Digital Financial Literacy, Fraud Awareness, and Safe Mobile Payment Behavior among Filipino Consumers: The Mediating Role of Perceived Control

Randy A. Cruz[1]*, Maria Lourdes Santos[2], Nur Aina Hamzah[3]
[1]Department of Business Analytics, Polytechnic University of the Philippines, Manila, Philippines
Email: randy.cruz@pup.edu.ph
[2]College of Business Administration, Technological University of the Philippines, Manila, Philippines
Email: mlsantos@tup.edu.ph
[3]Faculty of Computing and Industrial Management, Universiti Malaysia Pahang Al-Sultan Abdullah, Kuantan, Malaysia
Email: nur.aina@umpsa.edu.my
*Corresponding author: randy.cruz@pup.edu.ph

Abstract

Digital payments have become ubiquitous in Southeast Asia, yet the expansion of cashless ecosystems has been accompanied by rising fraud attempts, phishing, and social engineering schemes that disproportionately affect consumers with limited digital financial competence. This study examines how digital financial literacy influences safe mobile payment behavior among Filipino consumers, focusing on fraud awareness and perceived control as key psychological mechanisms. Drawing on protection motivation theory, self-efficacy perspectives, and perceived risk logic, the model conceptualizes literacy as a capability that improves threat appraisal, strengthens coping appraisal, and increases the likelihood that consumers adopt safe practices such as verification, device hygiene, and transaction monitoring. Survey data were collected from 644 active mobile payment users across Luzon, Visayas, and Mindanao. Partial Least Squares Structural Equation Modeling (PLS-SEM) was applied to test direct effects and serial mediation. Results indicate that literacy strengthens fraud awareness and perceived control; awareness increases perceived control by clarifying threats and actionable responses; perceived control strongly predicts safe payment behavior. The findings suggest that anti-fraud outcomes depend not only on awareness campaigns but also on building consumer confidence to execute protective routines. Policy implications emphasize integrating literacy modules into wallet onboarding and community-based education tailored to local fraud narratives.

Keywords: *Digital Financial Literacy, Mobile Payments, Fraud Awareness, Perceived Control, Safe Behavior, Philippines, PLS-SEM.*

A. INTRODUCTION

Digital payments have become an everyday infrastructure for consumption and peer-to-peer transfers across the Philippines. Wallet ecosystems and bank-linked apps allow users to pay bills, send remittances, purchase goods online, and transact at physical stores with minimal cash handling. This convenience has supported inclusion goals, particularly in contexts where bank branch density is uneven and traditional financial services remain costly (Afroze & Rista, 2022; Lai & Liew, 2021). The rapid diffusion of mobile payments has also reshaped consumer habits, turning smartphones into default payment instruments for a wide range of transactions.

Alongside these benefits, fraud risks have expanded. Phishing links, fake customer support hotlines, account takeover attempts, and social engineering scams are now widely reported in public discourse. The problem is not only technical (Hopalı et al., 2022; Sabri et al., 2023). Many scams exploit behavioral vulnerabilities, such as haste, social pressure, and limited understanding of security cues. When users cannot distinguish legitimate prompts from malicious ones, they may expose credentials or authorize transfers under deception. Fraud can erode trust and trigger avoidance, which undermines the promise of digital inclusion (Jegerson et al., 2024; Sandhu et al., 2022).

The effectiveness of fraud prevention depends on more than disseminating warnings. Consumers must be able to interpret threats and perform protective routines consistently. Digital financial literacy, understood as the capability to understand digital payment processes, evaluate risks, and manage personal financial information, is likely to shape such routines. Literacy enables users to recognize suspicious patterns, verify transaction details, and respond calmly to incidents, reducing the chance that fear or confusion leads to costly mistakes (Raza et al., 2024; Simatele, 2024).

Fraud awareness is a necessary mechanism but rarely sufficient. Awareness campaigns can increase knowledge of threat types, yet users may still fail to act safely if they do not believe they can execute protective behaviors effectively. Perceived control captures this belief. Users with higher perceived control feel capable of verifying recipients, managing app permissions, and taking steps after suspicious activity. Perceived control resembles self-efficacy in the security domain and can determine whether awareness translates into behavior (Namahoot & Jantasri, 2023; Yadav & Banerji, 2024).

This study develops and tests a model linking digital financial literacy to safe mobile payment behavior through fraud awareness and perceived control. The Philippines provides a relevant context because wallet adoption is high, remittance flows are substantial, and fraud narratives are common in both urban and provincial communities (Chatterjee, 2021; Dzogbenuku et al., 2022). The study addresses three research questions: (1) whether literacy predicts safe behavior, (2) whether awareness and perceived control mediate this relationship in sequence, and (3) how these mechanisms inform anti-fraud policy and platform design in an ASEAN setting.

The study contributes to digital finance research in two ways. It shifts focus from adoption toward safety outcomes and clarifies the behavioral pathway through which capability influences protection by integrating protection motivation theory with literacy and control constructs, and it also provides practical guidance for wallet providers and policymakers seeking to reduce fraud without discouraging usage through fear-based messaging.

B. LITERATURE REVIEW

Digital Financial Literacy and Fraud Awareness

Digital financial literacy should increase fraud awareness because literate users recognize how scams exploit payment workflows. Users who understand authentication and transaction confirmation can detect suspicious requests and inconsistent cues. Literacy also helps users interpret platform announcements and distinguish genuine notifications from fake messages (Ali, 2024; REYNON et al., 2022). Fraud prevention in digital payments intersects with cybersecurity, behavioral economics, and consumer finance. Protection Motivation Theory (PMT) provides a useful framework because it explains protective behavior as a function of threat appraisal and coping appraisal. Threat appraisal involves perceived severity and vulnerability, while coping appraisal involves response efficacy and self-efficacy. Digital financial literacy can influence both forms of appraisal by improving understanding of payment processes and by enabling users to evaluate risks more accurately (Ahmad Ramli & Hamzah, 2021; Binaluyo et al., 2024).

Digital financial literacy extends conventional financial literacy by emphasizing digital interfaces, data privacy, authentication, and platform rules. In mobile payments, literacy includes understanding how to verify recipients, how to interpret confirmation messages, and how to distinguish legitimate support channels from impostors. Higher literacy should increase fraud awareness because informed users can recognize threat patterns and understand common scam tactics (Khan & Abideen, 2023; Lestari et al., 2024). This relationship suggests that literacy functions as an upstream capability that shapes the quality of threat appraisal, reducing underestimation of risk and improving recognition of deception.

H1: Digital financial literacy is positively associated with fraud awareness.

Fraud Awareness and Perceived Control

Fraud awareness can strengthen perceived control when knowledge is paired with actionable steps. Awareness clarifies what to check, when to pause, and how to respond after a suspicious message. Users who understand threat patterns are less likely to panic and more likely to behave deliberately, increasing confidence in managing risk. Fraud awareness captures knowledge and vigilance regarding scam techniques (Samonte et al., 2024; Sanchez & Tanpoco, 2023).

Safe mobile payment behavior includes actions such as enabling stronger authentication, avoiding sharing one-time passwords, verifying QR codes and links, monitoring transaction history, updating apps, and contacting official channels when suspicious activity occurs. These behaviors require cognitive effort and habit formation, suggesting that perceived control is a proximal driver. Awareness without coping resources can increase anxiety (Sarwar et al., 2024; Ullah et al., 2022). The model therefore tests whether awareness, in general, supports perceived control by making protective actions clearer.

H2: Fraud awareness is positively associated with perceived control.

Digital Financial Literacy, Perceived Control, and Safe Behavior

Digital financial literacy is expected to strengthen perceived control because literate users are more familiar with app settings, verification steps, and official support processes. Familiarity reduces cognitive barriers and supports the belief that protective behavior is feasible. Perceived control should predict safe mobile payment behavior because users who feel capable are more likely to enact protective routines consistently rather than relying on luck (Nguyen et al., 2024; Okello Candiya Bongomin & Ntayi, 2020). This includes verifying recipients, using strong authentication, and monitoring transactions.

Synthesizing these perspectives, the study proposes a serial mechanism: literacy strengthens awareness, awareness strengthens perceived control by clarifying threats and responses, and perceived control increases safe behavior. The model recognizes that literacy may also influence perceived control directly by reducing confusion and increasing competence. Literacy is also expected to relate directly to safe behavior because knowledge can drive routine adoption even without explicit awareness mediation (Gyaisey, 2023; Tanpoco et al., 2022).

H3: Digital financial literacy is positively associated with perceived control.

H4: Perceived control is positively associated with safe mobile payment behavior.

H5: Digital financial literacy is positively associated with safe mobile payment behavior.

Serial Mediation Hypothesis

The theoretical logic suggests a serial pathway: literacy strengthens fraud awareness, awareness strengthens perceived control, and control increases safe behavior. This pathway aligns with PMT by linking capability to both threat and coping appraisals. The model also allows for direct paths that capture additional effects (Binaluyo et al., 2024; Sarwar et al., 2024).

Awareness can increase protective behavior by encouraging caution, yet it can also produce fear if users lack coping resources. Perceived control is essential for converting awareness into action. When users feel they can manage settings, verify transactions, and recover from incidents, they are more likely to adopt safe routines consistently (Jegerson et al., 2024; Yadav & Banerji, 2024).

H6: Fraud awareness and perceived control serially mediate the relationship between digital financial literacy and safe mobile payment behavior.

C. METHOD

A quantitative explanatory design was employed to examine the proposed serial mediation model. A cross-sectional survey approach was selected because literacy, awareness, and perceived control are psychological and behavioral dispositions that are effectively measured through multi-item self-report instruments anchored in concrete routines. Data were collected from 644 active mobile payment users across the Philippines, covering Luzon, Visayas, and Mindanao. Eligibility required at least three mobile payment transactions within the previous month to ensure recent experience. Recruitment relied on community organizations, workplace networks, and online panels, with screening and attention checks to improve data quality.

Digital financial literacy was measured through items assessing understanding of authentication, verification steps, fee awareness, and ability to identify official channels. Fraud awareness measured familiarity with common scams, vigilance toward suspicious messages, and recognition of social engineering tactics. Perceived control measured confidence in verifying transactions, managing settings, and responding to suspected fraud. Safe behavior measured frequency of protective actions, including using stronger authentication, verifying recipients, avoiding credential sharing, and monitoring transaction history.

All measures used five-point Likert scales. Partial Least Squares Structural Equation Modeling (PLS-SEM) was applied to evaluate the measurement model and test structural relationships and serial mediation. Bootstrapping supported inference about indirect effects, with interpretation centered on mechanism logic.

D. RESULT AND DISCUSSION

Result

The measurement model evaluation indicated that constructs showed acceptable reliability and validity. Respondents distinguished fraud awareness from perceived control, supporting the interpretation that knowledge of threats and confidence to act are related but distinct psychological states. Structural evaluation supported the proposition that digital financial literacy strengthens fraud awareness and perceived control. Fraud awareness related positively to perceived control, suggesting that knowledge clarifies actionable responses and increases confidence rather than merely increasing fear.

Perceived control emerged as a strong predictor of safe mobile payment behavior, indicating that confidence to execute protective routines is a proximal driver of security-related habits. Digital financial literacy also related positively to safe behavior, reflecting the direct influence of competence on routine adoption. Serial mediation analysis supported the pathway literacy → awareness → control → safe behavior, indicating that literacy improves safety partly by enhancing threat recognition and then strengthening coping confidence. Tables summarize hypothesis support and mechanism logic without emphasizing coefficient magnitudes.

Table 1. Measurement Model Summary

Construct	Internal Consistency	Convergent Validity	Discriminant Validity
Digital Financial Literacy	Established	Established	Confirmed
Fraud Awareness	Established	Established	Confirmed
Perceived Control	Strong	Established	Confirmed
Safe Mobile Payment Behavior	Established	Established	Confirmed

Source: data proceed

A richer interpretation treats safe behaviour not as a one-off decision but as a habit system embedded in real-world constraints, where the binding problem is rarely “knowing what to do” and more often “doing it every time when it matters.” Many protective actions in digital finance or messaging environments are technically simple, such as checking a sender’s identity, verifying a recipient, confirming a URL, or pausing before authorising a transfer; the difficulty arises because these actions must be executed consistently under time pressure, attentional overload, and social influence. Scam messages are deliberately engineered to compress deliberation time and to hijack social norms, for example by invoking authority, urgency, embarrassment, reciprocity, or implied consequences if the victim delays.

The cognitive cost is not the complexity of the protective action itself, but the need to interrupt an ongoing routine and to switch into a verification mode that feels “slow” relative to the emotional tempo of the scam. Digital literacy, in this framing, matters less as abstract knowledge and more as a mechanism for converting checks into automatic scripts: a short sequence of steps that can be triggered quickly and reliably without heavy deliberation. Perceived control then becomes the psychological infrastructure that sustains those scripts when emotions spike. When fear, urgency, or perceived loss is activated, people tend to narrow attention and prioritise immediate relief over accuracy; control is what keeps a user anchored to process even when the message is designed to make process feel costly.

Table 2. Hypotheses Testing Summary

Hypothesis	Relationship	Supported
H1	Literacy → Fraud Awareness	Yes
H2	Fraud Awareness → Perceived Control	Yes
H3	Literacy → Perceived Control	Yes
H4	Perceived Control → Safe Behavior	Yes
H5	Literacy → Safe Behavior	Yes
H6	Serial mediation (Literacy → Awareness → Control → Safe Behavior)	Yes

Source: data proceed

This habit-system lens clarifies why fraud awareness campaigns sometimes fail and occasionally backfire. Raising awareness by emphasising threat can increase vigilance in the short term, yet fear-based messaging without coping tools can also increase cognitive load, reduce self-efficacy, and paradoxically make users more vulnerable when confronted with high-pressure situations. If users internalise "scams are everywhere" but do not internalise a concrete action routine, the message produces anxiety rather than competence. Anxiety is not neutral; it can impair working memory, shorten time horizons, and promote avoidance, all of which are favourable conditions for manipulation. The mechanism implied here is that effective education should prioritise procedural learning over abstract warnings: step-by-step routines that can be rehearsed, recalled quickly, and executed under arousal. Practice scenarios become crucial because they simulate the same emotional and social triggers that scams exploit. A community-based approach can be especially powerful, not simply because it spreads information, but because it normalises verification as a social norm and reduces stigma around "double-checking." When training includes simulated scam conversations, role-played persuasion attempts, and guided debriefs, users learn not only what to verify but also how to manage the interpersonal discomfort of verification. This is a subtle but decisive point: many people comply with scams because refusing or delaying feels socially costly, especially when the scam impersonates a boss, family member, or authority figure. Rehearsal helps users adopt language that preserves relationships while still slowing the interaction, for example, "I'm going to call you back through the official number," or "I'll verify this through the app before proceeding." In effect, training should teach behavioural scripts and social scripts together, because scams attack both cognition and social coordination.

Platform design can extend this behavioural logic by reducing reliance on perfect user self-control and instead providing default structures that make safe behaviour easier than unsafe behaviour. The most effective interventions tend to be those that preserve usability while quietly shifting risk probabilities. Making strong authentication the default is a canonical example: if multi-factor authentication, device binding, or biometric confirmation is opt-out rather than opt-in, the baseline security posture improves without demanding that users actively choose security every time. Clear recipient confirmation screens also matter because many scams depend on the victim being uncertain, distracted, or rushed; an interface that surfaces the recipient name, bank or wallet identifier, and a salient "does this match your intended recipient?" checkpoint can interrupt autopilot. Adding friction to high-risk actions is often criticised as harming user experience, yet the habit-system frame shows why targeted friction is rational: it introduces a small pause at precisely the moment when scammers want speed. The goal is not to punish legitimate users, but to create a structured moment for verification that is easy to comply with. Importantly, such friction works best when it is intelligible and framed as empowerment. If users interpret safeguards as arbitrary obstacles, they will seek ways around them; if they interpret safeguards as tools that protect them from manipulation, they are more likely to accept the pause as part of normal financial hygiene. In design terms, this suggests that microcopy and interface cues should emphasise agency and protection, for example "Take 10 seconds to confirm," rather than punitive language such as "Action blocked."

Table 3. Mechanism Summary for Interpreting the Results

Mechanism	Interpretive Logic	Practical Meaning
Literacy → Awareness	Competence improves recognition of scam patterns and suspicious cues.	Users detect phishing links, fake support, and OTP requests more reliably.
Awareness → Control	Knowing threats clarifies what actions to take, strengthening confidence.	Users pause, verify, and use official channels rather than reacting impulsively.
Control → Safe Behavior	Confidence increases consistent enactment of protective routines.	Users enable stronger authentication, monitor transactions, and avoid credential sharing.

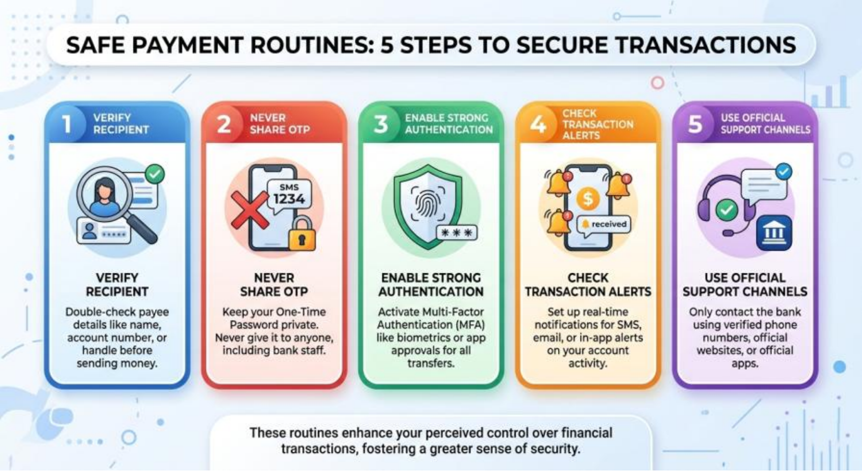
Source: data proceed

From an ASEAN perspective, the risk environment is amplified by cross-border remittances, interoperability initiatives, and the rapid diffusion of new payment rails. As systems become more connected, attackers gain more routes to move funds quickly and to exploit gaps between jurisdictions, reporting standards, and platform policies. Interoperability is economically valuable, yet it increases exposure to novel scam vectors because it expands the set of entities, identifiers, and workflows that users must recognise as legitimate. The habit-system frame implies that expanding connectivity without harmonised safety infrastructure creates a mismatch: the complexity of the ecosystem increases faster than the user's capacity to verify. One response is to treat fraud reporting and intelligence sharing as part of the common infrastructure, not as isolated platform responsibilities. Harmonised reporting protocols and shared blacklists of fraudulent accounts can reduce the speed advantage that scammers rely on, especially when combined with rapid freezing procedures and cross-platform escalation pathways. Consumer-facing tools can also be coordinated: warning banners, verified official channels, and standardised confirmation steps should look and feel consistent across major platforms to reduce confusion. Consistency matters because scammers exploit ambiguity; when each platform uses different signals for "official" and "unsafe," users must relearn verification each time, which undermines habit formation. Coordinated cues create a regional "grammar of safety," allowing users to generalise scripts across platforms rather than starting from scratch.

Future work should also take segmentation seriously, because vulnerability is not uniform and one-size interventions can be inefficient. Older users may face lower baseline digital literacy, less familiarity with evolving scam tactics, and higher trust in authority cues, which can raise fraud risk; younger users may be more digitally comfortable but more exposed to social media manipulation, influencer scams, and rapid-fire messaging environments where attention is fragmented. Segmentation should not be reduced to age alone. Risk profiles could incorporate transaction patterns, exposure channels, prior scam encounters, and behavioural signals such as repeated failed authentication attempts or unusual device changes. A segmentation approach supports targeted interventions: high-risk users could receive stronger default protections, more salient warnings, and simplified verification routes, while low-risk users maintain smoother flows. This is not merely a convenience choice; it is a governance choice that allocates protective resources where marginal benefit is highest. It also reduces the chance of warning fatigue among lower-risk groups while ensuring that high-risk groups receive meaningful support.

Discussion

The findings support a capability-based account of anti-fraud behavior in mobile payments. Digital financial literacy strengthens safe behavior not simply by increasing fear of fraud, but by improving threat recognition and building confidence to execute protective routines. This distinction is important because fear-based messaging can reduce usage and undermine inclusion goals. The observed mechanism suggests that competence and control are more reliable drivers of safety than fear alone. Fraud awareness contributes to safety when it is actionable. Awareness appears to strengthen perceived control by clarifying what cues matter and what steps are effective. Users who understand how scams work can interpret suspicious messages as manageable rather than overwhelming, reducing panic-driven mistakes. This mechanism aligns with protection motivation logic, where coping appraisal determines whether threat appraisal produces protective action.



SAFE PAYMENT ROUTINES: 5 STEPS TO SECURE TRANSACTIONS

1 VERIFY RECIPIENT

VERIFY RECIPIENT

Double-check payee details like name, account number, or handle before sending money.

2 NEVER SHARE OTP

NEVER SHARE OTP

Keep your One-Time Password private. Never give it to anyone, including bank staff.

3 ENABLE STRONG AUTHENTICATION

ENABLE STRONG AUTHENTICATION

Activate Multi-Factor Authentication (MFA) like biometrics or app approvals for all transfers.

4 CHECK TRANSACTION ALERTS

CHECK TRANSACTION ALERTS

Set up real-time notifications for SMS, email, or in-app alerts on your account activity.

5 USE OFFICIAL SUPPORT CHANNELS

USE OFFICIAL SUPPORT CHANNELS

Only contact the bank using verified phone numbers, official websites, or official apps.

These routines enhance your perceived control over financial transactions, fostering a greater sense of security.

Figure 1. Safe Payment Routines to secure transaction

Perceived control emerges as a proximal driver of safe mobile payment behavior. Even when users know about scams, they may fail to act safely if they feel incapable of managing settings or verifying transactions. Control captures the psychological readiness to apply protective actions consistently, suggesting that education programs should emphasize practice-based learning rather than abstract warnings. A Philippine context adds practical relevance. Remittance-driven transfers and peer-to-peer payments are common, and scams often exploit urgency or social pressure. Community-based literacy programs can address these narratives by teaching verification scripts and official-channel habits. Wallet providers can embed literacy into onboarding with interactive checklists that normalize safe routines without increasing friction excessively.

An ASEAN comparative lens suggests that similar mechanisms likely operate region-wide, though dominant scam types differ. Indonesia and Vietnam have experienced rapid wallet growth and increasing phishing narratives, making literacy and control essential. Thailand's mature QR ecosystem still faces social engineering, indicating that trust and control remain relevant. Cambodia and Laos may exhibit higher vulnerability due to lower baseline literacy and fewer formal consumer protection resources, amplifying the importance of embedded education.

A deeper layer concerns how platforms can support perceived control, not merely by adding barriers but by making risk legible in ways that users can act on. Control grows when users can see what is happening and understand the consequences of actions before committing, which implies that interfaces should expose relevant information at the decision point, not bury it in settings or post-transaction logs. Real-time scam warning banners, context-sensitive prompts, and official-channel verification tools can function as cognitive scaffolding, especially when they are calibrated to avoid alarm fatigue. The line between helpful warning and background noise is thin: if warnings appear too often, users habituate and click through; if warnings appear only for high-risk patterns, they retain salience. This is where behavioural science aligns with security engineering: risk scoring can trigger additional confirmation steps only when the transaction resembles known scam patterns, such as first-time recipients, unusual amounts, cross-border routing, or rapid sequential transfers. Done well, this preserves low-friction experiences for ordinary behaviour while inserting deliberate friction where it matters.

Across these layers, the most actionable implication is to treat safety as an engineered behaviour rather than a moral expectation placed solely on users. Literacy and awareness are necessary, yet they are insufficient when scams are designed to defeat attention and exploit social compliance. Effective systems combine three elements: first, behavioural scripts that users can execute under pressure; second, psychological control support that keeps users anchored to scripts when emotions rise; third, platform and ecosystem design that makes safe behaviour the path of least resistance through defaults, intelligent friction, and coordinated signals. In this integrated view, education is most effective when it trains routines and coping strategies rather than only delivering warnings, platform design is most effective when it provides empowerment rather than restriction, and regional cooperation is most effective when it reduces fragmentation in reporting, verification cues, and fraud intelligence. The broader research agenda should then shift from asking whether users "know about scams" to measuring whether users and systems can reliably execute verification under realistic conditions, because that is where the real variance in vulnerability is produced.

Policy implications emphasize integrated consumer protection. Regulators can encourage standardized official-channel verification, incident reporting norms, and consistent disclosure of support contacts. Platforms can support perceived control through clearer security settings, real-time transaction alerts, and guided dispute workflows. Building competence and confidence supports both safety and sustained usage. Limitations highlight research opportunities. Cross-sectional data restrict causal inference, and longitudinal studies could track how literacy interventions change behavior over time. Objective behavioral data, such as enabling two-factor authentication and frequency of verification, could complement self-reports. Future work could also examine how social influence and emotional triggers interact with literacy, shaping susceptibility to scams.

E. CONCLUSION

This study demonstrates that digital financial literacy improves safe mobile payment behavior among Filipino consumers through a serial mechanism involving fraud awareness and perceived control. Literacy strengthens recognition of threats and increases confidence to enact protective routines, while perceived control acts as a proximal driver of consistent safe behavior. For policymakers and wallet providers, the findings imply that safety outcomes depend on capability-building rather than on warnings alone. Integrating literacy modules into onboarding, strengthening official-channel visibility, and designing interfaces that make protective actions easy can reduce fraud vulnerability without discouraging digital payment usage. As ASEAN digital finance ecosystems expand, combining inclusion with practical consumer protection becomes essential for sustaining trust and participation.

REFERENCES

Afroze, D., & Rista, F. I. (2022). Mobile financial services (MFS) and digital inclusion–a study on customers' retention and perceptions. *Qualitative Research in Financial Markets*, *14*(5), 768–785.

Ahmad Ramli, F. A., & Hamzah, M. I. (2021). Mobile payment and e-wallet adoption in emerging economies: A systematic literature review. *Journal of Emerging Economies & Islamic Research*, *9*(2), 1–39.

Ali, A. O. (2024). The payments security and convenience on consumer of mobile payments in Baguio city, Philippines. *European Journal of Management and Marketing Studies*, *9*(3).

Binaluyo, J. P., Santos, A. R., & Agustin, N. B. (2024). Challenges and opportunities for digital transformation in Philippine microfinance institutions. *International Journal of Economics and Financial Issues*, *14*(5), 269.

Chatterjee, A. (2021). Analysis of financial frauds in electronic payment systems in India and China. *Turkish Online Journal of Qualitative Inquiry*, *12*(7).

Dzogbenuku, R. K., Amoako, G. K., Kumi, D. K., & Bonsu, G. A. (2022). Digital payments and financial wellbeing of the rural poor: The moderating role of age and gender. *Journal of International Consumer Marketing*, *34*(2), 113–136.

Gyaisey, A. P. (2023). The Effect of Mobile Payment Technology Fraud Perception on Customer Intention to Continously Use the Service: A Study Moderated by Generation X, Y, and Z from a Developing Economy. *Y, and Z from a Developing Economy (Doctoral Dissertation, University of Ghana)*.

Hopalı, E., Vayvay, Ö., Kalender, Z. T., Turhan, D., & Aysuna, C. (2022). How do mobile wallets improve sustainability in payment services? A comprehensive literature review. *Sustainability*, *14*(24), 16541.

Jegerson, D., Khan, M., & Mertzanis, C. (2024). Adoption of cryptocurrencies for remittances in the UAE: the mediation effect of consumer innovation. *European Journal of Innovation Management*, *27*(6), 1837–1863.

Khan, W. A., & Abideen, Z. U. (2023). Effects of behavioural intention on usage behaviour of digital wallet: the mediating role of perceived risk and moderating role of perceived service quality and perceived trust. *Future Business Journal*, *9*(1), 73.

Lai, P. C., & Liew, E. J. Y. (2021). Towards a cashless society: The effects of perceived convenience and security on gamified mobile payment platform adoption. *Australasian Journal of Information Systems*, *25*.

Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. *Safer Communities*, *23*(4), 444–464.

Namahoot, K. S., & Jantasri, V. (2023). Integration of UTAUT model in Thailand cashless payment system adoption: the mediating role of perceived risk and trust. *Journal of Science and Technology Policy Management*, *14*(4), 634–658.

Nguyen, T. T., Tran, T. N. H., Do, T. H. M., Dinh, T. K. L., Nguyen, T. U. N., & Dang, T. M. K. (2024). Digital literacy, online security behaviors and E-payment intention. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(2), 100292.

Okello Candiya Bongomin, G., & Ntayi, J. M. (2020). Mobile money adoption and usage and financial inclusion: mediating effect of digital consumer protection. *Digital Policy, Regulation and Governance*, *22*(3), 157–176.

Raza, M., Bilal, M. A., & Khan, A. B. (2024). FinTech Adoption and Sustainability Performance: The Role of Digital Financial Literacy and Financial Inclusion in Pakistan's Banking Sector. *Journal of Innovative Research in Management Sciences*, *5*(4), 74–98.

Reynon, M. K., Bulatao, P. C., Vergel, J. A. N. N., Yabut, L. A., & Grimaldo, J. U. N. (2022). Consumer's attitude on online payment systems as driven by risks. *Journal of Business and Management Studies*, *4*(2), 13–26.

Sabri, M. F., Suhaimi, S. S. A., Nazuri, N. S., Magli, A. S., Burhan, N. A. S., & Othman, M. A. (2023). The International Review of Financial Consumers. *The International Review of Financial Consumers*, 1.

Samonte, M. J. C., Ibarreta, M. V. O., Ilagan, K. A. A., & Justo, A. R. L. (2024). Mitigating Risk in the Digital Age: An Analysis of Security Measures for Cashless Payments in Developing Countries. *2024 4th International Conference on Computer Systems (ICCS)*, 186–191.

Sanchez, J. A. R., & Tanpoco, M. (2023). Continuance intention of mobile wallet usage in the philippines: A mediation analysis. *Review of Integrative Business and Economics Research*, *12*(3), 128–142.

Sandhu, S., Kai, J., Maity, R., Saad, A., Syed Abu Bakar, S. M., & Singh, H. (2022). Convenience and risk factors affecting mobile banking adoption behavior: The mediating role of trust. *Journal of Emerging Economies & Islamic Research*, *10*(2), 127–151.

Sarwar, U., Bint-e-Naeem, N., Fahmeed, L., & Atif, M. (2024). Role of perceived security and financial attitude in shaping behavioral intention under the moderation of financial literacy. *Journal of Asian Development Studies*, *13*(3), 1380–1395.

Simatele, M. (2024). Trust as a mediator for continued mobile financial service use: a case of the Eastern Cape Province of South Africa. *Journal of African Business*, *25*(2), 330–348.

Tanpoco, M., Katalbas, R. E. I. I. I., Roxas, R. R. P., An, J., & Orlina, J. Z. (2022). The moderating role of financial literacy on the effects of subjective norms, product involvement, and perceived behavioral control on invest-ment intention of young investors from a mobile wallet app in the Philippines. *International Journal of Multidisciplinary: Applied Business and Education Research*, *3*(8), 1477–1490.

Ullah, S., Kiani, U. S., Raza, B., & Mustafa, A. (2022). Consumers' intention to adopt m-payment/m-banking: the role of their financial skills and digital literacy. *Frontiers in Psychology*, *13*, 873708.

Yadav, M., & Banerji, P. (2024). Systematic literature review on digital financial literacy. *SN Business & Economics*, *4*(11), 142.