American Journal of
Finance
(AJF)

A Review of the Role of Risk Management in Online Transactions: The Growing Issues of Network and System Security among Zambia's Financial Institutions

Gerry Mutibo Siampondo & Professor Mbuyu Sumbwanyambe

American Journal of Finance
ISSN 2520-0445 (Online)
Vol. 8, Issue 2, pp 1 - 12, 2023

www.ajpojournals.org

A Review of the Role of Risk Management in Online Transactions: The Growing Issues of Network and System Security among Zambia's Financial Institutions

Gerry Mutibo Siampondo[1*] & Professor Mbuyu Sumbwanyambe[2]
[1]Liquid Intelligent Technologies, Department of Customer Experience, Longacres, Lusaka 10101, Zambia
[2]University of South Africa, Department of Electrical Engineering, 11 Conblair, 69 Conrad Drive Blairgowrie Randburg 2194, South Africa
*Corresponding Author's Email: Gerry.mweemba@liquid.tech
Co-Author's Email: sumbwm@unisa.ac.za

Article history

Submitted 15.06.2023 Revised Version Received 21.06.2023 Accepted 23.06.2023

Abstract

Purpose: The present study offers an all-encompassing analysis of the significance of risk management in the context of online transactions, with a particular emphasis on the escalating concerns regarding network and system security within the financial institutions of Zambia.

Methodology: The research utilized a mixed-methods design, integrating an extensive review of relevant literature with an examination of primary data obtained through interviews with significant stakeholders.

Findings: The results underscore the significance of proficient risk management tactics in alleviating the susceptibilities linked with internet-based transactions, specifically within the financial industry of Zambia. This discourse delves into monetary establishments' obstacles in securing their networks and systems and the possible consequences of insufficient risk management methodologies.

Unique Contribution to Theory, Practice and Policy: The paper draws conclusions from the findings and suggests recommendations to improve risk management frameworks and bolster network and system security in online transactions in the financial sector of Zambia. The study was validated using a mixed-methods design, combining a comprehensive literature review with primary data obtained through interviews with significant stakeholders. This approach allowed the researchers to gather insights from existing knowledge and perspectives from relevant individuals involved in the financial institutions of Zambia. The exponential expansion of digital commerce has presented many obstacles for financial establishments operating in Zambia. One of contemporary society's foremost challenges is the increasingly salient problem of network and system security. It is because online transactions are frequently more susceptible to cyber threats than conventional offline transactions. Consequently, it is imperative for financial institutions operating in Zambia to undertake measures to enhance their risk management strategies to safeguard their clients and commercial operations. The effective management of risks associated with online transactions is a critical concern for financial institutions in Zambia. Robust network and system security measures are essential to mitigate potential threats and vulnerabilities.

Keywords: *Risk Management, Online Transactions, Network Security, System Security, Financial Institutions, Zambia.*

1.0 INTRODUCTION

Over the past few years, there has been a growing prevalence of online transactions across diverse industries, including the financial domain. The proliferation of digital platforms and the expansion of e-commerce have fundamentally transformed how financial transactions are executed, providing customers with enhanced convenience and efficacy (Neene et al., 2023). The swift proliferation of online commerce has ushered in novel hazards and complexities, particularly in network and system security (Kollmer et al., 2023). Like their counterparts in other nations, financial institutions operating in Zambia face various risks, encompassing cyberattacks and data breaches. This study aims to analyze the significance of risk management in mitigating the challenges mentioned earlier and suggest measures for improving network and system security in online transactions in the financial sector of Zambia (Anwer et al., 2023). The financial services industry has witnessed a notable surge in online transactions, making it a noteworthy trend in recent times. E-commerce transactions benefit customers and enterprises through enhanced convenience, swiftness, and reduced expenses. Notwithstanding the convenience of online transactions, they also entail several hazards, such as the possibility of fraudulent activities, identity theft, and cyber assaults.

The escalation of digital transactions has been notably swift in Zambia within the past few years. This phenomenon can be attributed to several factors, such as the proliferation of broadband internet, the widespread adoption of smartphones, and the surging demand for mobile banking solutions. Zambian financial institutions currently need help with network and system security. The risk of fraud has become increasingly prominent as perpetrators utilize a range of strategies such as phishing, malware, and social engineering to manipulate and take advantage of individuals unaware of their schemes (Ojeniyi et al., 2019). Identity theft is a prevalent hazard that entails the unapproved utilization of purloined personal data to perpetrate deceitful actions. The escalating apprehensions for financial institutions encompassed cyberattacks, including hacking, denial-of-service attacks, and data breaches. The inadequacy of resources allocated towards training and awareness programs has been identified as contributing to the vulnerability of institutions and their employees (Money et al., 2021. The need for more cooperation and exchange of information among industry participants underscored the impediment to devising comprehensive risk management strategies.

At the global level, there is a significant increase in online transactions across various industries, including finance. This trend is driven by factors such as advancements in technology, increased internet penetration, and the widespread adoption of digital platforms. The convenience, speed, and efficiency offered by online transactions have made them increasingly popular among consumers and businesses worldwide. However, according to Homann-Kee Tui, et al. (2023) this global shift towards online transactions has also led to an escalation in risks and challenges related to network and system security. Cyberattacks, data breaches, and fraud attempts have become more prevalent, targeting both individuals and organizations. The global financial sector is particularly vulnerable to these risks due to the sensitive nature of financial transactions and the value of the assets involved. At the regional level, the situation may vary based on factors such as technological infrastructure, internet penetration rates, regulatory frameworks, and economic development. In the case of Zambia, as mentioned in the previous passage, there has been a notable surge in online transactions within the past few years. This growth can be attributed to factors like the proliferation of broadband internet, widespread smartphone adoption, and increased demand

for mobile banking solutions. However, along with the expansion of online transactions, Zambia, like other regions, also faces challenges related to network and system security. Cyberattacks, data breaches, identity theft, and fraud attempts pose significant risks to financial institutions and their customers. The passage highlights the need for improved risk management strategies and enhanced network and system security measures in the financial sector of Zambia.

2.0 METHODOLOGY

The present study is grounded on a comprehensive analysis of the extant literature pertaining to risk management in the context of online transactions, as well as the escalating concerns surrounding network and system security within the financial institutions of Zambia. The literature review utilized diverse sources such as scholarly journals, industry reports, and government publications. The present research used a mixed-methods design to examine the function of risk management in online transactions and the obstacles encountered by financial institutions in Zambia. A thorough examination of the literature was undertaken to collect data on optimal methodologies and established frameworks for managing risks in electronic transactions. The review encompassed scholarly publications, industry analyses, and regulatory directives. The purpose of conducting the literature was to obtain valuable insights pertaining to the current practices of risk management, detect any vulnerabilities, and examine plausible strategies that could be implemented to augment the security of the network and system.

3.0 FINDINGS

The study's results illuminate the importance of risk management in online transactions in the financial sector of Zambia. Miti, et al. (2023) indicate that financial institutions are being subjected to advanced cyberattacks with greater frequency. It resulted in significant financial losses, damage to reputation, and a loss of trust among customers. These include insufficient cybersecurity infrastructure, restricted resources for training and awareness initiatives, and a need for more cooperation and knowledge exchange among industry participants (Kpodar & Andrianaivo, 2011). Moreover, prevailing risk management frameworks frequently fall short of tackling nascent hazards and susceptibilities linked with digital transactions. Financial institutions operating in Zambia must accord utmost importance to deploying resilient risk management tactics to tackle the aforementioned obstacles and bolster the security of networks and systems. Implementing robust security measures is pivotal in safeguarding networks and systems against cyber threats (Ge et al., 2022). The previous standards encompass the utilization of firewalls, intrusion detection systems, and encryption technologies. Firewalls function as a protective shield separating internal networks from external sources, thwarting unauthorized entry and the proliferation of malicious software. Intrusion detection systems are designed to oversee network traffic to identify any anomalous activities and subsequently issue alerts in the event of possible security breaches. Encryption technologies guarantee the secure encoding of sensitive data during transmission between systems, rendering it arduous for unauthorized individuals to intercept or decipher the information. Implementing these security measures can enhance the integrity of the networks and systems of financial institutions.

An essential aspect of risk management involves imparting knowledge to employees regarding the potential hazards linked with online transactions and the measures to safeguard themselves and the organization against fraudulent activities and identity theft. It is recommended that financial institutions allocate resources toward implementing training and awareness initiatives aimed at

bolstering the role of the human factor in the context of risk management. It is imperative to provide employees with proper training regarding optimal methods for managing confidential customer information, identifying phishing endeavors, and comprehending their responsibilities in preserving network and system security. Institutions can effectively mitigate the risk of security breaches caused by human error by fostering a culture of security awareness and vigilance (Brockmann-Hosseini et al., 2023). The surveillance of transactions to detect indications of fraudulent or dubious behavior is an additional crucial element of professional risk mitigation. Financial institutions must establish mechanisms for monitoring and scrutinizing transactional data, which would facilitate the identification of irregularities and the detection of possible occurrences of fraudulent activities. Institutions can reduce potential financial losses and safeguard their customers from fraudulent transactions by expeditiously detecting and addressing suspicious activities. The successful execution of this task necessitates the integration of sophisticated technologies, resilient data analytics competencies, and specialized teams for scrutinizing transactions and conducting inquiries (Siangulube et al., 2023). Malambo (2022), findings indicate several potential hazards linked to online transactions exist. One of the prevalent risks related to online transactions is fraudulence. Perpetrators may employ diverse tactics to unlawfully obtain individuals' funds, such as phishing schemes, malware, and social manipulation. Identity theft is a prevalent hazard linked with online transactions. Stealing personal information can enable identity thieves to engage in illicit activities, such as opening new accounts, making unauthorized purchases, and perpetrating other criminal acts. The incidence of cyberattacks poses an escalating threat to financial institutions. Cybercriminals can employ diverse methods to target financial institutions, such as hacking, denial-of-service attacks, and data breaches.

The prevalence of online transactions has recently surged, albeit with a concomitant increase in the potential hazards that financial institutions may encounter. The potential hazards encompass fraudulent activities, identity misappropriation, and cyber assaults. Online transactions are frequently exposed to the risk of fraudulent activities, which is considered one of the most prevalent hazards. Perpetrators of financial fraud can employ diverse tactics to unlawfully obtain funds from individuals, such as phishing schemes, malicious software, and manipulation of human behavior. Phishing attacks refer to fraudulent attempts to get sensitive information, such as login credentials and financial details, by disguising as trustworthy entities, such as banks or credit card companies, through emails or text messages. Frequently, electronic communications such as emails or text messages comprise a hyperlink that, upon activation, redirects the recipient to a counterfeit website that bears a striking resemblance to the authentic website. The perpetrator can illicitly appropriate it upon submitting their personal information on the fake website. Malware refers to a type of software that has been specifically created to cause damage to a computer system (Mwiya et al., 2022). The installation of malware onto a computer system can occur through multiple avenues, including but not limited to the act of clicking on a malicious link, opening an attachment that has been infected, or downloading a file from a source that is not deemed trustworthy. Upon installation, malware can exfiltrate personal data, impair files, and potentially commandeer the entire computer system. Social engineering refers to a cyberattack whereby perpetrators employ deceptive tactics to obtain confidential information from unsuspecting individuals. Several methods can be used to get personal information, including but not limited to impersonating a customer service representative, soliciting personal information via telephone, or sending a persuasive email requesting personal information. Hacking is a form of cyber assault wherein malevolent actors illicitly obtain entry to a computer system or network without proper

authorization. Upon infiltrating a computer system or network, hackers can purloin personal data, impair files, or potentially usurp the system (Kumar et al., 2021). Denial-of-service attacks refer to cyberattacks whereby malevolent actors inundate a website or server with excessive traffic, rendering it inaccessible to authorized users. This can be achieved by flooding a website or server with substantial requests or leveraging a botnet to execute the same action (Adefemi Alimi et al., 2022). Data breaches refer to occurrences where confidential information is disclosed to unauthorized parties. There are several potential causes for such an occurrence, including but not limited to a cyber intrusion, a lapse in human judgment, or an act of nature. In a data breach, unauthorized parties may compromise and access confidential information such as personal and financial data (Gopi et al., 2022). Financial institutions must recognize these risks and implement measures to alleviate them. Implementing robust security protocols, providing employee training, and monitoring transactions for indications of fraudulent or anomalous behavior are effective measures for achieving this objective.

Discussion

The discussion section delves into the challenges identified in the findings. It underscores the significance of employing proactive risk management strategies to alleviate the risks linked to online transactions in the financial institutions of Zambia. The text explores the importance of implementing robust cybersecurity protocols, providing comprehensive employee training and awareness programs, fostering collaboration among relevant parties, and considering the potential consequences of insufficient risk management strategies. Financial institutions encounter a significant obstacle in establishing robust security protocols to safeguard their networks and systems against cyber threats. Institutions must implement a comprehensive and resilient cybersecurity infrastructure to effectively mitigate the constantly changing landscape of substructures (Dimolianis, 2022). The implementation of firewalls, intrusion detection systems, and encryption technologies are encompassed within this context. Firewalls function as a protective shield that separates internal networks from external sources, thereby mitigating the risk of unauthorized entry and the proliferation of malicious software. Intrusion detection systems are designed to oversee the network, identify anomalous activities, and notify relevant parties of potential security breaches. Encryption technologies guarantee the secure encoding of sensitive data during transmission between systems, rendering it arduous for unauthorized individuals to intercept or decipher the information. Security measures are paramount in protecting networks and systems against possible breaches and unauthorized access.

A crucial element of risk management involves imparting knowledge to the employees regarding the potential hazards related to online transactions and the measures to safeguard themselves and the organization against fraudulent activities and identity theft. It is recommended that financial institutions prioritize the implementation of training and awareness programs to strengthen the role of the human factor in risk management. Employees must receive proper training on optimal methods for managing confidential customer information, identifying and thwarting phishing schemes, and comprehending their responsibility to preserve networks and systems' security. Institutions can effectively mitigate the probability of security breaches caused by human error by fostering a culture that prioritizes security awareness and vigilance (Haabazoka, 2019). The surveillance of transactions to detect indications of fraudulent or dubious behavior is an essential element of professional risk management. Financial institutions must establish mechanisms for monitoring and scrutinizing transactional data, which would facilitate the identification of

irregularities and the detection potential fraudulent activities. Institutions can reduce potential financial losses and safeguard their customers from fraudulent transactions by expeditiously detecting and addressing suspicious activities. The successful implementation of this task necessitates the integration of cutting-edge technologies, professional data analysis competencies, and specialized personnel to scrutinize transactions and conduct inquiries.

Financial institutions must establish a comprehensive strategy to address and mitigate cyberattack impacts effectively. The proposed plan should delineate the measures to be implemented during a security breach, encompassing incident response, recuperation protocols, and communication tactics. Institutions can mitigate the impact of a cyberattack and expedite a successful recovery by implementing a clearly defined incident response plan. It is imperative to conduct routine testing and simulations of the technique to detect any deficiencies or opportunities for enhancement, thereby facilitating immediate modifications to optimize its efficacy. Effective risk management in online transactions necessitates collaboration among financial institutions, regulatory bodies, and other stakeholders (de Luna-Martinez, 2012). Exchanging information, knowledge, and personal encounters among institutions facilitates the enhancement of network and system security in a collaborative manner. Creating collaborative platforms and information-sharing mechanisms promotes the transfer of knowledge and the advancement of optimal methodologies. It is recommended that financial institutions proactively participate in industry associations, forums, and partnerships as a means of remaining abreast of emerging threats, trends, and regulatory mandates. Collaborative endeavors may encompass cooperative undertakings to mitigate cyber hazards, including exchanging threat intelligence, synchronizing incident response, and executing joint cybersecurity drills.

The imperative facet of risk management in online transactions is the collaboration among financial institutions, regulatory bodies, and other stakeholders. Exchanging information, knowledge, and personal encounters among institutions facilitates the enhancement of network and system security in a collaborative manner (Davradakis & Santos, 2019). Creating collaborative platforms and information-sharing mechanisms enables the transfer of knowledge and the advancement of optimal methodologies. It is recommended that financial institutions proactively participate in industry associations, forums, and partnerships to remain informed about emerging threats, trends, and regulatory obligations. Collaborative endeavors may also encompass cooperative initiatives to counter cyber threats, such as exchanging threat intelligence, synchronizing incident response, and executing joint cybersecurity drills. Financial institutions may face severe consequences due to insufficient risk management practices in online transactions (Aurick et al., 2017). With comprehensive risk management measures, organizations can avoid financial losses resulting from fraudulent activities, harm to their reputation, failure to comply with regulatory requirements, and declining customer confidence. The above outcomes can substantially affect the organization's financial performance, impede its capacity to allure and maintain clientele and result in legal and regulatory ramifications. Hence, it is imperative that financial institutions prioritize risk management, allocate resources, and implement strategies necessary to safeguard their networks, systems, and customer data.

Financial institutions in Zambia must implement efficient risk management strategies for online transactions. Institutions can effectively reduce the risks associated with online transactions by implementing robust security measures, educating employees, closely monitoring transactions, promoting stakeholder collaboration, and investing in comprehensive risk management strategies.

The ever-evolving nature of cyber threats necessitates a perpetual assessment and adjustment of risk management methodologies. Through risk management prioritization, financial institutions in Zambia's financial sector can safeguard their clients, uphold their reputations, and sustain the integrity of online transactions (Nuwagaba & Brighton, 2014). Insufficient risk management practices in online transactions can seriously affect financial institutions. With effective risk management strategies, organizations can avoid financial losses resulting from fraudulent activities, damage to reputation, non-compliance with regulatory requirements, and declining customer confidence. The above outcomes can significantly affect the organization's financial performance, impede its capacity to draw and retain clientele and result in legal and regulatory ramifications. Hence, it is imperative that financial institutions prioritize risk management, allocate resources, and implement strategies necessary to safeguard their networks, systems, and customer information. Financial institutions in Zambia must implement efficient risk management strategies for online transactions. Institutions can effectively reduce the risks associated with online transactions by adopting robust security measures, providing comprehensive employee training, closely monitoring transactions, establishing a clearly defined incident response plan, and promoting stakeholder collaboration. Recognizing the dynamic nature of cyber threats and the consequent adaptation of risk management practices are crucial imperatives for financial institutions. In Zambia's financial sector, institutions can safeguard their customers, uphold their reputations, and ensure the integrity of online transactions by giving precedence to risk management.

4.0 CONCLUSION AND RECOMMEDNATIONS

Conclusion

The present study offers an all-encompassing analysis of the significance of risk management in the context of online transactions, with a particular emphasis on the escalating concerns regarding network and system security within the financial institutions of Zambia. The results emphasize the significance of deploying efficient risk management tactics to alleviate the susceptibilities linked with virtual transactions (Malambo, 2022). Enhancing network and system security can be achieved through critical measures such as reinforcing cybersecurity infrastructure, allocating resources towards training and awareness programs, and promoting collaboration among industry players and regulatory bodies. By adopting prescribed methodologies, financial establishments in Zambia can enhance the security of their networks and systems, guaranteeing the integrity and reliability of digital transactions. The proliferation of digital transactions has presented various obstacles for financial institutions operating in Zambia. Financial institutions must implement measures to enhance risk management practices to safeguard their clients and enterprises. Financial institutions can improve their risk management practices by adopting robust security measures, providing comprehensive training to their staff, closely scrutinizing transactions, and devising contingency strategies to address potential cyber threats.

Recommendations

The present review has led to the formulation of recommendations to bolster risk management frameworks and augment network and system security in online transactions within Zambia's financial sector.

1. Financial institutions are recommended to allocate resources toward establishing a resilient cybersecurity infrastructure, which encompasses advanced technologies such as firewalls,

intrusion detection systems, and encryption mechanisms (Habanyati, 2022). Implementing these measures is expected to enhance the security of networks and systems by mitigating the risk of potential breaches and unauthorized access.

2. It is recommended that financial institutions prioritize cybersecurity training and awareness programs for their employees to enhance their efficacy. This entails training personnel on optimal methodologies for managing confidential customer information, identifying phishing schemes, and comprehending their responsibilities in upholding network and system security.
3. To promote collaboration and information sharing, it is recommended to create platforms that facilitate such activities among financial institutions, regulatory bodies, and other relevant stakeholders. This enables sharing of information and perspectives and developing risks to collaboratively enhance network and system security throughout the sector.
4. It is recommended that financial institutions establish and maintain comprehensive incident response plans to address cyber incidents adequately. These plans should be periodically reviewed and tested to ensure their effectiveness (Andrianaivo & Kpodar, 2011). Conducting routine assessments and simulations of these strategies can aid in detecting possible deficiencies and opportunities for enhancement.
5. Multifactor authentication (MFA) is recommended for financial institutions to secure access to their online transaction systems. MultifactorMultifactor authentication (MFA) enhances security measures by necessitating users to furnish multiple forms of identification, including a password and a specific token or biometric authentication.
6. Performing periodic security audits is crucial to evaluate the efficiency of current risk management protocols and detect any susceptibilities or deficiencies in the network and system security framework. The performance of audits can be carried out either internally or by third-party professionals specialized in cybersecurity.
7. Financial institutions must remain vigilant and apprised of developing cybersecurity threats, patterns, and regulatory mandates. To stay abreast of the latest developments in the field of cybersecurity, it is imperative to engage in a range of activities, such as regularly perusing industry publications, attending pertinent conferences and seminars, and actively participating in cybersecurity communities.
8. Financial institutions are recommended to establish unambiguous channels to facilitate reporting and disseminating information about cybersecurity incidents. Implementing this measure will expedite reactions and streamline collaborative endeavors to reduce potential hazards and preempt future occurrences.
9. It is recommended that financial institutions conduct routine security awareness campaigns to inform their customers about optimal online transaction security practices. This entails offering direction on the secure management of passwords, identifying possible fraudulent schemes, and reporting questionable actions.
10. It is recommended that financial institutions adopt continuous monitoring systems to identify and address potential security threats promptly. This approach enables real-time detection and response to such threats. Conducting routine risk assessments to detect emerging vulnerabilities and modify risk management tactics accordingly is imperative.

Implementing these recommendations has the potential to bolster the risk management frameworks of financial institutions in Zambia and fortify the security of networks and systems in online transactions. The aforementioned action is poised to facilitate the establishment of trust between customers and financial institutions, minimize the likelihood of financial losses, and preserve the reputation of the financial industry in its entirety.

REFERENCES

Adefemi Alimi, K. O., Ouahada, K., Abu-Mahfouz, A. M., Rimer, S., & Alimi, O. A. (2022). Refined LSTM Based Intrusion Detection for Denial-of-Service Attack in Internet of Things. Journal of Sensor and Actuator Networks, 11(3), 32.

Anwer, S. A., Hamad, H. A., Ibrahim, H. K., Gardi, B., Hamza, P. A., Othman, R. N., ... & Hamad, K. Q. (2023). The Role of Credit Risk Management in Performance of Commercial Banks: Analysis of Commercial banks' Performance in Erbil. QALAAI ZANIST JOURNAL, 8(2), 1172-1193.

Aurick, M., Munalula, M., Mundia, L., Mwale, N. S., & Vincent, K. (2017). Urban informality and small scale enterprise (SME) development in Zambia: an exploration of theory and practice. Journal of Behavioural Economics, Finance, Entrepreneurship, Accounting and Transport, 5(1), 19-29.

Andrianaivo, M., & Kpodar, K. (2011). ICT, financial inclusion, and growth: Evidence from African countries.

Brockmann-Hosseini, N., Jell-Ojobor, M., & Windsperger, J. (2023). Market Entry Through Multilateral Networks in Developing Countries: The Case of Public–Private Development Partnership in Zambia. In Networks in International Business: Managing Cooperatives, Franchises and Alliances (pp. 279-307). Cham: Springer International Publishing.

Chellappa, R. K. (2008). Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security. under submission, 13.

de Luna-Martinez, J. (2012). Access to financial services in Zambia (Vol. 4061). World Bank Publications.

Davradakis, E., & Santos, R. (2019). Blockchain, FinTechs and their relevance for international financial institutions (No. 2019/01). EIB Working Papers.

Dimolianis, M. (2022). Intelligent Services for Detection and Mitigation of Distributed Denial-of-Service Attacks in Programmable Network Environments..

Gopi, A. P., Gowthami, M., Srujana, T., Gnana Padmini, S., & Durga Malleswari, M. (2022). Classification of Denial-of-Service Attacks in IoT Networks Using AlexNet. In Human-Centric Smart Computing: Proceedings of ICHCSC 2022 (pp. 349-357). Singapore: Springer Nature Singapore.

Ge, X., Han, Q. L., Wu, Q., & Zhang, X. M. (2022). Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks. IEEE/CAA Journal of Automatica Sinica.

Haabazoka, L. (2019). A study of the effects of technological innovations on the performance of commercial banks in developing countries-A case of the zambian banking industry. In The Future of the Global Financial System: Downfall or Harmony 6 (pp. 1246-1260). Springer International Publishing.

Habanyati, H. (2022). Lived experiences of multi-banked bank account holders with a focus on banks at Manda hill mall Lusaka, Zambia (Doctoral dissertation, The University of Zambia).

Homann-Kee Tui, S., Kakwasha, K., Wilkinson, M., Chongo, C., Zulu, S., Mubanga, C., ... & Jacobs-Mata, I. (2023). Impact of CSA technology packages on smallholder farmers under the accelerator program in Zambia.

Kpodar, M. K., & Andrianaivo, M. (2011). ICT, financial inclusion, and growth: Evidence from African countries. International Monetary Fund.

Kollmer, T., Durani, K., Peterhänsel, F., Eckhardt, A., & Augustin, N. (2023). Exploring Consumers Risk Mitigation Strategies in E-Commerce: A Qualitative Study of High-Risk Transactions.

Kumar, A. A., Prabhu, M., & Anbazhagan, A. (2021). ARTIFICIAL INTELLIGENCE PERFORMANCE-A CASE STUDY IN INVESTRUST BANK PLC, ZAMBIA. Annamalai International Journal of Business Studies & Research, 13(1).

Khiaonarong, T. (2014). Oversight issues in mobile payments. International Monetary Fund.

Malambo, J. N. (2022). A critical review of digital innovations challenges on customer satisfaction among financial institutions in Zambia: a case study of Stanbic bank Zambia, Lusaka (Doctoral dissertation, The University of Zambia).

Money, A., Carew-Jones, G., Rowley, L., Grey, J., Daka, R., Ching'ambo, L., ... & Ndiili, N. (2023). Mobilising investment for climate-compatible growth through Zambia's Constituency Development Fund. Climate Compatible Growth Programme.

Mwiya, B., Katai, M., Bwalya, J., Kayekesi, M., Kaonga, S., Kasanda, E., ... & Mwenya, D. (2022). Examining the effects of electronic service quality on online banking customer satisfaction: Evidence from Zambia. Cogent Business & Management, 9(1), 2143017.

Miti, J. J., Perkiö, M., Metteri, A., & Atkins, S. (2023, May). Implementing a Public Policy to Extend Social Security to Informal Economy Workers in Zambia. In Forum for Development Studies (pp. 1-19). Routledge.

Neene, V., Chembe, C., Phiri, M., Jere, B. E., & Kalunga, P. (2023). Challenges of Crowdfunding (Village Banking) in Zambia: Solutions and Opportunities.

Nuwagaba, A., & Brighton, N. (2014). Analysis of e-banking as a tool to improve banking services in Zambia. International Journal of Business and Management Invention, 3(11), 2319-8028.

Ojeniyi, J. A., Edward, E. O., & Abdulhamid, S. M. (2019). Security risk analysis in online banking transactions: Using diamond bank as a case study. International Journal of Education and Management Engineering, 9(2), 1-14.

Siangulube, F. S., Ros-Tonen, M. A., Reed, J., Djoudi, H., Gumbo, D., & Sunderland, T. (2023). Navigating power imbalances in landscape governance: A network and influence analysis in southern Zambia. Regional Environmental Change, 23(1), 41.