FINANCIAL LITERACY AND CYBERSECURITY AWARENESS

Beyond Cashless Convenience: Understanding Financial Literacy, Cyber Fraud Vulnerabilities, and UPI Security Practices in the Modern Economy

Harshal Balwani, Anshuman Coomar

Department of Business Administration, Amity Business School, Amity University, Navi Mumbai, Maharashtra, India

Published November 2026

Abstract

The rapid proliferation of digital payment technologies has transformed retail commerce in India, positioning the Unified Payments Interface (UPI) as the primary transaction architecture across campuses and commercial markets. However, high operational usage does not necessarily equate to comprehensive financial capability or cybersecurity hygiene. This study examines the personal financial literacy competencies, cyber fraud vulnerabilities, and UPI security practices of retail consumers and micro-merchants based on a primary empirical survey of 120 respondents in Navi Mumbai, Maharashtra, utilizing a descriptive research design and structured bilingual questionnaires. The sample encompassed undergraduate students (61.7%), salaried young professionals (25.8%), and local micro-retailers (12.5%). The findings reveal near-universal formal banking inclusion (95.0%) and high daily UPI adoption (90.8%), yet expose critical cognitive and behavioral deficits: 78.3% of respondents budget irregularly or never, 51.7% cannot differentiate capital preservation (saving) from capital growth (investing), and 36.7% harbor the dangerous misconception that a UPI PIN is required to receive incoming funds. Furthermore, while 81.7% have been targeted by fraudulent communication and 36.7% have experienced fraud directly or through close contacts, 71.7% are completely unaware of the National Cybercrime Helpline 1930 or the critical 'Golden Hour' fund-freezing protocol. An overwhelming 88.4% expressed active demand for structured, peer-led safety workshops. The study concludes that sustainable digital financial inclusion requires shifting focus from transactional onboarding to practical, peer-led behavioral education, automated application safeguards, and prominent institutional dispute escalation mechanisms.

Keywords: 1930 Helpline; behavioral economics; consumer protection; cyber fraud; digital payments; financial literacy; Navi Mumbai; phishing; UPI security

1 Introduction

Financial literacy represents the cognitive, behavioral, and analytical capacity of individuals to comprehend, manage, and optimize personal economic resources to sustain material well-being across life stages. Historically, economic literature evaluated financial competence through physical, tangible instruments: balancing handwritten passbooks, maintaining cash allocation envelopes, calculating compound interest manually, and purchasing physical sovereign savings certificates.

With the dematerialization of money into distributed electronic database ledgers and real-time clearing switches, retail payments have undergone an unprecedented transformation. In India, the Unified Payments Interface (UPI), developed by the National Payments Corporation of India (NPCI) and regulated by the Reserve Bank of India (RBI), has emerged as the world's most widely adopted real-time payment architecture. Built upon Immediate Payment Service (IMPS) rails, UPI enables

instant, direct interbank fund transfers via Virtual Payment Addresses (VPAs) and QR codes without disclosing sensitive bank account or branch credentials.

However, in a smartphone-mediated cashless ecosystem, financial literacy can no longer be decoupled from digital operational literacy and cyber defense hygiene. A consumer who understands compounding returns but cannot identify a spoofed payment gateway or phishing link remains acutely vulnerable to catastrophic capital loss. Modern digital financial literacy therefore operates as an interdependent tripartite structure:

- **Fundamental Financial Prudence:** Cash flow budgeting, debt avoidance, regular savings habits, and understanding inflation.
- **Digital Operational Fluency:** Navigating payment applications, checking transaction logs, scanning QR codes, and executing P2P/P2M transfers.
- **Cyber Hygiene & Fraud Defense:** Maintaining strict credential secrecy (PIN, OTP), recognizing social engineering tactics, and executing emergency fraud reporting via official channels.

2 Problem statement

While payment application interfaces are deliberately engineered to minimize operational friction and maximize transaction throughput, public security literacy has not kept pace. Young digital natives navigate smartphone applications with tactile fluency, but field observations reveal an alarming 'Operational Fluency vs. Security Literacy' paradox: users frequently mistake tactile application familiarity for cybersecurity competence. Furthermore, the absence of physical currency depletion creates a 'frictionless spending bias,' accelerating micro-transaction leakage among youth. Concurrently, cybercriminals exploit cognitive blind spots through reverse 'Collect Request' scams, remote desktop screen-sharing manipulation, and counterfeit merchant QR overlays. This study investigates the empirical extent of these vulnerabilities across students, working adults, and micro-vendors in Navi Mumbai.

3 Objectives of the study

1. To evaluate the baseline level of personal financial literacy, budgeting regularity, and savings discipline among students and community members.
2. To examine the level of awareness regarding online financial frauds, phishing schemes, and deceptive payment prompts.
3. To assess adherence to essential UPI security practices, specifically the fundamental UPI PIN directional rule (sending vs. receiving funds).
4. To analyze the institutional emergency reporting gap concerning the National Cybercrime Helpline 1930 and the Golden Hour fund-freezing protocol.
5. To measure community demand for structured digital safety educational programs and formulate actionable policy recommendations for consumers, institutions, and FinTech platforms.

4 Research questions and hypothesis

- **RQ1:** Does near-universal smartphone payment adoption translate into adequate conceptual financial literacy and budgeting discipline?

- **RQ2:** What is the extent of public vulnerability regarding the fundamental UPI PIN directional rule during reverse collect request scams?
- **RQ3:** How widespread is cyber fraud exposure and victimization across collegiate and commercial demographics?
- **RQ4:** What is the level of awareness regarding emergency dispute escalation channels (Helpline 1930) following a fraudulent transaction?

Hypothesis (H1): High operational dexterity in executing digital payments does not significantly correlate with conceptual financial literacy, cyber hygiene adherence, or emergency fraud dispute readiness.

5 Literature review

This study builds upon and extends key institutional frameworks and behavioral economics literature:

- **National Centre for Financial Education (NCFE, 2020):** In the National Strategy for Financial Education (NSFE 2020-2025), the technical committee identifies core financial competencies—budgeting, savings discipline, and risk management—as vital prerequisites for inclusive economic stability.
- **Reserve Bank of India (RBI, 2021, 2023):** The Payment and Settlement Systems Vision 2021-2025 emphasizes safety, security, and customer protection. The RBI Integrated Ombudsman Scheme reports indicate that digital payment disputes and social engineering frauds represent the fastest-growing categories of consumer grievances.
- **National Payments Corporation of India (NPCI, 2024):** Technical guidelines define the architectural distinction between push (payer-initiated credit) and pull (payee-initiated collect) transactions, establishing that PIN entry is exclusively an authorization for account debit.
- **Ministry of Home Affairs (MHA / I4C, 2023):** The Citizen Financial Cyber Fraud Reporting & Management System (CFCFRMS) operational manual defines the 'Golden Hour' protocol (reporting within 2 to 24 hours via 1930) as essential for freezing illicit fund dispersion across mule accounts.
- **Behavioral Economic Theories:** Lusardi and Mitchell (2014) demonstrate that planning and budgeting are strongly associated with long-term wealth accumulation. Prelec and Loewenstein (1998) establish that cashless transactions decouple the pain of paying from consumption, inducing frictionless spending biases. Kahneman (2011) explains how heuristic cognitive shortcuts leave users vulnerable to high-pressure social engineering tactics.

Gap Addressed: While institutional literature details regulatory frameworks and technical switches, empirical field-based baselines measuring grassroots behavioral compliance, PIN misconceptions, and reporting literacy among common users remain scarce. This study provides that primary empirical baseline.

6 Research methodology

- **Research Design:** Descriptive empirical research design evaluating baseline competencies and behavioral vulnerabilities.

- **Target Population & Study Area:** Navi Mumbai, Maharashtra, encompassing university campus clusters, hostel common areas, commercial market streets, and vendor stalls.
- **Sample Size:** 120 validated respondents across three distinct user cohorts.
- **Sampling Method:** Purposive sampling technique ensuring balanced representation across key demographic segments.
- **Data Source & Collection:** Primary data collected via structured, 18-question bilingual questionnaires administered in-person and through digital forms.
- **Variables Studied:** Bank inclusion, budgeting regularity, savings vs. investing distinction, fraud exposure, OTP confidentiality, Helpline 1930 awareness, UPI adoption, PIN directional comprehension, and workshop demand.

Table 1. Composition of the survey sample (N = 120).

Group	Target Demographic Segment	Responses	Share (%)
Group A	Undergraduate & Postgraduate University Students	74	61.7%
Group B	Salaried Young Professionals & Office Staff	31	25.8%
Group C	Small Shopkeepers, Tuck Shops & Street Vendors	15	12.5%

7 Data analysis and interpretation

7.1 Personal financial habits and the budgeting deficit

The survey demonstrates near-universal institutional financial inclusion, with 95.0% (n=114) of participants holding an active bank account, primarily driven by digital student onboarding and Jan Dhan initiatives. However, account ownership does not translate into financial discipline. Only 21.7% (n=26) of respondents consistently prepare a monthly budget, while 43.3% (n=52) budget sporadically and 35.0% (n=42) maintain no budget at all. As illustrated in Figure 1, nearly four out of five respondents (78.3%) manage funds without systematic planning. This behavior is strongly linked to the frictionless spending bias of digital payments: cashless transactions reduce the sensory 'pain of paying', accelerating micro-expenditure leakage over time.

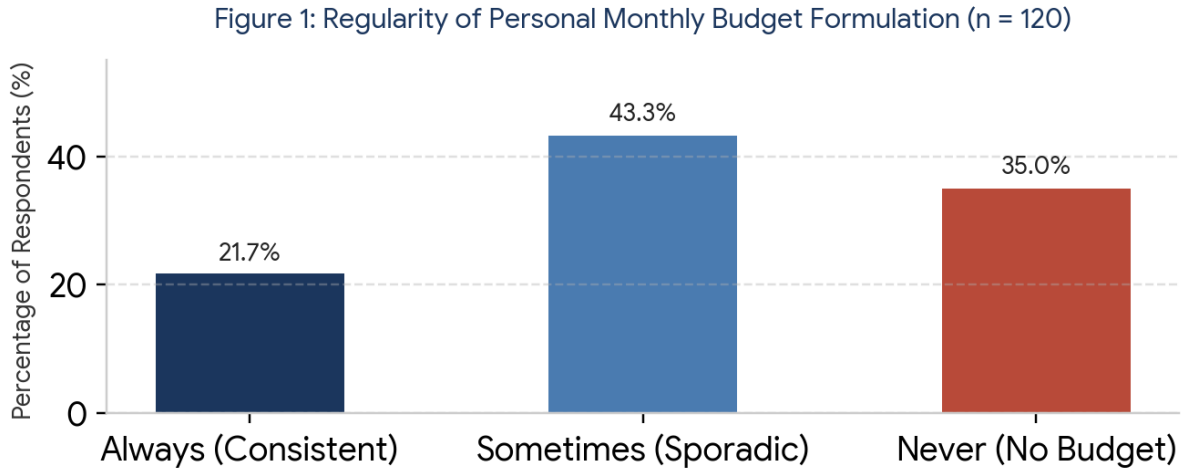


Figure 1. Regularity of Personal Monthly Budget Formulation (n = 120).

7.2 The conceptual wealth gap: saving vs. investing

While 58.3% (n=70) of respondents report setting aside savings regularly, qualitative follow-ups indicate that savings are largely treated as an afterthought ('residual saving' of whatever remains at month-end) rather than deliberate accumulation. Crucially, 51.7% (n=62) of respondents cannot articulate the fundamental difference between saving and investing, erroneously conflating idle bank balances with inflation-hedged wealth creation. Furthermore, 60.0% of participants rate their financial knowledge as 'Average' or 'Poor', and 81.7% (n=98) have never attended a structured financial literacy workshop.

Table 2. Personal financial literacy competencies (n = 120).

Core Competency Metric	Response Options	Count (n)	Share (%)
Bank Account Ownership	Yes / No	114 / 6	95.0% / 5.0%
Budget Preparation	Always / Sometimes / Never	26 / 52 / 42	21.7% / 43.3% / 35.0%
Regular Monthly Savings	Yes / No	70 / 50	58.3% / 41.7%
Saving vs. Investing Distinction	Aware (Yes) / Unaware (No)	58 / 62	48.3% / 51.7%
Prior Literacy Program	Attended (Yes) / Never (No)	22 / 98	18.3% / 81.7%

7.3 Digital fraud exposure and victimization rates

Exposure to cyber fraud is pervasive across the sample: 81.7% (n=98) of respondents reported receiving fraudulent phone calls, fake electricity bill SMS alerts, or suspicious collect requests. More critically, 36.7% (n=44) confirmed direct financial loss or victimization within their immediate family and peer circle. As shown in Figure 2, retail users operate within an active cyber threat landscape where social engineering attempts are routine occurrences.

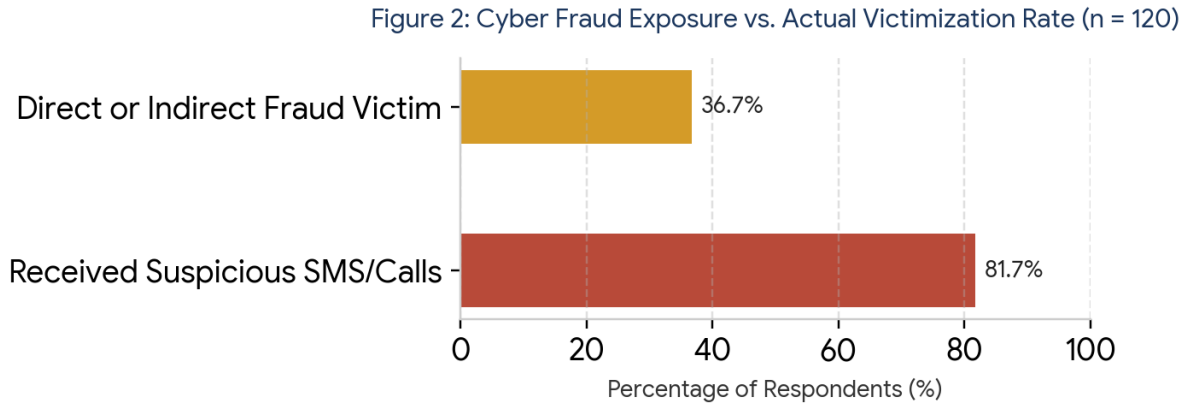


Figure 2. Cyber Fraud Exposure vs. Actual Victimization Rate (n = 120).

7.4 The operational fluency vs. security literacy disconnect: the UPI PIN directional gap

UPI adoption is widespread, with 90.8% (n=109) using payment apps daily. PhonePe (44.2%) and Google Pay (38.3%) dominate market share, capturing 82.5% of user activity. However, the study uncovered a critical security vulnerability: 36.7% (n=44) of respondents believe or are unsure whether entering a UPI PIN is required to receive incoming payments (Figure 3). This conceptual error is the precise attack vector exploited in online marketplace scams (e.g., OLX collect requests),

where fraudsters trick victims into authorizing debits under the guise of receiving cash advances or prize rewards.

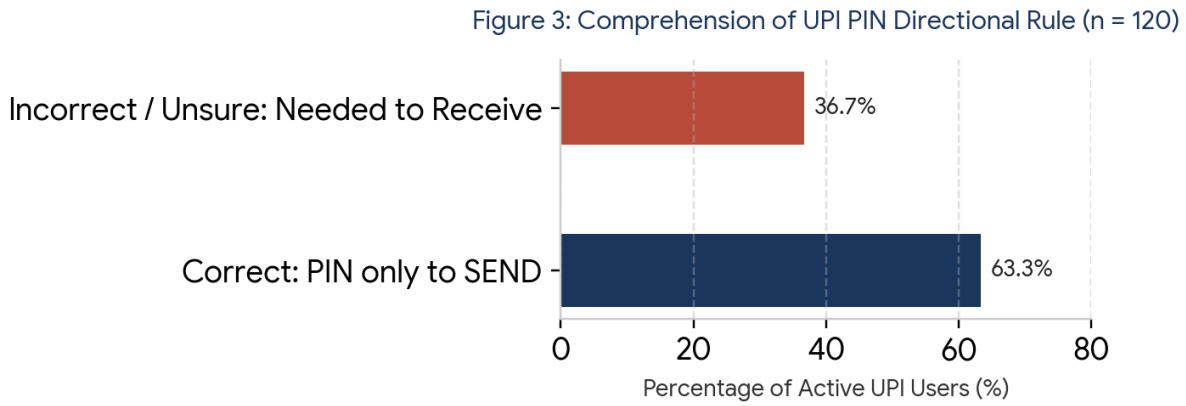


Figure 3. Comprehension of UPI PIN Directional Rule (n = 120).

7.5 Verification discipline and the 1930 emergency Helpline blindspot

While OTP confidentiality messaging has achieved strong cognitive penetration (91.7% aware), user verification habits remain inconsistent: only 38.3% (n=46) always verify links/QRs before transacting, and 38.3% do not consistently check the receiver's registered legal name. Most alarmingly, 71.7% (n=86) have no knowledge of the National Cybercrime Helpline 1930 or the Golden Hour fund-freezing mechanism (Figure 4). When fraud occurs, victims typically delay reporting, allowing fraudsters to disperse funds through mule accounts and cash ATM withdrawals.

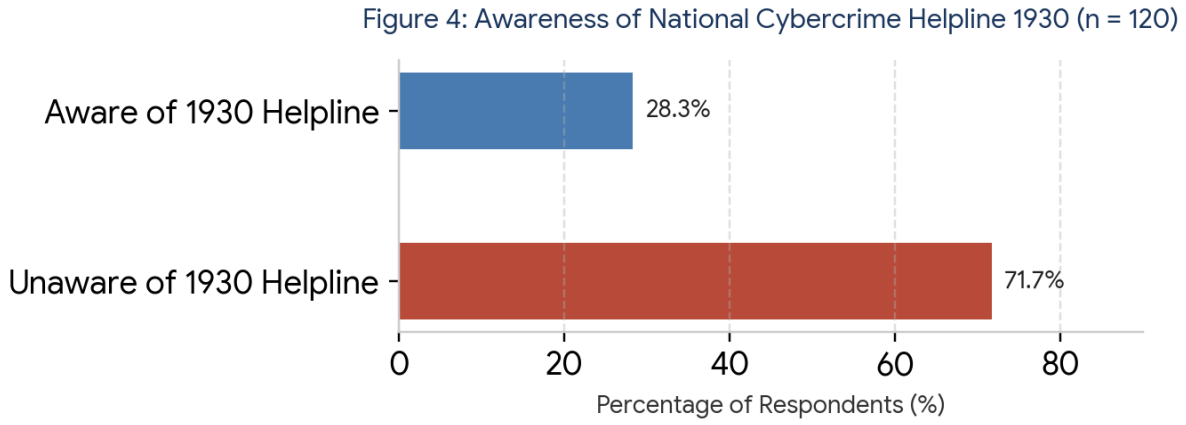


Figure 4. Awareness of National Cybercrime Helpline 1930 (n = 120).

7.6 Community demand for safety programs

An overwhelming 88.4% (n=106) of respondents expressed positive demand (56.7% Strongly Agree, 31.7% Agree) for regular, community-level digital financial safety workshops (Figure 5). This confirms that community members recognize their operational vulnerabilities and actively welcome structured, peer-led educational interventions.

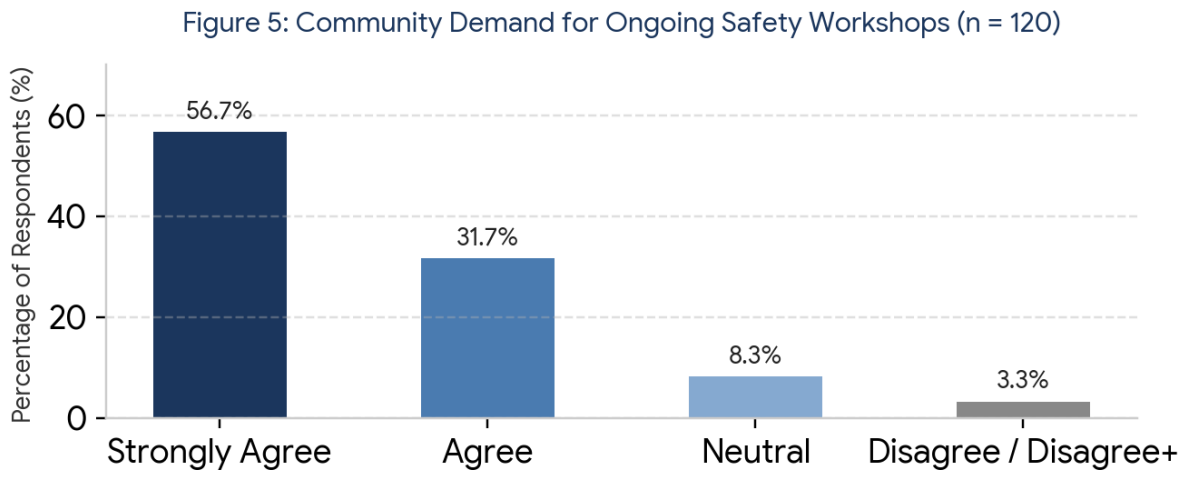


Figure 5. Community Demand for Ongoing Safety Workshops (n = 120).

8 Findings

1. Near-universal bank inclusion (95.0%) coexists with a severe personal budgeting deficit (78.3% budget irregularly or never), driven by frictionless cashless spending biases.
2. A conceptual wealth creation gap exists: 51.7% of respondents cannot distinguish saving from investing, leaving uninvested capital vulnerable to inflation erosion.
3. A critical 'Operational Fluency vs. Security Literacy' disconnect is evident: while 90.8% use UPI apps daily, 36.7% fail to understand the fundamental UPI PIN directional rule.
4. Cyber fraud targeting is pervasive (81.7% exposure), resulting in a high direct or indirect victimization rate of 36.7% across the community.
5. A severe institutional emergency escalation blindspot exists: 71.7% of respondents are unaware of the National Cybercrime Helpline 1930.
6. Market platform concentration is duopolistic: PhonePe (44.2%) and Google Pay (38.3%) capture 82.5% of total user volume.
7. Community receptivity to digital safety education is exceptionally high (88.4% positive demand), validating peer-led outreach as an effective educational model.

Table 3. Consolidated key empirical findings (N = 120).

Core Empirical Indicator	Result (Count & Share)
Total Respondents Surveyed	120 (100.0%)
Hold Active Bank Account	114 (95.0%)
Prepare Monthly Budget Consistently	26 (21.7%)
Budget Irregularly or Never	94 (78.3%)
Save Part of Income/Allowance Regularly	70 (58.3%)
Cannot Differentiate Saving from Investing	62 (51.7%)
Rate Personal Financial Knowledge Average or Poor	72 (60.0%)
Never Attended Formal Financial Literacy Training	98 (81.7%)
Received Fraudulent Phone Calls / Phishing SMS	98 (81.7%)

Core Empirical Indicator	Result (Count & Share)
Direct or Indirect Fraud Victimization Experience	44 (36.7%)
Aware that OTP Should Never Be Shared	110 (91.7%)
Unaware of 1930 Cybercrime Helpline	86 (71.7%)
Active Daily UPI Payment Users	109 (90.8%)
PhonePe Market Share	53 (44.2%)
Google Pay Market Share	46 (38.3%)
Misunderstand UPI PIN Directional Rule (Believe PIN needed to receive)	44 (36.7%)
Admit Sharing Banking Passwords / UPI PINs	14 (11.7%)
Always Verify Legal Beneficiary Name Before Payment	74 (61.7%)
Support Regular Community Digital Safety Workshops	106 (88.4%)

9 Suggestions and recommendations

- **For Individual Consumers:** Internalize the PIN Directional Rule: Remember that a UPI PIN is strictly an authorization to debit funds. Entering a PIN will never credit money. Always verify the registered legal name of the receiver before confirming transactions.
- **For Micro-Merchants:** Protect Countertop QR Stands: Regularly inspect physical QR standees for fraudulent sticker overlays, and rely on voice soundbox announcements rather than customer phone screens, which can show fabricated payment screenshots.
- **For Academic Institutions:** Mandatory Campus Cyber Hygiene: Higher education institutions should incorporate practical digital financial literacy and fraud mitigation modules into first-year student orientations, prominently displaying 1930 helpline banners across campuses.
- **For FinTech Platforms & Regulators:** Dynamic Warning Prompts: Payment applications must replace generic PIN entry screens with high-contrast, mandatory confirmation dialogs for collect requests that state in bold: 'WARNING: YOU ARE ABOUT TO PAY MONEY, NOT RECEIVE IT.' In-app one-tap emergency account freezes should also be implemented.
- **For Policy & Community Initiatives:** Scalable Peer-to-Peer Workshops: Regulators and merchant associations should partner with university student extension programs to deliver recurring, localized digital safety demonstrations.

10 Conclusion

India's digital payment revolution, spearheaded by the UPI ecosystem, has successfully dematerialized retail transactions, delivering remarkable speed and convenience across all demographic segments. However, this study demonstrates that high operational adoption does not equal financial safety or conceptual capability. A dangerous gap exists between user tactile dexterity and security literacy: over one-third of active users do not understand the UPI PIN directional rule, over 70% are unaware of the emergency 1930 helpline, and nearly 80% manage funds without budgeting discipline. Resolving these challenges requires shifting the policy and institutional focus from transactional onboarding to practical, peer-to-peer behavioral education, cognitive friction in user interface designs, and accessible dispute resolution mechanisms. Ensuring digital financial safety is essential to sustaining public trust in India's cashless digital economy.

11 Limitations and scope for further research

- **Sample Boundaries:** The sample of 120 respondents was drawn from urban collegiate and commercial zones in Navi Mumbai using purposive sampling, and may not fully generalize to rural or semi-urban populations.
- **Observational Scope:** The study captures self-reported behaviors and cross-sectional baseline perceptions; it did not track longitudinal financial performance or post-victimization recovery outcomes over time.
- **Scope for Further Research:** Future studies should conduct longitudinal evaluations after 6 and 12 months to measure knowledge retention following outreach interventions, expand comparative analysis to Tier-2 and rural merchant clusters, and assess the effectiveness of video-based versus hands-on demonstrations.

Acknowledgement

The authors carried out this study under the guidance of Dr. Bhojraj Y. Shewale, Assistant Professor.

References

[1] Chaffey, D., & Ellis-Chadwick, F. (2022). Digital marketing and fintech interface: Strategy, implementation and practice (8th ed.). *Harlow: Pearson Education*.

[2] Kahneman, D. (2011). Thinking, fast and slow. *New York: Farrar*, Straus and Giroux.

[3] Kotler, P., Kartajaya, H., & Setiawan, I. (2021). Marketing 5.0: Technology for humanity. *Hoboken*, NJ: John Wiley & Sons.

[4] Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. Journal of Economic Literature, 52(1), 5–44.

[5] Ministry of Home Affairs (MHA), Government of India. (2023). Citizen Financial Cyber Fraud Reporting & Management System (CFCFRMS / 1930 Helpline) operational manual. *Indian Cyber Crime Coordination Centre (I4C)*.

[6] Mukhopadhyay, B. (2020). Understanding digital public infrastructure: The growth and impact of India's UPI ecosystem. Journal of Payments Strategy & Systems, 14(2), 112–126.

[7] National Centre for Financial Education (NCFE). (2020). National strategy for financial education (NSFE 2020–2025). *Technical Group on Financial Inclusion and Financial Literacy*, RBI, SEBI, IRDAI, PFRDA.

[8] National Payments Corporation of India (NPCI). (2024). Unified Payments Interface (UPI): Procedural guidelines, system architecture and security protocols. https://www.npci.org.in

[9] Prelec, D., & Loewenstein, G. (1998). The red and the black: Mental accounting of savings and debt. Marketing Science, 17(1), 4–28.

[10] Reserve Bank of India (RBI). (2021). Payment and settlement systems in India: Vision 2021–2025. *Mumbai: Central Office*.

[11] Reserve Bank of India (RBI). (2023). Annual report on the Reserve Bank - Integrated Ombudsman Scheme (2022–23). *Mumbai: Department of Regulation*.

[12] Thaler, R. H., & Shefrin, H. M. (1981). An economic theory of self-control. Journal of Political Economy, 89(2), 392–406.

[13] Primary Fieldwork: Balwani, H., & Coomar, A. (2026). Primary survey of 120 citizens, students, and micro-merchants on financial literacy, digital payment habits, and UPI cyber security in Navi Mumbai. *Unpublished empirical dataset*, Amity Business School, Amity University.