compliance and monitoring, aided by technology, remains paramount.[44] Efforts to regulate mobile banking services, whether led by telecommunications companies or banks, must address the specific risks associated with each mobile money scheme. Given the array of FinTech products and services available, this paper will focus on addressing varieties of financial risks, efforts that have been taken and the remaining gaps that need to be bridged.

4.0 Prevalent Risk Types in the FinTech Sector in the Era of AI

The integration of Artificial Intelligence (AI) in the FinTech sector has revolutionized financial services, but it also introduces a range of risks. Here are the common risk types prevalent in the FinTech sector amid AI advancements

4.1 Operational Risks

Operational risk pertains to the possible financial loss stemming from ineffective or malfunctioning internal procedures, structures, personnel, or external occurrences. It encompasses a broad spectrum of risks that may emerge during the routine functioning of an entity. It is also encompassing disruptions caused by system malfunctions, data breaches, or inadequate monitoring of AI-driven applications. External factors like cyber-attacks or natural disasters further amplify this risk. As per the Basel Committee on Banking Supervision, operational risk is defined as "the risk of experiencing losses due to deficient or unsuccessful internal processes, personnel, and systems, or due to external events.[45] According to the risk management guidelines for banks and financial institutions in Tanzania, 2010, Operational risk can stem from various sources including human actions, internal procedures, system failures, and external incidents like terrorism, vandalism, and earthquakes. This risk is present in both

[44] Ibid.
[45] A. Ally, Mobile Money Regulations in Tanzania, PhD thesis, *above at note* 40.

conventional banking and mobile banking, particularly in Payment Systems, encompassing Processing, Authorization, and Computational functions. For instance, whether a payment transaction is processed manually or through automated systems (or a blend of both), there's a risk associated with its successful completion within a satisfactory timeframe or at all.[46]

4.2 Fraud Risk

One of the fundamental risk surrounding consumers with respect to FinTech products, and transactions that are taking place online are losses from fraud or other misconduct by Financial Service Providers (FSPs) as well as third-party fraud. While AI enhances fraud detection, it also introduces new avenues for sophisticated fraud techniques that exploit AI tools. Fraud risk is the possibility of any unexpected loss, be it financial, reputational, or material, due to fraudulent activity by an internal or external actor. The Association of Certified Fraud Examiners (ACFE), the world's leading anti-fraud body, defines fraud as any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.[47] Mobile money fraud can therefore be defined as fraud that takes place on assets owned or held by a mobile money service to the detriment of a mobile money service provider, its customers, agents or third parties. Assets include money, information, and intangible assets such as brand, reputation, or services.[48] The conditions under which such losses do occur are numerous, such as internal theft of funds, identity theft, or phishing. Potential perpetrators include FSPs themselves, their employees, agents, merchants, business partners and service providers, and external actors. These criminals, and the data or facilities being affected, may be located remotely such as in the cloud and even internationally, creating additional enforcement and evidence gathering difficulties.[49]

The impact of fraud can be seen in the form of financial losses**,** due to theft, embezzlement, or other types of financial crime. Fraud in the digital environment could be classified into two categories namely, direct and indirect frauds. Direct fraud would include credit/debit card fraud, employee embezzlement, and money laundering and salami attack. Indirect fraud would include phishing, pharming, hacking, virus, spam, advance fee and malware. It

[46] Ibid.
[47] GSMA, Mobile money fraud typologies and mitigation strategies, 2024.
[48] Ibid.
[49] World Bank Group, Consumer Risks in FinTech New Manifestations of Consumer Risks and Emerging Regulatory Approaches, Policy Research Paper, 2021.

involves impersonation and theft of identity, credit card number or other identifying information to carry out fraudulent activities.[50]

Fraud poses a significant risk within both mobile money systems and traditional banking institutions. Funds can be illicitly siphoned from the system through a variety of unlawful methods. For instance, account details may be compromised leading to unauthorized debits from customers' accounts. Other fraudulent practices encompass techniques such as phishing for PIN codes to access e-wallets or assuming false identities to gain remote entry into a service provider's server. The potential for large-scale fraud increases substantially in cases of data security breaches occurring at payment providers or any entity storing payment information along the payment process.[51]

According to Global Risk Report 2020 issued by World Economic Forum, Data & Money Theft, Fraud Risk and Cyber security attacks occupy the 6th and 7th place among the world's Top 10 risks. In terms of likelihood and impact on a scale of 1 to 5, Data Theft/Fraud and Cyber-attack map to close to 4 in terms of both likelihood and impact. This explains why the Trio of Data Privacy, Fraud & Cyber-attacks must be a locus of attention for Business entities, Regulatory bodies and the Government.[52] Different fraudulent techniques typically put consumers and targeted institutions at risk. Attackers employ various sophisticated tactics to gain unauthorized access to data. Cyber-attacks can result in data breaches, allowing unauthorized parties to access sensitive or confidential information, often serving as a precursor for criminals seeking to make unauthorized payments. Scammers successfully acquire personal information or credentials belonging to individuals or businesses, enabling them to manipulate targets or access payment accounts to initiate transactions.[53]

4.3 Regulatory Risk

One significant risk associated with the FinTech sector is regulatory uncertainty. Consumers using FinTech products may find themselves with less protection compared to those using traditional financial services, primarily due to gaps in existing financial consumer protection regulations. This can leave consumers vulnerable, lacking adequate legal safeguards and access to complaint-handling mechanisms specifically tailored to address issues arising

[50] S. Dzomira, Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe, Risk governance and control: *financial markets and Institutions, Vol. 4, Issue 2,* 2014. p.17.
[51] Ibid.
[52] K. Chari, Fraud Risk in a Digitized FinTech ecosystem troubling trends, issues and approaches to mitigate Fraud Risk, 2020, p.1.
[53] WBG, Fraud risks in fast payments, 2023, p.4.

from FinTech services.[54] Regulatory risk is defined as the potential for financial loss due to non-compliance with laws, regulations, or standards. This risk encompasses the challenges and consequences associated with adhering to or failing to adhere to regulatory guidelines and rules. Key areas of regulatory compliance include anti-money laundering (AML) and combating the financing of terrorism (CFT) measures, Know Your Customer (KYC) protocols, data privacy requirements, account and transaction limitations, trust account regulations, and the use of agents. Ensuring compliance in these areas is critical for mitigating regulatory risk and safeguarding the integrity and stability of financial operations.[55]

For instance, consumers who use e-deposit services under the non-bank-led model face significant risks because their deposits are not protected by deposit insurance, which is only available for the bank-led model.[56] The current dominance of FinTech in the financial sector, particularly with the integration of AI, lacks a specific legal framework, resulting in numerous unresolved legal gaps. The liabilities of autonomous agents remain a contentious issue in the legal sphere. Consequently, compliance and regulatory risks are more pronounced in FinTech services. There are several blind spots and loopholes in existing financial laws, regulations, and supervisory rules. The industry's inadequate legal treatment and supervision allow for some illegal operations. Institutions exploit these legal gaps to engage in criminal and unlawful activities, leading to economic losses for financial entities.[57]

4.4 Technology Risk

Technology Risk refers to technology failure that leads to the inability to transact. It is closely linked to operational risk. Transactions within a Digital Financial Services (DFS) travel through several communications systems and devices in order to initiate the transaction, transfer funds, and communicate confirmations with clients.[58] There are numerous examples of technology risks within financial technology systems, one of which pertains to transaction delays

[54] World Bank Group. (2021). Consumer Risks in FinTech New Manifestations of Consumer Risks and Emerging Regulatory Approaches, Policy Research Paper.

[55] The Master Card Foundation and International Finance Corporation. (2016). Digital financial services and risk management, Handbook, p. 24.

[56] A.M Ally, Legal and regulatory framework for mobile banking in Tanzania, *International Journal of Law and Management Vol. 66 No. 1*, Emerald Publishing Limited, 2024.

[57] M. Hasan and A. Hoque., FinTech Risk Management and Monitoring, *International Series in Operations Research and Management Science, Volume 336,* 2023 pp. 3-16.

[58] The Master Card Foundation and International Finance Corporation, Digital financial services and risk management, Handbook, 2016), p.24.

arising from insufficient capacity to handle demand, consequently leading to system queues.

According to Huang and Tan,[59] it is having been revealed that the technological developments such as the Internet, computers, and other technological infrastructure have made the security of data during long-distance transmission to be increasingly complex. The more base stations that data passes through, the greater the risk of leakage, posing significant threats to data security. FinTech, which relies heavily on emerging technologies such as artificial intelligence (AI), big data, and cloud computing, faces additional challenges in ensuring the secure collection, transmission, and storage of data. Security vulnerabilities in these processes can be exploited by criminals, leading to potentially severe financial losses for users.[60] Besides, when financial service providers are constrained by their technological capabilities, often resort to outsourcing strategies to build their data platforms. However, the quality and trustworthiness of employees in outsourcing companies can be inconsistent. Malicious actions by such employees, including deliberate information leaks, can expose users to significant risks.[61]

Jain et al[62] has observed that the rapid development of domestic FinTech has occurred in an environment lacking a robust social credit system. This leapfrog growth, while impressive, is accompanied by technological limitations that hinder the ability to identify and mitigate newly emerging financial risks. Consequently, these unidentified risks can spread more easily, exacerbating potential threats to the financial ecosystem. To address these challenges, it is crucial for FinTech companies and traditional banks to implement rigorous security protocols, conduct thorough vetting of outsourcing partners, and continually update their technological safeguards. Additionally, the establishment of a comprehensive social credit system could play a pivotal role in mitigating these risks and fostering a more secure financial environment.

The complexity of Digital Financial Services (DFS) involves multiple interconnected systems, wherein a breakdown at any juncture can trigger

[59] A. Huang and D. Tan, The Study and Overview of FinTech's Impacts on the Risk-Taking of the Traditional Bank Industry. Theoretical Economics Letters, 2024, 14, 1441-1454. https://doi.org/10.4236/tel.2024.144069

[60] Ibid.

[61] J.A Barefoot, Digital Technology Risks for Finance: Dangers Embedded in Fintech and Regtech, Mossavar-Rahmani, Center for Business and Government Weil Hall | Harvard Kennedy School | 2020, www.hks.harvard.edu/mrcbg.

[62] R. Jain, et al, Systematic Literature Review of the Risk Landscape in Fintech. Risks 11: 36, 2023, https://doi.org/10.3390/risks11020036.

transaction delays, often leaving both customers and agents uncertain about transaction completion. This uncertainty may manifest in delays in receiving confirmation SMSs on the customer's device. Another significant risk in DFS is Network Connectivity Failure, presenting challenges such as intermittent coverage, insufficient availability, and network downtime, all of which impede transactions and pose a threat to business continuity. Connectivity encompasses internal networks of providers, communication infrastructure linking third-party channels, and clients. When networks falter, users are unable to initiate transactions, potentially resulting in reputational damage due to prolonged wait times for network restoration, thus undermining the customer experience.[63]

4.5 Agent Management Risk

The introduction of agents to act on behalf of financial services providers presents many benefits in cost, geographical reach, and scale, but also introduces new risks. The management and supervision of agents is imperative to a well-functioning service that protects customers. The use of agents can trigger operational, technological, legal, reputational, and fraud risk. An agent's business operations may be put at risk from excessive deposits.[64] The cash may be stolen, and this is especially the risk if the agent develops a reputation for holding large amounts of cash. Agents and their tellers may make key stroke errors in entering transactions or counting errors in cash management that will result in a float being unreconciled and sustaining losses either to the agent or to the customer. Teller errors also include the risk of losing or damaging paper records that may put the agent and provider at risk of regulatory non-compliance.[65] In the realm of AI, the integration of agents in FinTech services offers a wide array of benefits, significantly transforming how financial services are delivered. These advantages include cost efficiency, as AI-driven agents reduce operational expenses by automating routine tasks and optimizing resource allocation. Additionally, they enhance geographical reach, enabling financial institutions to penetrate underserved or remote areas where traditional banking infrastructure is limited. Scalability is another key benefit, as AI systems can handle an increasing volume of transactions and interactions without proportional increases in costs or time, thus supporting business growth.[66]

However, the integration of AI into agent management introduces a range of complex risks and challenges that demand careful consideration. One primary

[63] Ibid.
[64] M. Kerse, The use of agents by digital Financial Services Providers, Technical Note, CGAP/World Bank, 2020.
[65] Ibid.
[66] Ibid.

concern is the security of AI systems, as these agents become potential targets for cyberattacks, data breaches, and manipulation. The reliance on AI also raises questions about reliability, particularly in situations where algorithmic errors or biases could lead to financial inaccuracies, regulatory non-compliance, or discrimination against certain customer groups. Moreover, the use of AI in managing FinTech agents necessitates addressing ethical concerns, such as transparency and accountability. The decision-making processes of AI agents often lack explainability, making it difficult for stakeholders to understand or challenge outcomes. This opacity can erode trust in financial services and complicate regulatory oversight.[67]

4.6 Liquidity Risk

Liquidity reflects a bank's capacity to fund the expansion of its assets and meet both expected and unexpected cash or collateral demands at a manageable cost, all while avoiding substantial losses. Proper liquidity management is essential, as it enables a bank to maintain operations and fulfill its financial obligations, even during periods of economic stress or financial uncertainty.[68] Liquidity risk arises when a financial institution cannot meet its cash flow needs and obligations as they come due, potentially leading to insolvency. This risk is particularly critical because it can affect a bank's solvency, market reputation, and overall stability. Managing liquidity risk involves maintaining an adequate cushion of liquid assets, ensuring access to funding markets, and implementing robust contingency funding plans.[69] A bank's capacity to manage liquidity risk effectively is crucial for its resilience and long-term viability. Inadequate liquidity can force a bank to sell assets at a loss or resort to expensive emergency funding, both of which can erode capital and undermine confidence. Therefore, banks must continuously monitor their liquidity positions, stress-test their funding strategies, and adopt proactive measures to mitigate potential liquidity shortfalls. In today's interconnected financial environment, liquidity risk management also involves understanding and preparing for systemic risks. Disruptions in one part of the financial system can quickly propagate and amplify liquidity pressures across institutions, highlighting the importance of regulatory oversight and coordination among financial entities. By adopting

[67] M. Kerse, et al, The use of agents by digital Financial Services Providers, Technical Note, CGAP/World Bank, 2020.

[68] Bank for International Settlements. (2008). Principles for Sound Liquidity Risk Management and Supervision, Basel Committee on Banking Supervision

[69] M. Kumar and G.C Yadav, Liquidity risk management in bank: a conceptual framework, *AIMA Journal of Management & Research, May* 2013, *Volume 7, Issue 2/4*

comprehensive liquidity risk management practices, banks can better navigate financial uncertainties and maintain their operational integrity.[70]

The integration of financial institutions and the telecommunications sector in offering e-money stored in trust accounts has introduced significant consumer risks, particularly concerning insolvency. One major concern with e-money arrangements is the potential insolvency of the provider, which could result in insufficient funds to meet the demands of e-money holders.[71] Unfortunately, e-money deposits kept in trust accounts are not covered under deposit insurance schemes. This lack of protection means that, in the event of insolvency, e-money holders would be treated as unsecured creditors. Consequently, they would be paid only after deposit holders, secured creditors, and other creditors with statutory priority. This situation places e-money holders at a considerable disadvantage, potentially leading to substantial financial losses.[72]And the sad story is that the e-money deposit kept in a trust account is not covered under deposit insurance scheme. The result of this lack of protection is likely to be that e-money holders will rank with other unsecured creditors and will be paid after any deposit holders, any secured creditors, and any other creditors with some other form of statutory priority.[73] To mitigate these risks, regulators and policymakers need to consider extending deposit insurance or creating specific safeguards for e-money deposits. Enhanced oversight and stricter regulatory frameworks can also help ensure that e-money providers maintain sufficient reserves to protect consumers. Additionally, increased transparency and consumer education about the risks associated with e-money can empower users to make more informed decisions.

4.7 Money-laundering risks

The Financial Action Task Force on Money Laundering (FATF), which is recognized as the international standard setter for anti-money laundering efforts, defines the term money laundering as "the processing of criminal proceeds to disguise their illegal origin" in order to legitimize the ill-gotten gains of crime.[74] Money laundering risk refers to the potential of financial institutions, businesses, or individuals to be used as a conduit for illegal activities, such as drug trafficking, terrorism financing, or other criminal activities. The innovations in FinTech have advanced traditional ways of

[70] Ibid.
[71] Fraud Net, Top 7 Risks for Financial Institutions and FinTech, 2023.
[72] Ibid.
[73] WBG, *above at note* 42, p.138
[74] M. Yusarina. Etal, Money Laundering Risk: From the Bankers' and Regulators Perspectives, 7th International Conference on Financial Criminology, 2015.

undertaking transactions and provided immense opportunities to individuals and businesses, such as faster and more efficient settlement of payment. However, it has also fueled illegalities such as money laundering, which essentially involves making illegally-gained financial proceeds appear to have legitimate source.[75]

A primary concern regarding FinTech is that many FinTech firms operate outside the scope of traditional banking regulations and are not fully subject to existing anti-money laundering (AML) legislation and regulations. Although mobile money (M-money) service providers are required to adhere to Know Your Customer (KYC) rules, they are not encumbered by the same rigorous banking regulations that govern traditional financial institutions. Additionally, the rapid growth of crypto currency assets poses significant money laundering risks due to the lack of comprehensive regulation in this sector. Criminals can exploit the quasi-anonymity of block chain and place assets on the market without being identified. Furthermore, the transactions are even harder to detect when criminals use mules in the layering phase, Moreover, crypto currencies provide opportunities to cash out illicit gains by transferring them anonymously to individuals which can be challenging, if not impossible, to trace.[76] As FinTech firms often bypass professional intermediaries such as banks, they may not be held to the same financial reporting standards, which are crucial for maintaining market stability.[77]

Technological innovations in payment services have made the world a global village and this enables criminal syndicates to perpetrate crime from any part of the world, particularly jurisdictions with ineffective money laundering regulations and enforcement. Hence with the aid of technology, 'dirty money' can conveniently be transferred undetected across dual or multiple regions in the global space in a snap of fingers.[78]The e-money can also be a tool for money launderers due to the impossibility of tracking it, its confidentiality, and its speed, as it is possible, in a short period, to transfer any amount through it without any obstacles and without the need for a financial intermediary.[79] In

[75] U. Anichebe, Combating Money Laundering in an Age of Technology and Innovation, 2020, SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.3627681.

[76] M Heidimaria, The Anti-money Laundering Challenges of FinTech and Crypto currencies,2023, *Nordic Journal of Legal Studies*, Vol.2(1) pp.7-19.

[77] A.R Nicholas, FinTech and Anti-Money Laundering Regulation: Implementing an International Regulatory Hierarchy Premised on Financial Innovation, 2022. *9 Tex. A&M L. Rev. 465* Available at: https://doi.org/10.37419/LR.V9.I2.5.

[78] Ibid.

[79] I . A Gailan, Fintech in Iraq and the risks of using it in money laundering operations, World Economics & Finance Bulletin (WEFB), 2022 Available Online at: https://www.scholarexpress.net Vol. 17, ISSN: 2749-3628

traditional transactions a third-party, typically a licensed bank, has had an important role in guaranteeing the authenticity and the integrity of fund transfers.

4.8 AI risks

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into the financial sector is reshaping operations, data analysis, and customer service.[80] These technologies enhance efficiency, from personalized chatbots to predictive analytics for investments. Yet, they also introduce significant risks that demand careful management. AI in FinTech poses concerns like data privacy breaches, biases influencing lending decisions, and systemic risks from interconnected AI systems. Unregulated, these technologies can amplify vulnerabilities. Mitigating AI risks is vital for consumer protection, financial stability, and trust in evolving technologies.[81]

Regulatory oversight balances innovation with risk management, aiming to harness AI's potential while safeguarding against downsides. Challenges include fairness and bias; while AI aims to be unbiased, it can perpetuate biases in training data, impacting loan approvals and exacerbating inequality. Moreover, AI's deployment in finance raises cyber security concerns. Instances such as ChatGPT's restrictions due to privacy issues highlight regulatory scrutiny and potential misuse for phishing and deep fakes. Safeguarding against these risks is crucial for maintaining cyber security and trust in AI-driven financial services.[82]

The decentralised architecture of many AI-driven financial platforms, particularly those built on block chain technology, presents significant challenges in terms of jurisdiction and dispute resolution. The distributed nature of these platforms surpasses national borders, often making it difficult to determine which legal authority has jurisdiction over cross-border transactions. Traditional legal frameworks are generally ill-suited to address the complexities that arise from these decentralized, often anonymous, platforms.[83] A key issue for the AI legal risk is the lack of harmonization in the legal and regulatory approaches taken by different countries. This creates substantial legal risks for

[80] N. Deepaak, The Future of Finance in the Era of Artificial Intelligence and Machine Learning, 2024.
[81] Y. Han et al, The Impact of Artificial Intelligence on the Financial Services Industry, *Academic Journal of Management and Social Sciences*, 2023Vol. 2, No. 3.
[82] G Shabsigh, and E. Boukherouaa, E. Generative Artificial Intelligence in Finance: Risk Considerations, 2023.

[83] H. Daiya, H, AI-Driven Risk Management Strategies in Financial Technology, *Journal of Artificial Intelligence General Science JAIGS, Vol., 5 Issue 01*, 2024, pp. 194-216.

both consumers and FinTech companies operating across multiple jurisdictions. While some nations have proactively updated their legislative frameworks to accommodate the rise of FinTech and AI technologies, others have been slower to adapt, leading to inconsistent regulatory environments. This regulatory fragmentation results in a complex and often contradictory legal landscape, which can hinder the global scalability of FinTech solutions. Companies must navigate not only the technical and operational challenges of working with emerging technologies but also the varied legal standards related to data privacy, cyber security, financial compliance, and consumer protection.[84]

The lack of global regulatory consensus poses additional risks in terms of enforcement and compliance. For example, in some jurisdictions, block chain transactions may be classified differently under financial law, complicating the resolution of disputes. Moreover, the absence of clear regulatory guidance on issues such as smart contracts and algorithmic governance leaves significant gaps in accountability. As the adoption of AI in FinTech continues to accelerate, international cooperation and the establishment of more uniform legal standards will be crucial to fostering innovation while ensuring consumer protection and regulatory oversight.[85]

5.0 Legal Framework for Addressing Consumer Risks in the FinTech Industry in the Era of AI

The legal framework governing the FinTech sector in Tanzania is complex, encompassing various laws designed to regulate the industry and provide a secure platform for commercial transactions. These regulations establish the groundwork for financial institutions offering mobile banking services and set the standards for electronic transactions. Key legislation includes the Banking and Financial Institutions Act (BFIA) of 2006, which oversees the operations of financial institutions. The Electronic Transactions Act (ETA) of 2015 provides guidelines for conducting electronic transactions, while the National Payment System Act, 2015, focuses on the regulation of payment systems. Additionally, the Electronic and Postal Communications Act of 2010, the Cybercrime Act of 2015, and the Personal Data Protection Act of 2022 address various aspects of digital communication, cyber security, and data privacy, respectively.[86]

[84] F. Igbinenikaro and A.O Adewusi, Navigating the legal complexities of artificial Intelligence in global trade agreements, *International Journal of Applied Research in Social Sciences, Volume 6, Issue 4*, 2024 pp. 488-505.

[85] Ibid.

[86] D. P. Macha, and N.M Massawe, Financial Technology in Tanzania: Assessment of Growth Drivers, AERC Working Paper FI-007 African Economic Research Consortium, Nairobi, 2023.

The Tanzania Insurance Regulatory Authority (TIRA) and the Capital Markets and Securities Authority (CMSA) also play roles in regulating specific sectors within the FinTech ecosystem. However, the primary regulatory bodies for the FinTech sector are the Bank of Tanzania (BOT) and the Tanzania Communication Regulatory Authority (TCRA). These institutions are chiefly responsible for overseeing and ensuring compliance within the industry, thereby fostering a stable and secure environment for FinTech innovations to flourish.[87] Section 4(1) of the National Payment System Act, 2015 grants the Bank of Tanzania (BoT) a broad range of regulatory and supervisory powers over the country's payment systems. Under this section, the BoT is authorized to issue licenses and approvals, regulate and supervise payment system operations, investigate potential issues, and ensure oversight of the entire ecosystem. Additionally, the BoT is responsible for providing settlement services to payment systems, clearinghouses, and central securities depositories. It also has the authority to own and operate a real-time gross settlement system, coordinate activities with relevant stakeholders, and participate in inter-bank clearing and settlement operations. In essence, the BoT is tasked with the administration and enforcement of this Act, ensuring the integrity and efficiency of payment systems in Tanzania.

Furthermore, Section 5 of the Act extends these powers by mandating that no individual or entity may operate a payment system without obtaining a valid license issued by the BoT. This ensures that all operators are subject to stringent regulatory scrutiny, thereby safeguarding the security and stability of the payment infrastructure in the country. While the Bank of Tanzania (BoT) is tasked with overseeing the financial sector, the Tanzania Communications Regulatory Authority (TCRA) is responsible for regulating electronic and postal communications in the country. The TCRA's mandate is defined by the Electronic and Postal Communications Act (EPOCA) of 2010 and the TCRA Act of 2003, which govern telecommunications, broadcasting, postal services, and the management of the radio spectrum. These laws cover a wide range of electronic technologies and Information and Communication Technologies (ICT). TCRA's key objective is to ensure the delivery of high-quality ICT services while promoting their widespread and reliable implementation.

In the FinTech sector, the Tanzania Communications Regulatory Authority (TCRA) plays a pivotal role in ensuring that mobile network operators comply with established standards for conducting financial transactions, particularly within the mobile money ecosystem (TCRA Act, 2003). However, while TCRA

[87] Ibid.

oversees the operational and technical aspects of these companies, the regulation of financial transactions is the mandate of the Bank of Tanzania (BoT). This dual regulatory framework introduces a potential risk factor within the FinTech industry, as the overlapping responsibilities between TCRA and BoT can lead to governance challenges and regulatory ambiguities, potentially hampering effective oversight and enforcement.[88]

In the midst of evolving financial technologies in Tanzania, the rise of mobile money systems, which operate under two distinct models bank-led and non-bank-led has introduced significant regulatory challenges. Notably, the non-bank-led model exhibits a certain lenience in Prudential Financial regulations, creating potential loopholes for illicit activities such as money laundering and financial terrorism. Compounding this issue is the emergence of crypto currencies, which remain beyond the regulatory scope of the Bank of Tanzania (BoT), raising serious concerns about consumer protection and the potential for misuse in illegal financial activities.

While the National Payment System Act of 2015, aligned with the 2022 G20/OECD High-Level Principles on Financial Consumer Protection, aims to safeguard consumers in both the bank-led and non-bank-led models, the effectiveness of these protections is undermined by gaps in the regulatory language. For example, Section 51(1) of the Act grants broad regulatory powers to financial authorities, yet the ambiguous language within the section detracts from its intended purpose, failing to adequately protect consumers from the risks inherent in emerging financial technologies.

Further complicating the regulatory landscape is the legal oversight of international remittances within the non-bank-led model. A closer examination of both the National Payment System Act of 2015 and the Electronic Transactions Act of 2015 reveals a critical lack of provisions addressing cross-border remittance activities. This omission is particularly concerning given the increasing role of telecommunication companies in facilitating cross-border financial transactions within the East African Community (EAC). Despite the growing importance of such initiatives, these efforts have yet to be adequately integrated into the legal and regulatory framework.

[88] A.M. Ally, Legal and regulatory framework for mobile banking in Tanzania, *International Journal of Law and Management Vol. 66 No. 1, Emerald Publishing Limited, 2024, pp. 44-60.*

In this complex legal environment, a thorough review of Tanzania's financial regulatory system is necessary. The current framework not only leaves significant gaps that increase risks for consumers but also fails to address the realities of a rapidly evolving financial ecosystem. Strengthening the regulatory oversight of non-bank-led mobile money services, ensuring the inclusion of crypto currency within the regulatory perimeter, and addressing cross-border remittance activities must all be priorities in order to mitigate risks and enhance consumer protection. A more coherent and comprehensive approach is essential for the sustainable development of FinTech in Tanzania, ensuring both innovation and security in the financial sector.[89]

Within Tanzania's current legal landscape, consumer protection faces significant challenges, particularly as laws addressing consumer rights in the FinTech sector remain fragmented. Key legislation, such as the Constitution of the United Republic of Tanzania, 1977 (specifically Articles 11, 14, and 18), offers broad consumer protection. Additionally, various statutes like the Fair Competition Act, 2003, the Bank of Tanzania Act, 2006, the Tanzania Communications Regulatory Authority (TCRA) Act, 2003, the Cybercrimes Act, 2015, the National Payment Systems Act, 2015, and the Electronic Transactions Act, 2015 aim to address specific areas. However, these laws do not comprehensively cover the unique challenges posed by FinTech innovations like mobile money (M-Money).

The rise of M-Money services presents a critical legal gap, as they fall outside traditional financial sector regulations. Telecommunications companies, which provide these services, are regulated by the TCRA rather than financial authorities, creating regulatory ambiguity. While the Bank of Tanzania (Financial Consumer Protection) Regulations, 2019, attempt to safeguard consumer rights within financial services, M-Money operations have exposed a legal void. This gap leaves M-Money consumers vulnerable to risks not adequately addressed by the current regulatory framework.

Further complicating consumer protection efforts is the inadequacy of laws like the Cybercrimes Act, 2015. Although the Act was established as a penal statute to criminalize offenses involving computer systems and Information and Communication Technologies (ICT), it falls short in addressing jurisdictional challenges in the digital realm. Part III of the Act, particularly Section 30(1),

[89] Ally, A.M. (2024). Legal and regulatory framework for mobile banking in Tanzania, International Journal of Law and Management Vol. 66 No. 1, Emerald Publishing Limited,pp. 44-60.

briefly touches on jurisdiction but lacks clarity and detail, failing to specify which courts have original jurisdiction over cybercrime cases. This ambiguity becomes problematic in the context of a virtual, global, and borderless FinTech environment where anonymity reigns, complicating the enforcement of laws across borders. Without clear jurisdictional guidance, Tanzanian courts may struggle to assert authority over complex cross-border cybercrimes, hindering effective legal proceedings.

The rise of Artificial Intelligence (AI) in FinTech further exacerbates these challenges. The Cybercrimes Act does not account for offenses that could emerge from the increasing integration of AI in financial systems. Autonomous systems can be exploited to commit various financial crimes, such as generating fraudulent transactions, automating phishing schemes, engaging in identity theft, and unlawfully harvesting personal data. These actions pose significant privacy risks and can result in severe financial and personal harm to consumers. These gaps in the legal framework underscore the urgent need for a more robust and forward-looking regulatory approach. A comprehensive strategy is essential to address the jurisdictional complexities inherent in cross-border FinTech activities and to mitigate the emerging threats posed by AI technologies. Strengthening legal provisions in these areas will be crucial in ensuring that consumer rights are adequately protected in an increasingly digital and interconnected financial landscape. Another significant legal challenge that jeopardizes consumer rights in the FinTech sector is the rapid growth of artificial intelligence (AI). While AI holds the potential to transform financial services by improving efficiency, accuracy, and expanding financial inclusion, it also introduces a range of risks within the regulatory landscape. One such risk is the ambiguity around accountability and liability when AI systems malfunction or cause unintended consequences.

Although Section 26 of the Electronic Transactions Act of 2015 attempts to establish the validity of contracts formed between individuals and interactive systems, the current legal framework is limited in scope. It addresses the initial formation of contracts but fails to extend its coverage to more complex issues arising from the deployment of autonomous agents in the financial sector. These autonomous systems, which can make decisions without human intervention, create new layers of uncertainty regarding liability. For instance, if an AI system causes financial loss due to an error in decision-making, who is held responsible? The developer of the system, the financial institution using it, or the AI itself?

This gap in the law raises important questions about consumer protection. As AI technologies become more sophisticated, the potential for errors or unintended outcomes also increases, making it critical for regulators to provide clear guidance on liability and accountability. The absence of such clarity not only threatens consumer rights but also undermines trust in AI-driven financial services. Moreover, this challenge is compounded by the global nature of FinTech, where different jurisdictions may have varying standards of regulation, creating inconsistencies that could further expose consumers to risks.

To address this issue, it is imperative for regulators to update existing legal frameworks to reflect the realities of AI in financial services. This might include creating provisions that assign liability in the case of harm caused by autonomous agents, as well as establishing safeguards to ensure transparency and accountability in the deployment of AI systems. In doing so, regulators can help strike a balance between fostering innovation in the FinTech sector and ensuring robust consumer protection.

6.0 Conclusion and Recommendations for Strengthening the Legal Framework

The evaluation of the legal framework for managing risks and security issues in mobile banking in Tanzania highlights both strengths and weaknesses. While the current laws and regulations establish a foundation for secure mobile banking transactions, significant gaps persist, particularly regarding consumer protection and trust in the sector. These gaps underscore the urgent need for specific regulations that directly address the unique challenges posed by the FinTech sector, which operates largely within a telecom-centric model. One key area requiring attention is the question of liability, especially in an era where autonomous agents and artificial intelligence (AI) are becoming integral to financial services. While AI adoption offers numerous advantages, such as increased efficiency and enhanced financial inclusion, it also introduces new challenges related to consumer risk. The lack of clear liability provisions when these technologies fail or act unpredictably puts consumers at risk. Therefore, it is crucial to establish clear legal standards that define liability in cases where AI systems and other automated technologies are involved in financial transactions.

Moreover, regular security audits of mobile banking platforms should be mandated to ensure that any vulnerabilities are identified and rectified promptly. Alongside this, public awareness campaigns are essential to educate

consumers about the potential risks and best practices for securing their mobile banking activities. This would help bolster trust in the system, encouraging broader adoption of mobile banking services.

Additionally, while the introduction of the Agent Banking Guidelines for Banks and Financial Institutions, 2017 was a positive step, these regulations do not cover financial activities conducted under non-bank-led models. This regulatory gap creates a significant loophole for consumers using mobile financial services offered by telecommunications companies. Without adequate legal protection in place, these consumers are left vulnerable to risks that are not adequately addressed by the existing regulatory framework. To remedy this, it is necessary to develop a legal instrument specifically targeting agent banking within the telecom-centric model. This would ensure that all participants in the mobile banking ecosystem, regardless of the platform they use, are afforded the same level of legal protection and security.