

	Global Journal of Arts Humanity and Social Sciences				
	ISSN: 2583-2034				
	Abbreviated key title: Glob.J.Arts.Humanit.Soc.Sci				
	Frequency: Monthly				
	Published By GSAR Publishers				
Journal Homepage Link: https://gsarpublishers.com/journal-gjahss-home/					
Volume - 6	Issue - 9	September 2026	Total pages 864-868	DOI: 10.5281/zenodo.23080606	

TECHNOLOGY-RELATED BANK FRAUD AND THE EFFECTIVENESS OF THE LEGAL FRAMEWORK IN TANZANIA

By

DR. FRANCISCO MWIZAMHOLYA¹, MARIAM OMAR²

[2nd Year LLM Student, St. Augustine University, Mwanza, Tanzania]



Article History

Received: 10- 09- 2026

Accepted: 28- 09- 2026

Published: 30- 09- 2026

Corresponding author

**DR. FRANCISCO
MWIZAMHOLYA**

Abstract

The rapid adoption of technology in the banking sector has changed the manner in which financial services are provided and accessed in Tanzania. Electronic and mobile banking have improved the speed and convenience of banking transactions, but they have also created opportunities for fraudulent activities involving digital systems and electronic financial transactions. Tanzania has enacted several laws relevant to combating such fraud, including the Banking and Financial Institutions Act, the Cybercrimes Act, the Electronic Transactions Act, the National Payment Systems Act and the Personal Data Protection Act. Despite these legal measures, technology-related bank fraud continues to raise legal and practical concerns, particularly in relation to prevention, detection, investigation, electronic evidence, identification of offenders, recovery of fraudulently obtained funds and protection of affected customers. This article examines the effectiveness of the existing legal framework in responding to technology-related bank fraud in Tanzania, with particular reference to CRDB Bank PLC and NMB Bank PLC in Mwanza Region. It argues that the principal difficulty does not arise from a complete absence of applicable laws, but from the fragmented nature of the framework and challenges surrounding its implementation and enforcement. The article therefore considers the need for greater legal coherence, institutional cooperation, effective handling of electronic evidence, stronger investigative capacity and improved mechanisms for protecting customers and recovering fraudulently obtained funds.

Keywords: Technology-related bank fraud, electronic banking, banking law, cybercrime, electronic transactions, Tanzania.

1. GENERAL OVERVIEW

The banking sector in Tanzania has gradually moved from conventional branch-based services to greater reliance on electronic and digital technologies. The introduction and expansion of automated teller machines, electronic funds transfers, payment cards, internet banking and mobile banking have made banking services more accessible and convenient.ⁱ These developments have also changed the nature of risks associated with banking transactions. Fraud can now be committed through electronic systems, unauthorized access to accounts, manipulation of banking credentials and other technology-based methods without requiring the physical presence of the offender at the bank or in direct contact with the victim.ⁱⁱ

The increasing use of technology in banking has consequently created legal questions concerning the ability of the existing legal framework to respond to new forms of fraudulent conduct. Traditional banking regulation was largely developed around conventional banking operations, whereas technology-based transactions involve electronic records, digital identities, remote access and transactions that may take place across different technological platforms. This creates particular difficulties where an alleged fraudulent transaction has to be investigated, attributed to a particular person and supported by reliable electronic evidence.ⁱⁱⁱ

Tanzania has responded to technological developments through several pieces of legislation. The Banking and Financial Institutions Act provides the principal legal framework for the



regulation and supervision of banking institutions. The Electronic Transactions Act provides a legal framework for electronic transactions and electronic records, while the Cybercrimes Act addresses various offences involving computer systems and data.^{iv} The National Payment Systems Act regulates payment systems, and the Personal Data Protection Act establishes legal requirements concerning the collection, processing, use and protection of personal data.^v

The existence of several applicable laws, however, does not necessarily mean that technology-related bank fraud can be effectively addressed. The legal response involves more than defining unlawful conduct and prescribing penalties. It also requires effective mechanisms for detecting suspicious transactions, preserving electronic evidence, identifying offenders, investigating fraudulent activities, tracing transferred funds and providing appropriate remedies to affected customers. Where these mechanisms do not operate effectively, the existence of legislation may provide limited practical protection to banks and their customers.^{vi}

The problem is particularly significant in relation to electronic and mobile banking transactions. Fraudulent transactions may occur within a short period and funds may be transferred through several accounts or payment channels before the fraud is detected. The investigation may therefore require cooperation between banking institutions, regulatory authorities and law-enforcement agencies. Delays in reporting, preservation of records or obtaining relevant information may make it more difficult to establish what occurred and to trace the funds involved.^{vii}

Customer protection also forms an important part of the legal problem. A customer whose account has been affected by a fraudulent electronic transaction may require an effective mechanism for reporting the incident, investigating the transaction and seeking recovery of the lost funds. Difficulties relating to compensation, investigation and privacy have been identified as continuing concerns in the context of fraudulent mobile banking transactions in Tanzania. The legal framework must therefore be examined not only from the perspective of criminal enforcement but also from the perspective of the rights and remedies available to customers.^{viii}

Another concern is the fragmented character of the applicable legal framework. Different aspects of technology-related bank fraud are addressed under different statutes and may involve different institutions. Banking regulation, payment systems, electronic transactions, cybercrime and personal data protection are therefore governed within separate legal and institutional areas. While specialization may be necessary, the absence of effective coordination can create difficulties where a single fraudulent transaction raises issues falling within several regulatory and legal frameworks.^{ix}

The practical implications of these concerns are relevant to commercial banks operating in Tanzania, including CRDB Bank PLC and NMB Bank PLC. The use of technology-based banking services by customers creates a need for effective mechanisms for

prevention, detection and response to fraudulent transactions. The focus on Mwanza Region provides a practical setting for examining how the legal framework operates at the level of banking institutions, regulators, legal practitioners and customers. The central issue, therefore, is not simply whether Tanzania has laws dealing with banking, electronic transactions and cybercrime. The more important question is whether these laws, together with the institutions responsible for their implementation, provide an effective response to the changing nature of technology-related bank fraud. The assessment must take into accounts the adequacy of the substantive law as well as the practical challenges of investigation, electronic evidence, institutional cooperation, attribution of responsibility, recovery of funds and protection of affected customers.^x

The need for such an assessment is reinforced by the continuing development of financial technology. As banking services become increasingly dependent on digital systems, the legal framework must remain capable of responding to methods of fraud that may not have been contemplated when some of the existing legislation was enacted. A legal framework that is adequate in relation to one form of technology-related fraud may require further development when new technologies, payment mechanisms and fraudulent techniques emerge. Against this background, this article examines the effectiveness of the Tanzanian legal framework in combating technology-related bank fraud, with particular attention to the legal and institutional challenges affecting its implementation. It further considers measures that may strengthen prevention, investigation, enforcement, customer protection and recovery of fraudulently obtained funds.

2. LEGAL FRAMEWORK GOVERNING TECHNOLOGY-RELATED BANK FRAUD IN TANZANIA

Technology-related bank fraud in Tanzania is not regulated by a single statute. Instead, protection is derived from several laws dealing with banking regulation, computer-related offences, electronic transactions, payment systems and personal data. This arrangement provides different forms of legal protection, but it also means that the response to a fraudulent transaction may involve more than one legal regime.

2.1 Banking and Financial Institutions Act, Cap. 342 R.E. 2023.

The Banking and Financial Institutions Act provides the principal statutory framework for the regulation and supervision of banking institutions in Tanzania. Its relevance to technology-related bank fraud arises partly from the requirements imposed on banking institutions concerning internal controls, risk management and the proper conduct of banking operations.^{xi}

The requirement for adequate internal controls is particularly important in a banking environment where transactions are increasingly conducted through electronic systems. Internal controls may include measures for controlling access to banking systems, monitoring transactions, maintaining records and

identifying irregular activities. The regulatory powers of the Bank of Tanzania further provide a mechanism through which compliance with applicable requirements can be supervised.^{xii} The Act, however, does not establish a separate and comprehensive offence described specifically as technology-related bank fraud. Its contribution is therefore principally regulatory and supervisory, while the criminal aspects of technology-based fraudulent conduct may be addressed under other legislation. This creates a situation in which effective protection depends upon the interaction between banking regulation and laws dealing with electronic and computer-related offences.^{xiii}

2.2 Cybercrimes Act, Act No. 14 of 2015.

The Cybercrimes Act, 2015 forms an important part of the criminal-law response to technology-related bank fraud. The Act creates offences involving computer systems and information and communication technologies, including computer-related fraud. This provides a legal basis for criminal prosecution where fraudulent conduct is committed through or involves a computer system.^{xiv} The Act is also important from an investigative perspective. Technology-related bank fraud frequently leaves electronic traces, including transaction records, computer data and other digital information. The law therefore provides investigative mechanisms relating to the acquisition, preservation and handling of electronic evidence in cybercrime investigations. Such mechanisms are important because the successful prosecution of technology-related fraud may depend upon establishing the connection between the electronic activity, the transaction and person responsible.^{xv}

2.3 Electronic Transactions Act, Cap. 442 R.E. 2023.

The Electronic Transactions Act provides legal recognition and regulation of electronic transactions, electronic communications, electronic records and electronic signatures. Its relevance to banking arises from the fact that modern banking transactions generate substantial amounts of electronic information.^{xvi} Recognition of electronic records is particularly important when a fraudulent transaction is investigated or becomes the subject of legal proceedings. Transaction records, electronic communications and other digital information may provide evidence concerning the occurrence and circumstances of a disputed transaction. The legal recognition of such records therefore contributes to certainty in electronic banking and provides a legal foundation for relying upon electronic information.^{xvii} The Act does not, however, operate as a complete legal response to technology-related bank fraud. Its principal concern is the legal environment for electronic transactions rather than the comprehensive regulation of fraudulent conduct within the banking sector. Consequently, fraudulent conduct may still require reliance on other statutes, particularly criminal and banking legislation.^{xviii}

2.4 National Payment Systems Act, Cap. 437 R.E. 2023.

The National Payment Systems Act provides another important component of the legal framework by regulating payment systems and payment service providers. This is significant because many technology-related bank fraud incidents involve electronic

movement of funds through payment systems. The regulatory framework for payment systems provides a basis for supervision and control of the mechanisms through which electronic payments are processed. It therefore contributes to reducing risks associated with unauthorized or improper transactions. The role of the Bank of Tanzania in overseeing payment systems further provides an institutional mechanism for maintaining regulatory standards within the payment environment.^{xix} Nevertheless, the effectiveness of payment-system regulation in cases of fraud may depend upon the speed with which suspicious transactions are detected and reported. Once funds have been transferred through electronic channels, delays in intervention may make tracing and recovery more difficult. The legal framework must therefore operate together with effective institutional procedures for reporting, freezing, tracing and recovering suspected fraudulent funds.

2.5 Personal Data Protection Act, 2022

The Personal Data Protection Act, 2022 provides an additional layer of protection relevant to technology-based banking. Banking institutions ordinarily process substantial amounts of personal and financial information in providing electronic banking services. The protection of such information is therefore closely connected with the prevention of unauthorized access and misuse of customers' information. The importance of data protection becomes more apparent where fraudulent transactions result from the unauthorized acquisition or misuse of customers' personal information. Appropriate protection of personal data may reduce opportunities for offenders to obtain information that can subsequently be used to compromise banking accounts or conduct unauthorized transactions.^{xx}

The Act should therefore be viewed as complementary to the banking, cybercrime and electronic transaction framework. It does not replace the criminal and regulatory mechanisms contained in other legislation, but addresses an important part of the environment within which technology-related bank fraud may occur.

2.6 The Combined Operation of the Legal Framework

The foregoing laws demonstrate that Tanzania has several legal mechanisms capable of addressing different aspects of technology-related bank fraud. Banking legislation provides regulatory and supervisory mechanisms; the Cybercrimes Act addresses computer-related criminal conduct; the Electronic Transactions Act provides legal recognition for electronic transactions and records; the National Payment Systems Act regulates payment systems; and the Personal Data Protection Act addresses the protection of personal information.^{xxi} The difficulty lies in ensuring that these legal mechanisms operate together effectively. A single fraudulent transaction may involve unauthorized access to personal information, manipulation of a computer system, movement of funds through a payment system and a dispute concerning the customer's liability or recovery of the money. Such a situation may require the application of several laws and the involvement of different institutions.^{xxii}

The effectiveness of the framework should therefore be assessed not merely by examining whether individual statutes contain relevant provisions, but by considering whether the different legal and institutional mechanisms provide a coherent response when technology-related bank fraud occurs. The findings of the study indicate that fragmentation, difficulties in investigation and electronic evidence, limited institutional capacity, inadequate coordination and challenges in recovering fraudulently obtained funds continue to affect the practical operation of the framework.^{xxiii}

3. PRACTICAL CHALLENGES AFFECTING THE EFFECTIVENESS OF THE LEGAL FRAMEWORK

Although Tanzania has several laws applicable to technology-related bank fraud, their practical implementation faces a number of challenges. The study identified difficulties in investigating fraudulent transactions, particularly where electronic evidence must be identified, obtained and preserved.^{xxiv} The increasing sophistication of technology also makes it difficult to identify offenders, especially where fraudulent activities are conducted remotely or through different technological platforms.^{xxv}

Another challenge concern limited institutional capacity. Effective investigation of technology-related bank fraud requires personnel with appropriate knowledge of digital investigation, electronic evidence and financial transaction tracing. Where such capacity is limited, the existence of legal powers may not necessarily result in effective enforcement.

The study also identified inadequate cooperation among banking institutions, regulatory authorities and law-enforcement agencies as a practical concern. Technology-related bank fraud may require timely exchange of information between different institutions, particularly when tracing suspicious transactions and identifying persons involved. Delays or weak coordination may reduce the possibility of preventing further loss and recovering fraudulently obtained funds.^{xxvi}

A further challenge concerns the recovery of funds obtained through fraudulent transactions. Electronic transfers may move funds rapidly between different accounts or payment channels, making timely intervention important. The effectiveness of the legal framework therefore depends not only on criminal investigation and prosecution but also on practical mechanisms for tracing and recovering the proceeds of fraud.

Finally, customer protection remains an important concern. Customers require accessible mechanisms for reporting suspicious transactions, receiving appropriate assistance and seeking recovery where unauthorized transactions occur.^{xxvii} The findings therefore indicate that strengthening the existing framework requires improvements in legal clarity, institutional capacity, inter-agency cooperation, electronic evidence management and mechanisms for customer protection and recovery of fraudulent funds.

4. LEGAL AND INSTITUTIONAL MEASURES FOR STRENGTHENING THE FRAMEWORK

The effectiveness of the legal framework can be improved by addressing the practical weaknesses that affect the detection, investigation, prosecution and recovery of technology-related bank fraud. One important measure is to improve coordination among the Bank of Tanzania, commercial banks, law enforcement authorities, prosecution authorities and other relevant institutions. Timely exchange of information is particularly important where fraudulent transactions involve several accounts, electronic platforms or different financial institutions.^{xxviii}

There is also a need to strengthen the capacity of institutions responsible for investigating and prosecuting technology-related bank fraud. Investigators, prosecutors and other relevant officials require practical skills in handling electronic evidence, tracing digital transactions, identifying offenders and preserving evidence in a manner that supports its use in criminal proceedings. Investment in digital forensic facilities and specialized training would therefore strengthen the practical application of the existing laws.^{xxix}

The legal framework should also provide clearer and more effective mechanisms for tracing, freezing and recovering funds obtained through fraudulent electronic transactions. In practice, recovery may become difficult where funds are transferred rapidly between different accounts or financial platforms. Clear procedures for early intervention and cooperation between banks and investigative authorities would assist in reducing such difficulties.^{xxx}

Customer protection should receive greater attention within the implementation of the framework. Banks should continue strengthening transaction-monitoring systems, customer awareness and accessible mechanisms for reporting suspicious or fraudulent transactions. Early reporting is particularly important because delays may reduce the possibility of tracing and recovering fraudulently transferred funds.^{xxxi}

Finally, periodic review of the existing laws and regulatory measures is necessary because technology-related financial fraud continues to develop alongside changes in banking technology. Legal review should focus on coherence between the relevant statutes, electronic evidence, institutional responsibilities, investigation and prosecution procedures, liability, customer protection and recovery of fraudulent funds. Strengthening these areas would improve the practical capacity of the existing framework without relying solely on the creation of additional offences or legislation.

END NOTES

ⁱ Charles Ishengoma Kato, "Legal Framework Challenges to E-Banking in Tanzania," PSU Research Review, Vol. 3, No. 2, pp. 101-110.

- ⁱⁱ Rosemary Jotham Mukama, “Electronic Banking and Technological Development in Tanzania: A Legal Analysis,” Ruaha Law Review, Vol. 2, No. 2.
- ⁱⁱⁱ Electronic Transactions Act, Cap. 442 R.E. 2023; Cybercrimes Act, Act No. 14 of 2015.
- ^{iv} Electronic Transactions Act, Cap. 442 R.E. 2023; Cybercrimes Act, Act No. 14 of 2015.
- ^v National Payment Systems Act, Cap. 437 R.E. 2023; Personal Data Protection Act, 2022.
- ^{vi} Caroline A. Mutalemwa and John Ubena, “Are the Customers’ Rights Protected Against Fraud in Mobile Banking in Tanzania? A Review of the Laws and Practice,” Institute of Judicial Administration Journal, Vol. 6, No. 1, pp. 72-89.
- ^{vii} Ismail Emmanuel Msengi, “The Role of Law Enforcement in Combating Financial Cybercrime in Tanzania: Examining the Laws and Practice,” East African Journal of Law and Ethics, Vol. 7, No. 1, pp. 202-213.
- ^{viii} Mutalemwa and Ubena, above n 8, pp. 72-89.
- ^{ix} Banking and Financial Institutions Act, Cap. 342 R.E. 2023; Cybercrimes Act, Act No. 14 of 2015; Electronic Transactions Act, Cap. 442 R.E. 2023; National Payment Systems Act, Cap. 437 R.E. 2023; Personal Data Protection Act, 2022.
- ^x Ibid.
- ^{xi} Banking and Financial Institutions Act, Cap. 342 R.E. 2023, Section 23.
- ^{xii} Ibid.
- ^{xiii} Ibid.
- ^{xiv} Cybercrimes Act, Act No. 14 of 2015, Section 13.
- ^{xv} Ibid.
- ^{xvi} Electronic Transactions Act, Cap. 442 R.E. 2023.
- ^{xvii} Ibid.
- ^{xviii} Ibid; Cybercrimes Act, Act No. 14 of 2015.
- ^{xix} National Payment Systems Act, Cap. 437 R.E. 2023.
- ^{xx} Personal Data Protection Act, 2022.
- ^{xxi} Banking and Financial Institutions Act, Cap. 342 R.E. 2023; Cybercrimes Act, Act No. 14 of 2015; Electronic Transactions Act, Cap. 442 R.E. 2023; National Payment Systems Act, Cap. 437 R.E. 2023; Personal Data Protection Act, 2022.
- ^{xxii} Marium Omar, An Assessment of the Effectiveness of the Legal Framework in Combating Technology-Related Bank Fraud in Tanzania: A Case Study of CRDB Bank PLC and NMB PLC in Mwanza Region (LL.M Dissertation, St Augustine University of Tanzania, 2026).
- ^{xxiii} Ibid.
- ^{xxiv} Ibid.
- ^{xxv} Ibid.
- ^{xxvi} Ibid.
- ^{xxvii} Caroline A. Mutalemwa and John Ubena, “Are the Customers’ Rights Protected Against Fraud in Mobile Banking in Tanzania? A Review of the Laws and Practice,” Institute of Judicial Administration Journal, Vol. 6, No. 1, pp. 72-89.

- ^{xxviii} M. Omar, An Assessment of the Effectiveness of the Legal Framework in Combating Technology-Related Bank Fraud in Tanzania: A Case Study of CRDB Bank PLC and NMB PLC in Mwanza Region (LL.M Dissertation, St Augustine University of Tanzania, 2026).
- ^{xxix} Msengi, ‘The Role of Law Enforcement in Combating Financial Cybercrime in Tanzania: Examining the Laws and Practice’ (2024) 7(1) East African Journal of Law and Ethics 202-213.
- ^{xxx} Ibid.
- ^{xxxi} Mutalemwa and Ubena, ‘Are the Customers’ Rights Protected Against Fraud in Mobile Banking in Tanzania? A Review of the Laws and Practice’ (2023) 6(1) IJA Journal 72-89.