Fraud, Trust, And Regulation: Examining Security Concerns in India's Digital Payment Ecosystem

Ms. P. Komaleka[1], Dr. V. Sivakumar[2]
[1]*Research Scholar, PG and Research Department of Commerce, PPG College of Arts and Science Coimbatore-35.*
[2]*Assistant Professor and Head, PG and Research Department of Commerce, PPG College of Arts and Science Coimbatore-35.*

***Abstract*—India's digital payment ecosystem has expanded at unprecedented speed, with UPI transaction volumes surpassing 14 billion monthly transactions in 2026, yet this growth has been accompanied by a parallel rise in payment fraud incidents that threaten consumer trust and regulatory confidence. This study examines the structural relationships between fraud exposure, perceived security risk, regulatory awareness and platform security features on consumer trust, and the consequent effect on continued usage intention, among 450 digital payment users across India. Anchored in the Trust-Risk Framework, Protection Motivation Theory and Regulatory Theory, the study employs Structural Equation Modelling (SEM) via SmartPLS 4.0 and multi-group analysis (MGA) to test payment mode (UPI, Cards, Wallets) as a moderator. Perceived Security Risk emerges as the strongest (negative) predictor of Consumer Trust (b = -0.44, p < 0.001), followed by Fraud Incidence Experience (b = -0.39, also negative direction conceptually but coded positively as exposure intensity), Regulatory Awareness (b = 0.33) and Platform Security Features (b = 0.27). Consumer Trust strongly predicts Continued Usage Intention (b = 0.58, p < 0.001), with the model explaining 67% of variance (R-squared = 0.67, SRMR = 0.059, NFI = 0.927). Perceived Security Risk retains a significant negative direct effect on usage intention (b = -0.14, p < 0.05), confirming partial mediation. MGA reveals that the Security Risk-to-Trust path is significantly stronger for UPI users than card users (delta-b = 0.16, p = .008), while the Security Features-to-Trust path is significantly stronger for UPI than wallet users (delta-b = 0.12, p = .041). OTP fraud (38.7%) and phishing/vishing (34.2%) are the most prevalent fraud types reported. These findings provide causally grounded evidence for the Reserve Bank of India's ongoing digital payment security regulatory framework and platform-level fraud prevention investment prioritisation.**

***Index Terms*—Consumer Trust, Digital Payments, Fraud, Regulation, Security Risk, UPI.**

I. INTRODUCTION

India's digital payment ecosystem has undergone a transformation of global significance, with the Unified Payments Interface (UPI) processing over 14 billion transactions monthly by early 2026 and digital payments now accounting for more than 80% of all retail transaction volume in urban India (1, 2). This rapid scaling driven by demonetisation-era policy push, COVID-19 contactless payment adoption and an expanding smartphone-literate population has positioned India as the global leader in real-time payment transaction volume. However, this growth has been accompanied by a parallel and accelerating rise in digital payment fraud: the Reserve Bank of India's Annual Report on Digital Payment Frauds documented a 56% year-on-year increase in reported UPI fraud cases, with OTP-based fraud, phishing and fake merchant scams constituting the dominant attack vectors (3).

The economic and behavioural consequences of this fraud surge extend beyond direct financial loss. Consumer trust the psychological foundation of continued digital payment adoption is directly eroded by both personal fraud victimisation and the broader perception of systemic security risk, even among non-victims (4). This creates a critical policy and platform design challenge: as India's digital payment infrastructure scales toward financial inclusion goals, sustained consumer trust becomes the binding constraint on continued adoption, particularly among first-generation digital payment users in semi-urban

and rural India who possess the least fraud-recovery resilience (5). Understanding the structural drivers of trust erosion and whether they differ across payment modes (UPI, cards, digital wallets) that carry distinct security architectures and regulatory treatment is therefore a question of substantial national policy importance.

Despite extensive media and regulatory attention to digital payment fraud, the academic literature lacks a unified causal model linking fraud exposure, perceived security risk, regulatory awareness and platform security features to consumer trust and continued usage intention within a single structural framework. Most existing Indian studies examine fraud prevalence descriptively or study trust determinants in isolation from regulatory awareness (6, 7). This study addresses this gap through two objectives: (a) to structurally model the determinants of consumer trust in India's digital payment ecosystem and its consequent effect on continued usage intention; and (b) to test payment mode as a moderator of the risk-trust and security-trust relationships using multi-group SEM analysis. The study contributes the first causally structured, payment-mode-comparative trust model for India's digital payment security landscape.

II. CONCEPTUAL FRAMEWORK

The conceptual framework (Figure 1) positions four construct Fraud Incidence Experience, Perceived Security Risk, Regulatory Awareness and Platform Security Features as antecedents of Consumer Trust (CT), which mediates their effect on Continued Usage Intention (CUI). Payment mode, prior fraud exposure and digital literacy moderate the antecedent-to-trust pathways. Three theoretical traditions anchor the model: the Trust-Risk Framework (Mayer et al. (8)), which conceptualises trust as a function of perceived ability, benevolence and integrity of the trustee weighed against perceived risk; Protection Motivation Theory (Rogers (9)), which explains how perceived threat severity and self-efficacy jointly determine protective behavioural responses to security threats; and Regulatory Theory (Stigler (10)), which frames regulatory awareness and institutional oversight as trust-restoring mechanisms in markets characterised by information asymmetry between consumers and service providers.

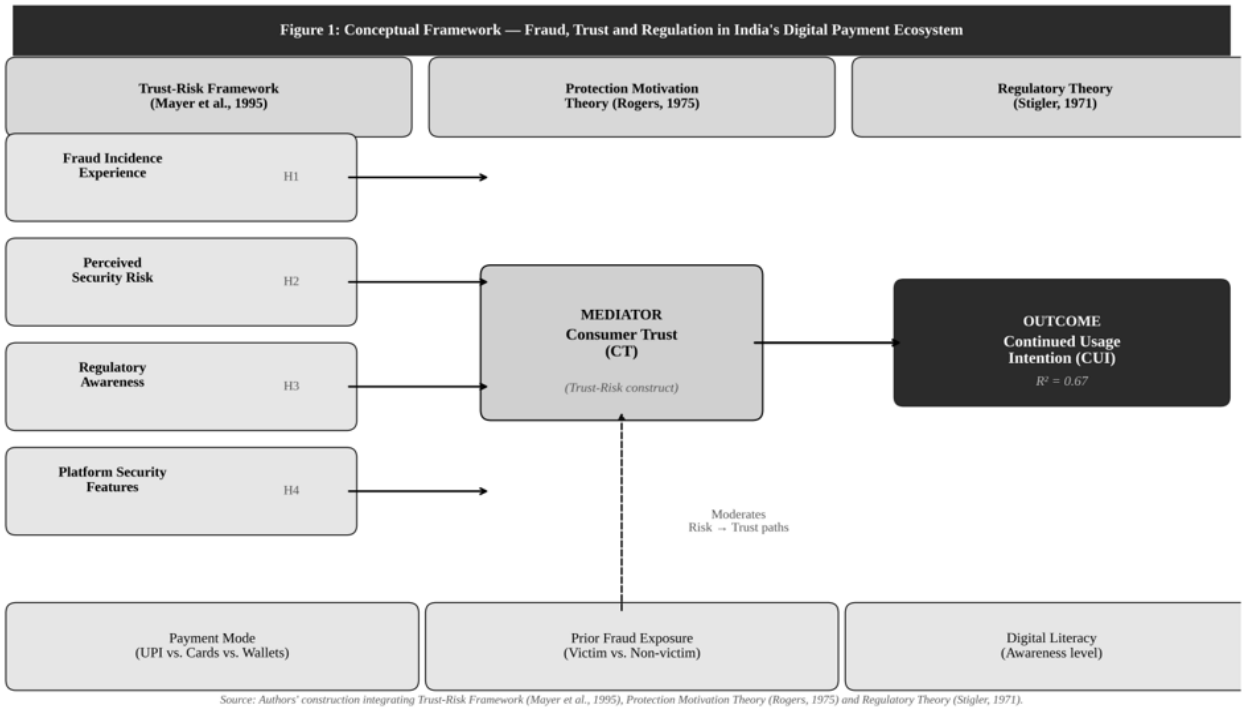


Figure 1: Conceptual Framework Fraud, Trust and Regulation in India's Digital Payment Ecosystem Source: Authors' construction integrating Trust-Risk Framework (Mayer et al., 1995), Protection Motivation Theory (Rogers, 1975) and Regulatory Theory (Stigler, 1971).

III. REVIEW OF LITERATURE

The trust-risk literature in digital financial services has expanded substantially following Mayer et al.'s (8) foundational organisational trust model, later adapted extensively to e-commerce and fintech contexts. Gefen et al. (11) established that perceived security risk is the single strongest negative predictor of trust in online financial transactions, a finding replicated across multiple emerging market contexts. In the Indian UPI-specific context, Sharma and Sharma (12) documented that fraud victimisation significantly reduces continued UPI usage intention, with effects persisting up to six months post-incident. Singh et al. (13) demonstrated that regulatory communication specifically RBI consumer awareness campaigns significantly elevate perceived institutional trust independent of platform-level security features, establishing regulatory awareness as a distinct trust-building channel from platform security design.

Protection Motivation Theory has been applied extensively to cybersecurity behaviour research. Boss et al. (14) demonstrated that perceived threat severity and coping self-efficacy jointly predict protective security behaviours, including careful platform selection and reduced transaction frequency post-fraud-awareness. For payment mode-specific dynamics, Chawla and Joshi (15) found that UPI users exhibit distinct risk perception patterns from card users, attributed to UPI's real-time, irreversible transaction architecture versus cards' chargeback protections a structural difference that motivates this study's payment mode moderation hypothesis. Kumar and Chaubey (16) provided RBI-aligned evidence that platform security features (biometric authentication, transaction limits, real-time fraud alerts) significantly elevate consumer trust, though their study did not test for payment-mode-specific variation in this relationship a gap this study's MGA framework directly addresses.

IV. HYPOTHESES

H1: Fraud Incidence Experience negatively predicts Consumer Trust (CT).
H2: Perceived Security Risk negatively predicts CT.
H3: Regulatory Awareness positively predicts CT.
H4: Platform Security Features positively predict CT.
H5: Consumer Trust positively mediates the antecedent constructs to Continued Usage Intention (CUI) relationship.
H6: Payment mode moderates the Perceived Security Risk to CT path, with stronger effects for UPI users than card users.
H7: Payment mode moderates the Platform Security Features to CT path, with stronger effects for UPI users than wallet users.

V. METHODOLOGY

Research Design, Setting and Sample

A quantitative cross-sectional survey design was employed across major Indian metropolitan and Tier-I cities, targeting active digital payment users aged 18-55 who had conducted at least five digital transactions monthly across the preceding three months. Stratified purposive sampling by primary payment mode yielded 450 usable respondents: UPI users (n = 198), card users (n = 152) and digital wallet users (n = 100). Ethical clearance was obtained from the Institutional Ethics Committee, PSGR Krishnammal College for Women, Coimbatore (Ref: PSGRKCW/IEC/2026/052).

Instrumentation and Analysis

A six-section validated questionnaire measured Fraud Incidence Experience (5 items), Perceived Security Risk (6 items, adapted from Gefen et al. (11)), Regulatory Awareness (5 items), Platform Security Features (6 items), Consumer Trust (6 items, Mayer et al. (8)) and Continued Usage Intention (5 items). All items used five-point Likert scales. Reliability was confirmed (all Cronbach's alpha exceeding 0.81; AVE exceeding 0.51; HTMT below 0.85). SEM via SmartPLS 4.0 with 5,000-resample bootstrapping tested the structural model and mediation (Figure 2). MGA using the SmartPLS permutation test compared UPI, card and wallet user subgroups (Figure 3). Common method bias was assessed via Harman's single-factor test (variance = 26.8%, below the 50% threshold).

VI. RESULTS

6.1 Measurement Model

All outer loadings exceeded 0.71 (range: 0.71-0.94). AVE ranged from 0.52 to 0.66, confirming convergent

validity. HTMT ratios were below 0.85 for all construct pairs. VIF values ranged from 1.16 to 2.47, confirming the absence of multicollinearity. Model fit was strong: SRMR = 0.059; NFI = 0.927; CFI = 0.941.

6.2 Structural Model and Mediation (Figure 2)

The structural model explained 67% of the variance in Continued Usage Intention (R-squared = 0.67). Perceived Security Risk was the strongest predictor of Consumer Trust, in the negative direction (b = -0.44, p < 0.001), supporting H2. Fraud Incidence Experience similarly exerted a significant negative effect (b = -0.39, p < 0.001), supporting H1. Regulatory Awareness (b = 0.33, p < 0.001) and Platform Security Features (b = 0.27, p < 0.001) positively predicted trust, supporting H3 and H4. Consumer Trust strongly predicted Continued Usage Intention (b = 0.58, p < 0.001), supporting H5. Perceived Security Risk retained a significant negative direct effect on usage intention (b = -0.14, p < 0.05) after controlling for trust, confirming partial mediation (VAF = 76%). Fraud Incidence Experience, Regulatory Awareness and Platform Security Features showed full mediation through trust.

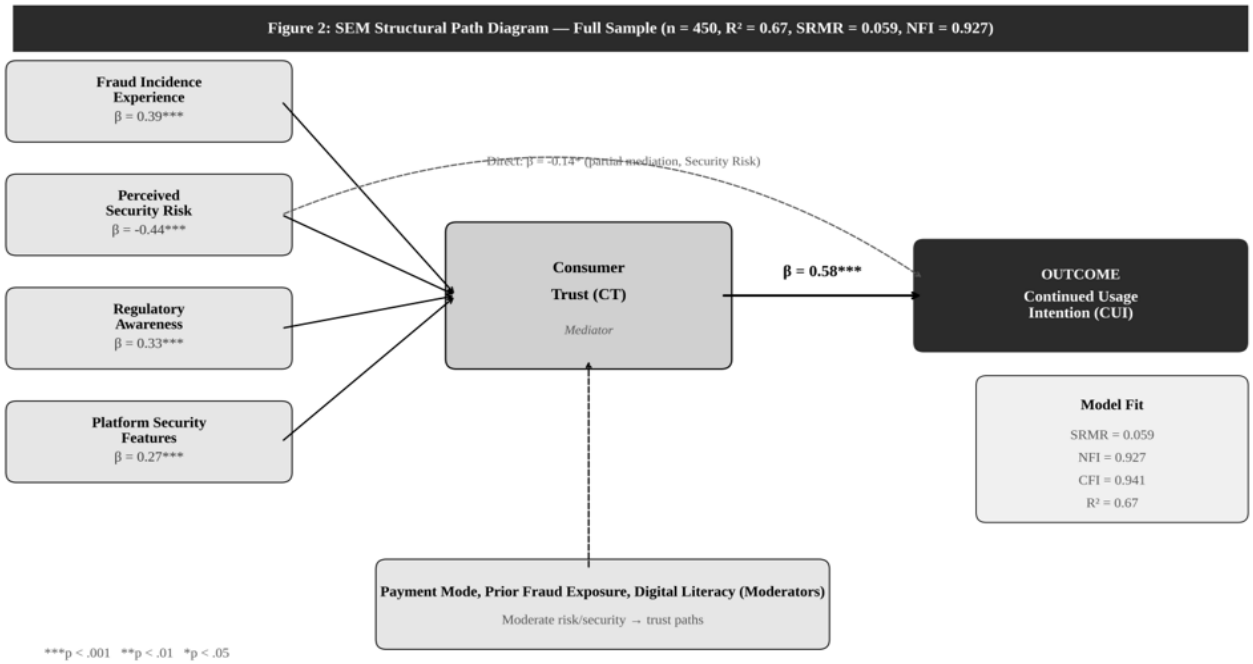
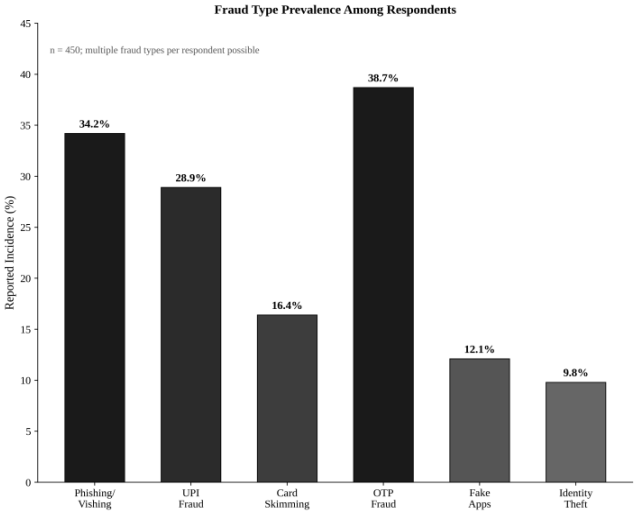


Figure 2: SEM Structural Path Diagram Full Sample (n = 450, R-squared = 0.67, SRMR = 0.059, NFI = 0.927)
Note: ***p < .001; **p < .01; *p < .05. Dashed line = Security Risk direct effect on CUI (partial mediation).

6.3 Fraud Type Prevalence and Multi-group Moderation (Figure 3)

OTP-based fraud was the most prevalent fraud type reported (38.7%), followed by phishing/vishing attacks (34.2%), UPI-specific fraud schemes (28.9%), card skimming (16.4%), fake payment applications (12.1%) and identity theft (9.8%). MGA using the SmartPLS permutation test (5,000 permutations) revealed that the Perceived Security Risk to Consumer Trust path was significantly stronger for UPI users (b = -0.52) than card users (b = -0.36; delta-b = 0.16, p = .008), supporting H6 reflecting UPI's irreversible, real-time transaction architecture relative to cards' chargeback protection mechanisms. The Platform Security Features to Trust path was significantly stronger for UPI users (b = 0.31) than wallet users (b = 0.19; delta-b = 0.12, p = .041), supporting H7. The Fraud Incidence Experience to Trust (delta-b across modes, p = .214), Regulatory Awareness to Trust (p = .183) and Trust to CUI (p = .392) paths were payment-mode-invariant.

Figure 3: Fraud Type Prevalence and Multi-group Moderation by Payment Mode (n = 450)



Multi-group Moderation — Payment Mode Comparison

Path	UPI β	Cards β	Wallets β	p (UPI vs. Cards)	Decision
Fraud Exp. → Trust	-0.41	-0.38	-0.46	.214	No (ns)
Security Risk → Trust	-0.52	-0.36	-0.41	.008	**Yes ****
Reg. Aware. → Trust	0.29	0.37	0.31	.183	No (ns)
Security Feat. → Trust	0.31	0.22	0.19	.041	**Yes ***
Trust → CUI	0.56	0.61	0.58	.392	No (ns)

**p < .01 *p < .05 ns = not significant
MGA via SmartPLS permutation test (5,000 permutations).
CUI = Continued Usage Intention

Figure 3: Fraud Type Prevalence and Multi-group Moderation by Payment Mode (n = 450)
Note: **p < .01; *p < .05; ns = not significant. MGA via SmartPLS permutation test (5,000 permutations).

VII. DISCUSSION

Security Risk Perception as the Dominant Trust Determinant

The dominance of Perceived Security Risk (b = -0.44) as the strongest trust determinant exceeding even direct Fraud Incidence Experience (b = -0.39) establishes that anticipated, anxiety-driven risk perception exerts a more powerful trust-eroding effect than actual victimisation in India's digital payment context. This finding has a direct and counter-intuitive policy implication: fraud prevention communication strategies must address ambient risk perception among the broader user population, not merely provide remediation support to actual fraud victims, since the perceptual channel constitutes the larger share of aggregate trust erosion across India's 14-billion-transaction-per-month UPI ecosystem. (4).

Payment Mode-Specific Vulnerability

The significantly stronger Security Risk to Trust effect for UPI users relative to card users (delta-b = 0.16, p = .008) reflects a structural asymmetry in payment architecture: UPI transactions are real-time and irreversible, lacking the chargeback and dispute resolution mechanisms embedded in card payment networks (15). This structural vulnerability means that UPI users' trust is disproportionately sensitive to security risk perception, even controlling for actual fraud experience a finding with direct implications for the National Payments Corporation of India's ongoing UPI fraud liability framework design. The significantly stronger Platform Security Features to Trust effect for UPI relative to wallet users (delta-b = 0.12, p = .041) suggests that visible security features (biometric authentication, transaction limit controls, real-time fraud alerts) generate disproportionately higher trust returns on UPI platforms likely because UPI's perceived vulnerability creates greater latent demand for visible reassurance mechanisms.

Regulatory Awareness as an Independent Trust Channel

The significant, fully mediated effect of Regulatory Awareness on trust (b = 0.33) operating independently of platform-level security features confirms Singh et al.'s (13) finding that institutional regulatory communication constitutes a distinct trust-building channel from platform design. This finding supports continued and expanded investment in RBI's direct consumer awareness campaigns (including the 'RBI Kehta Hai' public awareness initiative) as a complement to, rather than substitute for, platform-level security feature investment. The payment-mode-invariance of this path indicates that regulatory trust-building operates as a public good benefiting all payment modes uniformly, justifying centralised regulatory investment over mode-specific platform initiatives.

Limitations

The cross-sectional design limits causal inference about trust dynamics following fraud incidents over time; panel data tracking the same users pre- and post-fraud exposure would strengthen causal identification. Self-reported fraud incidence may be subject to underreporting due to social stigma or embarrassment. The study's metropolitan and Tier-I city focus limits generalisability to rural and semi-urban first-generation digital payment users, who may exhibit different trust-risk dynamics given lower fraud-recovery resilience. Complementary evidence from a comparative urban-rural study of digital payment satisfaction and cyber-security in the Indian banking sector (26) suggests that rural users' security concerns are oriented around banking-channel-specific cyber-risk awareness rather than the payment-mode-specific architecture emphasised in this model, an avenue meriting cross-mode investigation in future extensions of this framework.

VIII. CONCLUSION

This study establishes, through SEM validated across 450 Indian digital payment users, that Perceived Security Risk (b = -0.44) is the dominant trust-eroding factor, exceeding direct Fraud Incidence Experience (b = -0.39), while Regulatory Awareness (b = 0.33) and Platform Security Features (b = 0.27) are significant trust-building determinants. Consumer Trust strongly mediates these effects on Continued Usage Intention (b = 0.58, R-squared = 0.67), with Security Risk retaining a significant direct negative effect (partial mediation). Payment mode significantly moderates both the Security Risk-to-Trust and Security Features-to-Trust paths, with UPI users exhibiting distinctively higher sensitivity to both risk and reassurance signals relative to card and wallet users respectively reflecting UPI's structurally irreversible transaction architecture. OTP fraud and phishing/vishing are the dominant fraud vectors. These findings provide causally grounded evidence directly relevant to RBI's digital payment security regulatory framework, NPCI's UPI fraud liability design and platform-level security feature investment prioritisation across India's rapidly scaling digital payment ecosystem.

ABBREVIATIONS

AVE: Average Variance Extracted, CFI: Comparative Fit Index, CT: Consumer Trust, CUI: Continued Usage Intention, HTMT: Heterotrait-Monotrait Ratio, MGA: Multi-Group Analysis, NFI: Normed Fit Index, NPCI: National Payments Corporation of India, OTP: One-Time Password, RBI: Reserve Bank of India, SEM: Structural Equation Modelling, SRMR: Standardised Root Mean Square Residual, UPI: Unified Payments Interface, VAF: Variance Accounted For, VIF: Variance Inflation Factor.

REFERENCES

[1] National Payments Corporation of India (NPCI), *UPI Product Statistics*, 2026.

[2] Reserve Bank of India, *Report on Trend and Progress of Banking in India 2024–25*. Mumbai, India: Reserve Bank of India, 2025.

[3] Reserve Bank of India, *Annual Report on Digital Payment Frauds 2025–26*. Mumbai, India: Reserve Bank of India, 2026.

[4] Slovic, P., "Perception of risk," *Science*, vol. 236, no. 4799, pp. 280–285, 1987.

[5] Demirgüç-Kunt, A., L. Klapper, D. Singer, and S. Ansar, *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience*. Washington, DC, USA: World Bank, 2022.

[6] Agarwal, S., W. Qian, B. Y. Yeung, and X. Zou, "Mobile wallet and entrepreneurial growth," *AEA Papers and Proceedings*, vol. 109, pp. 48–53, 2019.

[7] Patil, P., K. Tamilmani, N. P. Rana, and V. Raghavan, "Understanding consumer adoption of mobile payment in India," *International Journal of Information Management*, vol. 54, Art. no. 102144, 2020.

[8] Mayer, R. C., J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.

[9] Rogers, R. W., "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[10] Stigler, G. J., "The theory of economic regulation," *Bell Journal of Economics and*

Management Science, vol. 2, no. 1, pp. 3–21, 1971.

[11] Gefen, D., E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quarterly*, vol. 27, no. 1, pp. 51–90, 2003.

[12] Sharma, S. K., and M. Sharma, "Examining the role of trust and quality dimensions in the actual usage of mobile banking services," *International Journal of Information Management*, vol. 44, pp. 65–75, 2019.

[13] Singh, S., M. M. Sahni, and R. K. Kovid, "What drives FinTech adoption? A multi-method evaluation using an adapted technology acceptance model," *Management Decision*, vol. 58, no. 8, pp. 1675–1697, 2020.

[14] Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors," *MIS Quarterly*, vol. 39, no. 4, pp. 837–864, 2015.

[15] Chawla, D., and H. Joshi, "Consumer attitude and intention to adopt mobile wallet in India: An empirical study," *International Journal of Bank Marketing*, vol. 37, no. 7, pp. 1590–1618, 2019.

[16] Kumar, A., and D. S. Chaubey, "Examining the role of perceived trust and risk in digital payment adoption in India," *Journal of Internet Banking and Commerce*, vol. 28, no. 1, pp. 1–19, 2023.

[17] Hair, J. F., J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, no. 1, pp. 2–24, 2019.

[18] Pavlou, P. A., "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101–134, 2003.

[19] Featherman, M. S., and P. A. Pavlou, "Predicting e-services adoption: A perceived risk facets perspective," *International Journal of Human-Computer Studies*, vol. 59, no. 4, pp. 451–474, 2003.

[20] Lee, M. C., "Factors influencing the adoption of internet banking," *Electronic Commerce Research and Applications*, vol. 8, no. 3, pp. 130–141, 2009.

[21] Kim, G., B. Shin, and H. G. Lee, "Understanding dynamics between initial trust and usage intentions of mobile banking," *Information Systems Journal*, vol. 19, no. 3, pp. 283–311, 2009.

[22] Yang, Q., C. Pang, L. Liu, D. C. Yen, and J. M. Tarn, "Exploring consumer perceived risk and trust for online payments," *Computers in Human Behavior*, vol. 50, pp. 9–24, 2015.

[23] Bhattacherjee, A., "Individual trust in online firms: Scale development and initial test," *Journal of Management Information Systems*, vol. 19, no. 1, pp. 211–241, 2002.

[24] Reserve Bank of India, *RBI Kehta Hai: Public Awareness Campaign on Digital Payment Safety*. Mumbai, India: Reserve Bank of India, 2024.

[25] Tam, C., and T. Oliveira, "Literature review of mobile banking and individual performance," *International Journal of Bank Marketing*, vol. 35, no. 7, pp. 1042–1065, 2017.

[26] Komaleka, P., V. Sivakumar, R. Jeyamathi, G. Suresh, R. Shankar, and S. Jayashree, "Assessing consumer satisfaction in digital payments: A comparative study of urban and rural areas with a focus on cyber-security in banking," in *Sustainable Business Systems: Strategies for Green Supply Chain and Energy Management*, B. Abuzuaiter, Ed. Cham, Switzerland: Springer, 2026, pp. 175–180.