International Journal of Scientific Research and Management (IJSRM)
||Volume||13||Issue||05||Pages||111-117||2025||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v13i05.as01

Factors That Influence the Uptake of an M-Pesa Security System among Mpesa Agents In Nairobi County

Irene Sitawa Sichangi

Africa Nazarene University, Kenya

Abstract

This study investigates factors influencing the adoption of an enhanced M-PESA security system among agents in Nairobi County, amidst growing concerns about vulnerabilities in mobile payment systems. With mobile commerce thriving globally, particularly in developing regions, the integration of robust security measures becomes paramount. The focus on M-PESA, a dominant player in the mobile money market, suggests the urgency of fortifying transactional security to prevent fraud and unauthorized access, challenges accentuated by the reliance on basic authentication methods like PINs. Utilizing the Technology Acceptance Model (TAM) as the theoretical framework, this research examines the impact of perceived vulnerability, response cost, response efficacy, self-efficacy, and both intrinsic and extrinsic rewards on security system uptake. The methodology involved a predictive correlational study design, gathering data from 375 M-PESA agents in Nairobi via structured questionnaires, ensuring a representative sample through a clustered sampling approach. Regression analysis was employed to quantify the influence of each factor. Results indicate that perceptions of vulnerability and personal confidence (self-efficacy) in handling security measures significantly predict the willingness to adopt enhanced security solutions. Interestingly, intrinsic rewards influenced adoption positively, reflecting a motivation rooted in personal satisfaction and responsibility, while extrinsic rewards and perceived response efficacy showed no significant impact. These findings suggest that enhancing M-PESA agents' self-efficacy and addressing their perceived vulnerabilities could be more effective than offering external incentives.

Key words: Mobile payment security , M-Pesa agents, Technology acceptance model

Introduction

Cash transactions remain predominant in numerous developing nations, where they constitute over 90% of all payments. Concurrently, the proliferation of mobile devices has revolutionized the daily routines of countless individuals(Uwamariya & Loebbecke, 2020). Mobile phones, now ubiquitous, facilitate a myriad of functions ranging from communication to entertainment and internet browsing (Pal et al., 2021). Recent scholarly focus has honed in on leveraging these devices for secure payment processing. Nonetheless, mobile platforms are constrained by limited storage and computational capacities, impeding the execution of robust encryption protocols(Shahad & Al-Haija, 2024). This deficiency exposes mobile devices to various security threats, including spoofing, phishing, malware, and sniffing attacks. For the secure design of Mobile Payment Systems (MPS), it is imperative to consider these vulnerabilities to ensure user safety and system integrity (Ahmed et al., 2021; Mogaji & Nguyen, 2022).

The surge in Information and Communication Technology (ICT) utilization globally has shifted traditional transaction paradigms towards more remote interactions, thus minimizing the need for physical presence during financial exchanges(Bojjagani et al., 2023). This shift facilitates transactions over the internet, employing digital data and internet infrastructure to mimic conventional payment systems. Digital or electronic money offers notable benefits, such as transaction anonymity and reduced necessity for physical presence(Alkhowaiter, 2020). However, it also raises significant concerns regarding the confidentiality,

integrity, and availability of financial data, underscoring the dual-edged nature of this technological advancement in financial transactions (Rashidi et al., 2024).

The exponential advancement in mobile phone technology has catalyzed the proliferation of internet services, ushering in the era of mobile commerce (m-commerce) as a viable alternative to traditional e-commerce. The integration of the internet with mobile devices has enabled electronic transaction systems that not only replicate but enhance the functionalities of e-commerce(Williams, 2021). M-commerce distinguishes itself by offering unique advantages such as the Mobile Payment System (MPS), which facilitates real-time financial transactions from any location with internet access. This mobility advantage, coupled with features like interoperability, speed, reduced costs, and the capability for cross-border payments, positions m-commerce as an increasingly preferred method of commercial interaction over its more stationary e-commerce counterpart (de Luna et al., 2020).

Security within MPS is paramount, requiring robust protocols that include authentication, access control, confidentiality, integrity, non-repudiation, and availability. Authentication processes are dual-faceted, involving both user verification and source origin verification, essential for safeguarding against unauthorized access and ensuring the legitimacy of transactions (Wang et al., 2020). Furthermore, the need for data protection against passive attacks calls for stringent confidentiality measures. The integrity and non-repudiation of data ensure that transaction records are both accurate and indisputably linked to their originators (Ahmed et al., 2021). Despite the implementation of security standards such as the Payment Card Industry Data Security Standard (PCIDSS), which has been instrumental since its inception in 2004 in upholding the CIA triad, vulnerabilities still persist. Breaches can expose sensitive information like card numbers and security codes, underscoring the continuous need for advanced security measures in MPS, including both account-based and token-based payment systems (Tabrizchi & Kuchaki Rafsanjani, 2020).

Mobile money services have seen significant growth over the last two decades, substantially enhancing financial inclusion for billions of people globally. These services have opened up vast opportunities for entrepreneurs and small businesses, revolutionizing economic activities especially in developing regions. Currently, there are approximately 1.75 billion registered mobile money accounts worldwide, processing an impressive total of $1.4 trillion annually (GSMA, 2024) This growth is particularly notable in Sub-Saharan Africa, which hosts nearly three-quarters of these accounts. Over the last decade, West Africa has become increasingly prominent in this domain, with countries like Nigeria, Ghana, and Senegal leading the expansion. The number of mobile money accounts in West Africa has doubled from 2013 to 2023, with the region now boasting 435 million active accounts(GSMA, 2024).

Agents play a crucial role in the mobile money ecosystem, facilitating transactions and service delivery. In 2023, these agents managed over $307 billion in transactions, marking a 12% increase from the previous year. This figure represents a significant portion of all funds entering the mobile money system. The number of both registered and active agents has continued to grow; there were 18.6 million registered agents in 2023, a 22% increase from the previous year, and 8.3 million of these were active monthly, up 14% from 2022. Most of this growth occurred in Sub-Saharan Africa, driven by the expansion of services and an increasing reliance on mobile financial solutions. This region remains pivotal to the mobile money landscape, particularly in countries like Kenya, where the Mpesa service alone has 262,000 agents (Safaricom, 2024).

Despite the remarkable success of M-PESA in revolutionizing financial accessibility in Kenya, the mobile money service has faced significant security challenges. A study by Jepkemboi (2018) revealed that a large majority of users, reported that the single factor authentication security feature is insufficient and it is one of the vulnerabilities in MPESA security system. This highlights a critical vulnerability in the security framework of mobile transactions, suggesting that the reliance on simple PIN authentication may not provide robust protection against unauthorized access.

Further complicating the security landscape, a more recent study conducted by Owiti et al (2023) identified a myriad of factors contributing to mobile financial fraud in Kenya. These include poor remuneration, peer pressure, and the allure of quick gains (celerity), as well as systemic issues such as weak policies, inadequate user awareness, variable transaction costs, non-standardized processes, and insufficient compliance monitoring. Additionally, the organizational culture, the maturity level of mobile money services, and intense interbank competition were also cited as contributing factors(Owiti et al., 2023). These studies shows the complex and multifaceted security challenges facing mobile money services like M-PESA, necessitating a more sophisticated and multi-layered approach to securing mobile financial transactions.

Scammers are continually crafting sophisticated methods to exploit mobile money systems, a sector that not only generates millions but also grows significantly each year. This rampant increase in fraudulent activities has prompted governments, business leaders, and various stakeholders to intensify their efforts in preventing, detecting, and mitigating such threats. Daily, many Kenyans fall prey to these fraudsters, who capitalize on the vulnerabilities present within mobile money platforms like M-Pesa. Given the rising concern among M-Pesa users and agents about these security gaps, this study is driven by a need to explore the factors that could promote the adoption of more robust security measures. Consequently, this paper aims to investigate the factors influencing M-Pesa agents in Nairobi County to adopt an improved M-Pesa security system, thereby enhancing the resilience of these financial transactions against malicious exploits.

Related Work On Mpesa Security

M-Pesa agents have been frequently accused of misappropriating funds after deposits are made without a corresponding SMS confirmation, highlighting a critical vulnerability in the current security measures provided by Safaricom. These measures are seen as inadequate due to their failure to address issues arising from unconfirmed transactions, an issue critical in the evaluation of security from the perspective of M-Pesa agents. These agents play a dual role as facilitators of the service and as representatives of Safaricom, tasked with the responsibility of advising on technical matters and updating customers about new system developments. Therefore, the security deficiencies at this transactional step are often viewed as failures of the entire M-Pesa system, placing the primary blame on the agents (Tuwei & Tully, 2021). Recognizing the agents' crucial role, this study suggests enhancing their functionality through a new prototype designed to improve identification and verification processes.

Sungi et al. (2022) explored the causes of crime and fraud conducted on MPESA. The study reported that Mobile money platforms like M-Pesa have been shown to facilitate organized crime by offering a complex and multifaceted environment that includes diverse actors. One of the factors identified in the study as a cause of MPESA Fraud and is the platforms' weaknesses exploited by criminals, enabling them to engage in various forms of transnational crime. The intricate structure of M-Pesa, combined with its widespread usage, creates an empowering environment for these criminal activities. The predominance of M-Pesa over card payments thus calls for more understanding of security challenges from different dimensions.

In a study by Jepkemboi (2018) to investigate the security issues associated with the authentication process of M-PESA, it was reported that the authentication feature has significant vulnerabilities in current security protocols. The findings underscore the critical need for advanced security measures in mobile money services to combat sophisticated fraud methods effectively. Additionally, the study by Gitau (2018) on identity theft in Kenya underscores the importance of developing systems that can effectively preempt and counteract fraudulent activities. Gitau proposes an agile-developed prototype that blocks the use of compromised SIM cards, highlighting a proactive approach to mitigating fraud risks associated with mobile money services.

Thus, the need for a nuanced understanding of the socio-economic and technological contexts in which mobile payment systems like M-Pesa operate is critical. This understanding informs the development of security measures that are not only technologically sound but also contextually appropriate, ensuring they are effective in the environments they are meant to serve. The proposed enhancements to the M-Pesa system through a new agent-centered prototype highlight a pathway toward securing transactions while maintaining the ease and convenience that have made mobile money a pivotal financial service in Kenya and beyond.

Theoretical Framework

Technology Acceptance Model

Granić and Marangunić (2019) notes that the Technology Acceptance Model (TAM) was developed concurrently with the Theory of Planned Behaviour; the theory aims to explore the motivations underlying actions, specifically concerning technology usage, Marandu et al. (2022), via the TAM, explores what drives the willingness to embrace new technologies and identifies three key factors of “perceived ease of use, perceived usefulness, and attitude towards the technology in question”. The first factor, perceived ease of use, is about the effort needed to utilise the technology; the lesser the effort, the higher the likelihood of the individual being inclined to use the technology. The second factor, perceived usefulness, refers to the benefits gained from adopting the technology; the greater the benefits, the stronger the motivation to switch.

Lastly, the attitude towards technology usage is seen as a result of these two motivational factors (Motswaborwa, 2020).

The design components of the technology under discussion play a pivotal role in shaping its perceived value and usability, which in turn influences user attitudes towards the technology. These elements are seen as critical attributes that define the technology. This research utilizes the Technology Acceptance Model (TAM) as its theoretical foundation and partially aims to propose a system with improved security features. The adoption of this system by its target users, M-PESA agents, is expected to depend significantly on the perceived advantages and ease of use of the proposed security enhancements (Alhassan et al., 2020).

However, TAM has its critics. Ajibade and Mutula (2020) contends that the model's applicability is constrained due to the omission of crucial factors that influence technology acceptance. Specifically, Ajibade highlights the proficiency of IT staff as a critical determinant of technology adoption. Furthermore, variables such as organizational policies and IT guidelines are seen to moderate the relationship between technology acceptance and user intentions. Addressing these limitations, Granić and Marangunić (2019) suggest several research directions to enhance the model, including examining the moderating effects of additional variables, exploring new variables, integrating actual usage and outcomes, and considering the theory's relevance to older adults. Despite these critiques, the enduring applicability and reliability of TAM across various sectors, including IT and education, underscore its validity. This theoretical framework has guided the current study in exploring the factors that influence the adoption of enhanced security systems among M-PESA agents in Nairobi, Kenya.

Material And Methods

The study employed a predictive correlational design to assess how threat protection and efficacy influence the acceptance of security solutions among M-Pesa agents in Nairobi, Kenya. The research focused on M-Pesa agents given their critical role in the mobile payment ecosystem, making them central to the study's investigation of security enhancements. A total of 375 M-Pesa agents were selected using a clustered sampling method based on the proportion of agents across various constituencies in Nairobi, as indicated by the latest census data. This approach ensured a representative distribution of respondents from different urban densities, which are believed to correlate with the number of active M-Pesa agents.

Data was collected through structured questionnaires distributed via a drop-and-pick method, which included sections ranging from biodemographic profiles to perceptions on security practices. The dependent variable was uptake of security solutions while independent factors were various predictors. The questionnaire's reliability and validity were rigorously tested through a pilot study involving 108 respondents. This preliminary phase was crucial for refining the questions and ensuring the measurement tools accurately captured the intended constructs. Data analysis was performed using SPSS v25, following coding and entry procedures that preserved the integrity and confidentiality of the responses. The analytical process included regression analysis and exploratory factor analysis to interpret the data's underlying patterns and validate the study's theoretical framework comprehensively.

Results And Discussion

Table 1 presents the results of a linear regression analysis assessing the factors influencing the uptake of security solutions among M-Pesa agents. This table lists both unstandardized and standardized coefficients, providing a clear quantification of how each predictor contributes to the dependent variable, the Uptake of Security Solutions.

Table 1 Regression Co-Efficient on Factors Influencing Security Solution Uptake

	Unstandardized Coefficients		Standardized Coefficients		
	β	Std. Error	βeta	t	Sig.
(Constant)	1.338	.423		3.159	.002
Severity	-4.798E-005	.034	.000	-.001	.999
Vulnerability	.240	.044	.276	5.406	.000
Intrinsic Reward	.260	.078	.156	3.326	.001
Extrinsic Reward,	.089	.048	.087	1.862	.063
Response Cost	-.005	.022	-.012	-.243	.808

ResponseEfficacy	.071	.067	.050	1.053	.293
SelfEfficacy	.227	.042	.278	5.469	.000

Dependent Variable: UptakeOfSecSolution

The regression analysis revealed significant predictors of the uptake of security solutions among M-Pesa agents. The variables Vulnerability ($B = 0.240$, $p < 0.001$) and Self-Efficacy ($B = 0.227$, $p < 0.001$) demonstrated strong positive associations with the dependent variable, indicating that perceptions of vulnerability and personal confidence in managing security significantly influence agents' readiness to adopt security measures. Intrinsic Reward also showed a positive effect ($B = 0.260$, $p = 0.001$), suggesting that internal motivations play a crucial role in the decision-making process. Conversely, Severity ($B = -0.000048$, $p = 0.999$) and Response Cost ($B = -0.005$, $p = 0.808$) were not statistically significant, indicating a negligible impact on security solution uptake.

The regression analysis further examined the impact of Extrinsic Reward and Response Efficacy on the uptake of security solutions among M-Pesa agents. Extrinsic Reward showed a positive but non-significant influence ($B = 0.089$, $p = 0.063$), suggesting that external incentives such as bonuses or public recognition might slightly encourage agents to adopt security measures, though this effect was not statistically robust. Response Efficacy, representing the agents' beliefs about the effectiveness of the proposed security measures, also showed a positive yet non-significant relationship ($B = 0.071$, $p = 0.293$). This indicates that while agents may appreciate the potential benefits of security interventions, their perceptions of the effectiveness of these measures do not significantly drive their adoption decisions. These findings highlight the critical role of psychological and motivational factors in the effective implementation of security practices within mobile money systems.

Discussion

This section presents the findings on the factors influencing the uptake of security solutions among M-Pesa agents. Vulnerability, with a significant positive coefficient, suggests that agents' perceptions of their vulnerability to security threats strongly motivate them to adopt security measures. This finding aligns with the Protection Motivation Theory (PMT), which posits that perceived risk is a critical driver in the motivation to engage in protective behaviors (Marikyan & Papagiannidis, 2023). Similar studies, such as by (Devi et al., 2023), found that perceived vulnerability significantly influenced the adoption of cybersecurity measures in corporate settings, underscoring the relevance of this factor across different contexts. However, this contrasts with (Nam, 2019), who reported a weak relationship between perceived vulnerability and the adoption of security measures, suggesting that other factors like institutional policies might overshadow personal perceptions in some environments.

Self-Efficacy also emerged as a robust predictor, indicating that agents who believe in their ability to effectively implement security solutions are more likely to do so. This is consistent with TAM Theory, which emphasizes self-efficacy as a determinant of behavior change. In the context of information security, research by (Hameed & Arachchilage, 2021) corroborates that self-efficacy enhances the likelihood of adopting security behaviors. Conversely, (Utomo et al., 2022) suggest that self-efficacy may not always translate into action without adequate support and resources, indicating the need for organizational backing in enhancing self-efficacy.

The significance of Intrinsic Reward highlights the impact of internal gratification in adopting security practices, reflecting findings from the field of psychology where intrinsic motivation is seen as a powerful driver for behavior (Dodge et al., 2023). This is particularly relevant in environments where external rewards are either minimal or inconsistent. Contrastingly, studies like by (Kumar et al., 2021) suggest that in high-stakes environments, extrinsic rewards or penalties might be more influential than intrinsic motivation.

The marginal influence of 'Extrinsic Reward' aligns with (Dodge et al., 2023), who noted that external incentives might undermine intrinsic motivation, thereby having a diluted effect on behavior that should ideally be internally motivated, such as security adherence. Conversely, (Otting, 2020). Kumar et al. (2021) found that external rewards could significantly enhance compliance when appropriately structured, suggesting that the nature of the reward might affect its efficacy.

Similarly, the modest role of 'Response Efficacy' supports Bisma et al. (2021) finding that belief in the efficacy of a solution alone does not robustly predict behavior change unless coupled with high threat perceptions and personal responsibility. This contrasts with studies by (Shillair, 2018), where perceived

effectiveness strongly influenced decision-making in health behaviors, suggesting sectoral differences in how efficacy perceptions impact actions. These results highlight the importance of integrating intrinsic motivational strategies and enhancing self-efficacy over purely extrinsic rewards or perceived effectiveness of interventions in promoting security solution uptake among financial service agents.

Severity and Response Cost, although theoretically significant in TAM, did not show significant effects in this study. This might indicate that the perceived severity of threats and the costs associated with implementing security solutions are not primary concerns for M-Pesa agents, possibly due to a lack of direct experience with severe consequences or because the costs are not sufficiently prohibitive. This finding diverges from the literature where severity has been shown to influence security behavior significantly in different settings (Dodge et al., 2023).

Conclusion

This study elucidates the various factors that influence the adoption of security solutions among M-Pesa agents in Nairobi, highlighting the importance of perceived vulnerability, self-efficacy, and intrinsic motivation in determining security behaviors. Findings indicate that vulnerability and self-efficacy significantly propel agents towards adopting enhanced security measures, demonstrating the need for targeted interventions that bolster these perceptions. Moreover, intrinsic rewards emerge as a crucial motivator, potentially more impactful than extrinsic rewards, which showed limited effect. This suggests that fostering a sense of personal responsibility and satisfaction in security practices might be more effective than offering external incentives. Ultimately, the study reinforces the importance of understanding psychological and motivational dynamics in the design and implementation of security solutions in mobile money systems, advocating for strategies that enhance internal motivation and perceived capability among agents.

References

1. Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). Security in next generation mobile payment systems: A comprehensive survey. *IEEE Access*, *9*, 115932–115950.
2. Ajibade, P., & Mutula, S. M. (2020). Big data, 4IR and electronic banking and banking systems applications in South Africa and Nigeria. *Banks and Bank Systems*, *15*(2), 187.
3. Alhassan, A., Li, L., Reddy, K., & Duppati, G. (2020). Consumer acceptance and continuance of mobile money: Secondary data insights from Africa using the technology acceptance model. *Australasian Journal of Information Systems*, *24*. http://journal.acs.org.au/index.php/ajis/article/view/2579
4. Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. *International Journal of Information Management*, *53*, 102102.
5. Bojjagani, S., Sastry, V. N., Chen, C.-M., Kumari, S., & Khan, M. K. (2023). Systematic survey of mobile payments, protocols, and security infrastructure. *Journal of Ambient Intelligence and Humanized Computing*, *14*(1), 609–654. https://doi.org/10.1007/s12652-021-03316-4
6. de Luna, I. R., Montoro-Ríos, F., Martínez-Fiestas, M., & Casado-Aranda, L.-A. (2020). Analysis of a mobile payment scenario: Key issues and perspectives. In *Impact of mobile services on business development and e-commerce* (pp. 22–47). IGI Global. https://www.igi-global.com/chapter/analysis-of-a-mobile-payment-scenario/238245
7. Granić, A., & Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, *50*(5), 2572–2593.
8. GSMA. (2024). *The State of the Industry Report on Mobile Money 2024* (pp. 1–90).
9. Hameed, M. A., & Arachchilage, N. A. G. (2021). The role of self-efficacy on the adoption of information systems security innovations: A meta-analysis assessment. *Personal and Ubiquitous Computing*, *25*(5), 911–925. https://doi.org/10.1007/s00779-021-01560-1
10. Jepkemboi, C. L. (2018). Enhancing Security of Mpesa Transactions by Use of Voice Biometrics. *Journal of Banking Fraud*, *10*(1).
11. Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *34*(6), 1597–1629.

12. Marandu, E. E., Kealesitse, B., & Motswaborwa, C. (2022). *Predicting Intention and Actual Use of Mobile Money Using the Technology Acceptance Model: The Case of University of Botswana Students*. https://www.researchgate.net/profile/Calvin-Motswaborwa/publication/368757289_Predicting_Intention_and_Actual_Use_of_Mobile_Money_Using/links/63f891c257495059453e6d3e/Predicting-Intention-and-Actual-Use-of-Mobile-Money-Using.pdf
13. Motswaborwa, C. (2020). *Predicting intention and actual use of mobile money using the technology acceptance model: The case of University of Botswana students*. http://ithuteng.ub.bw/handle/10311/2469
14. Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, 101122.
15. Owiti, S. O., Ogara, S., & Rodrigues, A. (2023). Contributing Factors to Mobile Financial Fraud within Kenya. *EPRA International Journal of Research and Development (IJRD)*, *8*(1), 32–39.
16. Pal, A., Herath, T., & Rao, H. R. (2021). Why do people use mobile payment technologies and why would they continue? An examination and implications from India. *Research Policy*, *50*(6), 104228.
17. Rashidi, F. U., Mohsini, M. H., & Mega, B. (2024). A framework for security improvement on usage of mobile money application based on iris biometric authentication method. *Information Security Journal: A Global Perspective*, 1–13. https://doi.org/10.1080/19393555.2024.2347240
18. Safaricom. (2024). *Audited Results for 2023 Financial Year*.
19. Shahad, A.-T., & Al-Haija, Q. A. (2024). Secure Mobile Payment (SMP): Challenges and Potential Solutions. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(11s), 103–120.
20. Sungi, S., Osiro, M., & Odhiambo, T. (2022). *M-Pesa and Transnational Organized Crime: Causes and Facilitation Factors*. https://www.researchgate.net/profile/Simeon-Sungi/publication/362656905_M-Pesa_and_Transnational_Organized_Crime_Causes_and_Facilitation_Factors/links/62f67c49c6f6732999c68c0e/M-Pesa-and-Transnational-Organized-Crime-Causes-and-Facilitation-Factors.pdf
21. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532. https://doi.org/10.1007/s11227-020-03213-1
22. Tuwei, D., & Tully, M. (2021). The role of change agents in the adaptation and use of mobile money services in Kenya. *Journal of African Media Studies*, *13*(1), 89–102. https://doi.org/10.1386/jams_00035_1
23. Wang, F., Shan, G. B., Chen, Y., Zheng, X., Wang, H., Mingwei, S., & Haihua, L. (2020). Identity authentication security management in mobile payment systems. *Journal of Global Information Management (JGIM)*, *28*(1), 189–203.
24. Williams, M. D. (2021). Social commerce and the mobile platform: Payment and security perceptions of potential users. *Computers in Human Behavior*, *115*, 105557.