

THE TRUST DEFICIT: CYBER SECURITY AS THE CORNERSTONE OF DIGITAL FINANCIAL INCLUSION'S NEXT PHASE

 Rakesh Singh*

 Manish Kumar**

 Shashi Bhushan Yadav***

 Sagar Soni****

 Rishu Singh*****

 Priti Neha Bara*****

Abstract

India's financial inclusion journey has achieved remarkable milestones - 58.70 crore Jan Dhan beneficiaries, a Financial Inclusion Index (FI-Index) of 70 and global leadership in real-time digital payments. Yet this expansion carries an underappreciated challenge, the rapid growth of digital financial services has also been accompanied by a significant increase in financial cyber fraud, highlighting the growing importance of cyber security within the digital financial ecosystem. This study argues that cyber security is no longer merely a technological concern for banks but a foundational trust infrastructure upon which Digital Financial Inclusion must be built. Unless digitally included population can transact with confidence and safety, the gains of the past decade may be undermined by a trust deficit that weakens sustained adoption of digital financial services. Drawing on data from regulatory reports and previous literature, this study examines the evolving financial cyber fraud landscape, assesses the regulatory response and proposes an integrated Cyber-Inclusive Finance Framework for strengthening trust, resilience and the long-term sustainability of India's digital financial inclusion agenda.

Keywords

Cyber security, Digital financial inclusion, Trust deficit, Newly included digital payment users

Introduction

The decade-long journey of financial inclusion in India is one of the most remarkable achievements of the twenty-first century. The Pradhan Mantri Jan Dhan Yojana (PMJDY) had enrolled 58.70 crore citizens in the formal banking system as on July 8, 2026¹, while the Unified Payments Interface (UPI) contributing to - with transaction of value 22,716.07 million and value of 28,92,138.67 crore, as of June 2026². The Financial Inclusion Index (FI-Index) for India increased to 70.0 in March 2026 from 67.0 in March 2025³, bringing the

country to the ranks of the fastest-improving nations in formal banking penetration (ORF, 2026).

Yet there is a paradox in this success which needs to be addressed immediately. The same infrastructure - Aadhaar-linked bank accounts, UPI-enabled smartphones and the Business Correspondent (BC) network - that has brought financial services to the previously unbanked population, has simultaneously opened an unparalleled attack surface for cybercriminals. In 2024, India recorded 22.68 lakh cybercrime incidents on the National Cyber Crime

* /*** /**** /***** /***** Research Associate, Bank of Baroda.

** Chief Manager, Bank of Baroda.

Disclaimer: The views expressed in this article are those of the author(s) and do not represent the official positions of any institution with which the author(s) may be affiliated.

¹PMJDY Progress Report, <https://pmjdy.gov.in/account>

²<https://www.npci.org.in/product/upi/product-statistics>

³Financial Inclusion Index for March 2026, RBI, https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=63164

Reporting Portal (NCRP) - up from 10.29 lakh in 2022. In 2025, the country recorded around 25 lakh cases of cyber crime. 70% of the reported cases were related to financial frauds, such as phishing, theft of One-Time Password (OTP), fake investment schemes and others. India's cybercrime landscape has grown by up to 400% since 2021, with the rural and semi-urban regions, where financial inclusion is expanding, becoming the new hotspot of digital fraud (ORF, 2026).

Due to cyber fraud, financial losses in 2024 stood at ₹22,845.73 crore - a near-threelfold rise from ₹7,465.18 crore in 2023⁴. In 2024, 60% of the fraud victims were individuals making their first digital payment (India Data Map, 2025). Low-income, newly included digital payment users are at higher risk of exploitation as they are unfamiliar with digital hygiene, have limited recourse options and when defrauded, may become reluctant to continue using formal digital financial services - negating years of financial inclusion efforts. The cyber fraud-induced trust deficit is the biggest risk to the sustainability of India's financial inclusion journey, especially digital financial inclusion.

This study examines the intersection of cyber security and digital financial inclusion, analyses the emerging financial cyber fraud landscape, study the evolving regulatory architecture under National Strategy for Financial Inclusion (NSFI) 2025–30 and the recent developments by regulator and proposes a Cyber-Inclusive Finance Framework to strengthen trust and resilience within India's digital financial ecosystem. Further, the paper presents the review of literature and identifies the research gap; methodology; Discussion; explore the fraud landscape, regulatory architecture, trust paradox and proposed framework and lastly, conclusion, implications and future scope.

Literature Review

International literature recognises digital finance

as a key enabler of financial inclusion by reducing transaction costs, expanding access to formal financial services and improving financial participation among underserved populations. Ozili (2018) argues that while digital finance has significantly strengthened financial inclusion, its long-term sustainability depends on maintaining users' confidence, trust and security within the digital financial ecosystem. These findings provide an important conceptual foundation for examining cyber security as an essential component of sustainable digital financial inclusion.

Recent evidence from the World Bank further highlights that while digital financial services have significantly expanded financial inclusion globally, their long-term benefits depend upon consumers' ability to use digital financial products safely, supported by appropriate consumer protection, digital financial literacy and trust-building mechanisms (Klapper, 2024).

With India's digital payment system growing at a rapid pace, the digital financial inclusion-cyber security nexus has gained increasing policy and academic focus. The RBI's Report on Currency and Finance 2023-24 noted that the growth of Digital Public Infrastructure (DPI) opens up new avenues for fraud vulnerabilities that need coordinated regulatory action (RBI, 2024). NABARD's All India Rural Financial Inclusion Survey (NAFIS) 2021-22, which surveyed one lakh rural households in 710 districts across 28 States and Union Territories of Jammu & Kashmir and Ladakh. Revealed that financial literacy of the rural households had increased from 33.9% to 51.3% between 2016-17 and 2021-22, but there was no equivalent measure of cyber-literacy (NABARD, 2024). The trend towards digital financial fraud and its disproportionate effect on newly banked population is consistently captured in the country. Bharti and

⁴Ministry of Home Affairs, (2025a). Lok Sabha Unstarred Question No. 432, 2 December 2025. <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/432.pdf>

Sharma (2026) specifically analyzed the vulnerability of UPI fraud in the state of Himachal Pradesh and concluded that lower educated and rural users are more vulnerable to UPI fraud. The Central Payment Fraud Information Registry (CPFIR) of the RBI, which was launched in March 2020, is the main institutional repository for monitoring the trend of payment fraud (Ministry of Finance, 2024). Although the scale of the problem is known from the existing institutional data, there is no integrated framework in the existing literature that connects the cyber security architecture with the outcomes of digital financial inclusion policy – which this study proposes with the Cyber-Inclusive Finance framework.

The OECD (2015) similarly emphasises that digital security should be viewed not merely as an technological issue, but as an economic and social enabler that supports confidence in the digital economy. This perspective reinforces the argument that cyber security should be integrated into digital financial inclusion policies rather than treated solely as a technical compliance requirement. Building upon these insights, the present study proposes a Cyber-Inclusive Finance framework that positions cyber security as the trust infrastructure underpinning sustainable digital financial inclusion.

Objectives

This study examines the intersection of cyber security and digital financial inclusion, analyses the emerging financial cyber fraud landscape, study the evolving regulatory architecture under NSFI 2025–30 and the recent developments by regulator and proposes a Cyber-Inclusive Finance framework to strengthen trust and resilience within India's digital financial ecosystem.

Methodology

This study adopts a descriptive method using secondary data obtained from various Government and regulatory data sources. The data collected from various reports released by Government, RBI and other research institutions. The previous literature were referred to prepare the conceptual framework. This study is proposing Cyber-Inclusive Finance framework, providing novel contribution.

Discussion

The Cyber Fraud Landscape: Scale, Patterns and Vulnerable Population

Trends in Financial Cyber Frauds

Cyber fraud in India has gone beyond being a law enforcement issue to a systemic financial stability concern. As per Ministry of Home Affairs (MHA) response to Parliament, financial losses due to cyber fraud rose sharply from ₹2,290.24 crore in 2022 to ₹7,465.18 crore in 2023 and ₹22,845.73 crore in 2024. In 2024 alone, NCRP received 22.68 lakh complaints of cybercrime. UPI fraud incidents rose from 4.07 lakh (₹242 crore) in 2021-22 to 13.42 lakh (₹1,087 crore) in 2023-24 and in FY 2024-25 stood at ₹981 crore involving 12.64 lakh incidents. As total digital payment transactions reached to 22,716.07 million (by volume) in June 2026, and 86% of households are now connected to internet, the attack surface has continued to expand. Financial cyber fraud complaints increased from 2,62,846 in 2021 to 24,02,579 in 2025, while reported financial losses increased from ₹551 crore to ₹22,495 crore during the same period. The steep rise in complaints and losses reflects the expanding cyber threat accompanying India's rapid digitalisation and underscores the need to integrate cyber security into digital financial inclusion policies.

Table 1: Financial Cyber Fraud Complaints and Reported Losses in India

Year	Financial Cyber Fraud Complaints	Reported Losses (₹ crore)
2021	2,62,846	551
2022	6,94,446	2,290
2023	13,10,357	7,465
2024	19,18,835	22,848
2025	24,02,579	22,495

Source: Ministry of Home Affairs Parliamentary Replies (Lok Sabha Unstarred Question No. 432, 2025; Rajya Sabha Unstarred Question No. 1349, 2026) and Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) data.

As digital finance has grown, so has the modus operandi of fraud. The most common fraud types include phishing and vishing attacks, impersonating bank officials or Government agencies to extract OTPs; UPI manipulation where fraudsters guide victims into entering their UPI PIN as if receiving a payment; investment scams through messaging platforms; ‘digital arrest’ scams where fraudsters impersonate enforcement agencies; and fake Know Your Customer (KYC) calls. A large proportion of cyber frauds are carried out by organised groups of criminals from outside the country (MHA, 2026a). This threat is transnational also and requires international and local law enforcement action.

Who is Most Vulnerable?

In a study of the vulnerability of UPI in Shimla district, Himachal Pradesh, Bharti and Sharma (2026) found that lower educated, lower income and rural users were the most vulnerable, and the most prevalent frauds are phishing, social engineering and fake QR code scams. Overconfident and underconfident digital users are exposed to higher risk: the former believing that they are less likely to be exposed to threats and the latter having less knowledge of how to recognize fraud patterns.

This picture is confirmed by national-level data. 60% of individuals become cyber frauds victims, while making first digital payment (India Data Map, 2025). In 2023, only 20% of Indians had received training in cyber safety (Indian Cyber Crime Coordination Centre [I4C] and India Data Map, 2025). Low-cost smartphones and cheap data plans have increased digital access in rural and semi-urban areas, without digital literacy to support it. Tier 2 and Tier 3 cities have seen an increase in cybercrime activity because of the lack of awareness and strong cyber defence systems (ORF, 2026). The instances of organised vishing fraud is an example of how digital inclusion can be turned into digital exploitation at scale without digital safety.

The repercussions are not just financial. Once defrauded, many individuals, especially, newly included digital payment users may discontinue using digital financial services. Above this, under-reporting of incidents is another challenge. Data from the Ministry of Home Affairs mentioned that 28 lakh cases were reported in 2025 and only 55,484 First Information Reports (FIRs) were filed. This enforcement deficit also undermines trust and formal financial inclusion of the most vulnerable groups. As complaints reported on the portal and registered FIRs represent different stages of the criminal justice process, the effectiveness of cybercrime response ultimately depends upon timely investigation and prosecution by the concerned Law Enforcement Agencies. Any gap between complaint reporting and enforcement outcomes may contribute to an enforcement deficit, which can adversely affect public trust in formal digital financial institutions.

The Regulatory Architecture: Strengthening the Shield

RBI Authentication Directions, 2025

In view of the growing fraud risks, on 25 September 2025, the RBI issued the Authentication Mechanisms

for Digital Payment Transactions Directions, 2025, applicable to all payment system providers - banks and non-banks - from 1 April 2026. The Directions require at least two-factor authentication for all domestic digital transactions, with the provisions that at least one factor must be dynamic - credentials such as OTPs, biometric data or hardware tokens must be unique to each transaction. This directly addresses the most frequent fraud vector: SMS-based OTP interception through SIM-swap and social engineering.

The Directions also introduce a risk-based authentication model: low-risk, low-value transactions from familiar devices may be verified less rigorously, while high-value, unusual or geographically anomalous transactions require enhanced authentication. This calibrated approach balances security with the user-experience imperative critical for newly included digital payment users - excessive authentication friction risks driving newly included population back to cash-based transactions.

While the Directions represent a significant regulatory step, implementation challenges exist in the digital financial inclusion context. Dynamic authentication requirements may present practical barriers in rural areas with limited internet connectivity. Supplementary guidelines addressing these gaps - particularly for BC-mediated and offline transactions - will be essential to ensure that rural inclusion contexts are not inadvertently disadvantaged. The RBI has also made provisions on consumer compensation mechanism under which eligible fraud victims would receive up to ₹25,000 or 85% of the fraud amount, whichever is lower, subject to conditions: (i) the transaction must be a domestic digital payment; (ii) the victim must not have been negligent in sharing credentials or authentication details; and (iii) the complaint must be lodged within the prescribed timeframe through official channels. This shared

liability mechanism is designed to simultaneously provide relief to vulnerable users and enable banks and payment operators to invest in stronger fraud detection.

Digital Payments Intelligence Platform and I4C

The NSFI 2025-30 emphasises the need for banks to implement the Digital Payments Intelligence Platform (DPIP) for detecting and preventing payment frauds, the effective utilisation of the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) to report and handle complaints of cyber fraud and use of pre-intimated official phone numbers by banks to counter vishing attacks. The I4C's Suspect Registry has declined transactions worth ₹8,031.56 crore. CFCFRMS has separately saved more than ₹8,189 crore across 23.61 lakh complaints till 31 December 2025, demonstrating that coordinated real-time intervention can materially limit losses.

RBI Cyber security Framework for Banks

The RBI's Cyber security framework for Scheduled Commercial Banks mandates board-approved cyber security policies, 24/7 Security Operations Centres (SOCs) for threat monitoring and incident response, dataleak prevention, regular vulnerability assessments and formal incident reporting. The Master Direction on Information Technology framework imposes tiered obligations for Non-Banking Financial Companies (NBFCs) based on asset size.

Rising internet penetration, smartphone adoption and the rapid expansion of digital services, has increased the attack surface for cyber threats. This digital adoption making cyber security investment a mandatory, rather than an option.

The Trust Paradox: When Inclusion breeds Exclusion

The central argument of this study is that cyber security is not a technical add-on to digital financial

inclusion, but it is a foundation to build trusted infrastructure. The trust paradox can be simply stated: digital financial inclusion expands access but also expands vulnerability. When the vulnerability is not managed, it erodes the trust that access is meant to build.

The fraud not only resulted into direct financial loss but in many cases deterred victims from ever using digital banking again. Each such incident is a reversal of inclusion - a newly banked person exiting the formal financial system because their experience of it was one of victimisation.

The NSFI 2025-30 explicitly acknowledges this, noting that the number of cybercrime reports rose by 24.4% between 2021-22 (NCRB, 2023), reflecting rising digital frauds. The complex procedures and negative experiences deter first-time users from engaging with digital finance. The strategy's fifth Panch-Jyoti goal - Customer Protection and Resilience - explicitly targets this through enhanced grievance redressal systems, DPIP deployment and regular awareness campaigns. But policy architecture alone cannot build trust. Trust is built through lived experience - millions of safe digital transactions, quick resolution when fraud occurs and knowledge of how to protect oneself.

That is why digital literacy and cyber hygiene - not authentication frameworks alone - are the ultimate measure of inclusion sustainability. NAFIS 2021-22 shows financial literacy improved from 33.9% to 51.3% between 2016-17 and 2021-22 (NABARD, 2024), yet nearly half of rural households still lack adequate financial literacy - and no equivalent cyber literacy metric is tracked. Thus, there is a need to fill this gap between digital adoption and digital financial literacy.

Towards a Cyber-Inclusive Finance Framework: Recommendations

To resolve this trust paradox, an integrated approach is needed that treats cyber security and digital

financial inclusion not as separate agendas but as a single programme. In this regard, the authors has proposed a Cyber-Inclusive Finance framework. The framework brings together the regulatory framework, the identified gap between inclusion and cyber safety and the field-level realities in six mutually reinforcing action components. The six components are: (i) Cyber Literacy Integration; (ii) Gender-Differentiated Cyber Safety; (iii) Accessible Fraud Reporting; (iv) Contextually Calibrated Authentication; (v) Public-Private Coordination; and (vi) Implementation. They are described below.

Embed Cyber Literacy in all Financial Literacy Programmes

The institutional structure for this integration is the NSFI 2025-30's National Centre for Financial Inclusion and the five-Cs of the National Financial Education Strategy (Content, Capacity, Community, Communication, Collaboration). All financial literacy modules should include a mandatory cyber hygiene component: identification of OTP scams, verification of caller identity, safe use of UPI and reporting of cyber fraud. The RBI's awareness campaign with Common Service Centre (CSC) e-Governance services, piloted in 2026, represents exactly this integration model and should be scaled nationally (RBI, 2026a).

Gender-Differentiated Cyber Safety Interventions

Women constitute 55.70% of PMJDY account holders, as on January 15, 2026; however, they remain disproportionately underrepresented among active digital financial service users and low access of knowledge about fraud detection, making them more vulnerable to cyber fraud. Cyber safety campaigns co-designed with and delivered through Self-Help Group (SHG) networks - already trusted institutions for financial literacy - can serve as an effective channel for reaching rural women with actionable cyber hygiene knowledge. BC women agents with direct community connections to newly banked customers should be trained as 'Cyber Sakhi' first responders,

providing immediate guidance when a fraud attempt is reported.

Simplify Fraud Reporting for low-literacy users

The complexity of progressing from complaint reporting to formal investigation may discourage newly included digital payment users from pursuing grievance redressal. The CFCFRMS (1930) should be made available in all 22 scheduled languages with voice-based reporting options for users with low literacy. Banks should designate a dedicated BC contact for each service area as the first point of contact for customers unable to navigate app-based fraud reporting.

Risk-Based, Contextually Calibrated Authentication

While the RBI's Authentication Directions, 2025 is a welcome step, implementation must be tailored to the rural, low-digital-literacy context. Biometric Aadhaar Enabled Payment System (AePS) - already deployed at BC points across rural India - provides fraud-resistant, low-friction authentication without requiring smartphone literacy. AePS-based biometric authentication may be considered for high-value transactions at Tier 4-6 centres, reducing dependence on SMS OTPs which are the dominant social engineering target.

Public-Private Coordination: The Cyber-Inclusion Compact

To address cyber fraud at the scale required by India's financial inclusion agenda, a Cyber-Inclusion Compact - a formal coordination mechanism between RBI, Government, NPCI, banks, telecom operators and fintech platforms - is needed. SIM-swap fraud is a telecom-layer problem requiring real-time data sharing between banks and operators. The real-time data integration could become powerful fraud prevention instrument. The regular publications of fraud typology reports disaggregated by geography and user demographics, can enable targeted

interventions in high-fraud districts.

Implementation of Directions

The consumer compensation mechanism—up to ₹25,000 or 85% of the fraud amount, subject to eligibility conditions—should be implemented and operationalised in a timely manner to strengthen consumer confidence and support sustained adoption of digital financial services. For low-income fraud victims, even partial recovery can be the difference between re-engagement with formal finance and withdrawal from formal digital financial services. The framework should be linked to mandatory bank-side fraud reporting timelines, establishing systemic accountability alongside consumer relief.

Conclusion

India's financial inclusion journey has achieved significant milestones, though full digital financial inclusion remains a work in progress. The next step, however, is from access to empowerment and the one condition that must be met is trust. In a digital financial system, trust is created or lost in a single transaction. The sharp rise in financial cyber fraud complaints and reported losses over recent years highlights that the sustainability of digital financial inclusion depends not only on expanding access but also on strengthening cyber security, consumer protection and public trust. Without adequate cyber resilience, the long-term gains of India's digital financial inclusion initiatives may be significantly undermined.

The regulators are cognizant of this challenge, as evidenced by the fifth Panch-Jyoti objective under NSFI 2025-30 and the Authentication Directions, 2025 issued by the RBI. The Digital Payments Intelligence Platform, the I4C's fraud intervention record of blocking ₹8,031 crore in fraudulent transactions and the consumer compensation mechanism are meaningful institutional responses. However, this institutional architecture has to be complemented

by grassroots action: Cyber literacy co-delivered with financial literacy; Cyber Sakhis in the SHG networks; biometric AePS at all BC touch points; and a consumer compensation mechanism that allows for survivability from fraud for the poor.

At the heart of Digital Financial Inclusion, lies the promise that formal digital financial services are not only accessible but also secure, reliable and trustworthy. Building and sustaining that trust will define the success of India's next phase of digital financial inclusion. Ultimately, the success of Digital Financial Inclusion will be reflected in whether every digitally included user — including those in rural and underserved communities — can transact with confidence, knowing that the financial system is secure, responsive and capable of providing effective protection and redress in the event of cyber fraud.

Implications and Future Scope

The findings of this study have practical implications for multiple stakeholders involved in India's digital financial inclusion ecosystem. For regulators, the proposed Cyber-Inclusive Finance framework highlights the importance of integrating cyber literacy, consumer protection and trust-building measures within the implementation of the National Strategy for Financial Inclusion (NSFI) 2025–30. For Public Sector Banks (PSBs) and other financial institutions, the study provides strategic directions for strengthening fraud prevention mechanisms, customer awareness programmes and accessible grievance redressal systems to enhance consumer confidence in digital financial services. For FinTech companies and payment system operators, the framework emphasises the need for user-centric design, context-sensitive authentication and simplified fraud reporting mechanisms that improve both security and user experience. For policymakers, the study offers a policy perspective for integrating cyber security into digital financial inclusion initiatives through

coordinated institutional mechanisms involving financial regulators, law enforcement agencies and technology service providers. Finally, for researchers, the proposed Cyber-Inclusive Finance framework provides a conceptual foundation for future empirical research examining the relationship between cyber security, consumer trust and sustainable digital financial inclusion.

Future studies should focus on empirically validating the proposed Cyber-Inclusive Finance framework across different socio-economic and geographical contexts. Longitudinal studies may be undertaken to examine whether improvements in cyber literacy led to sustained adoption of digital financial services and reduced fraud victimisation over time. Comparative studies across States, aspirational districts and urban–rural regions could identify contextual factors influencing cyber resilience among digitally-included population. Future studies can investigate the effectiveness of artificial intelligence-based fraud detection systems, behavioural interventions aimed at reducing phishing susceptibility and gender-specific cyber awareness programmes in improving digital financial safety. Comparative studies evaluating cyber security practices adopted by banks, fintech platforms and payment service providers would further strengthen policy understanding. Finally, cross-country comparative studies among emerging digital economies could provide valuable insights into global best practices for integrating cyber security with digital financial inclusion and enhancing consumer trust.

References

- Bharti, S. & Sharma, R. (2026). Socio-demographic and behavioral determinants of UPI fraud vulnerability: A descriptive study from Shimla District, Himachal Pradesh. *Journal of Forensic Sciences and Research*, 10. <https://www.forensicscijournal.com/>
- India Data Map. (2025, October 11). *Online fraud in India: 2025 projections and analysis*.

- Klapper, L. (2024). Expanding Financial Inclusion through Digital Financial Services: A Literature Review. World Bank Policy Research Working Paper No. 11008. Washington, DC: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099415112192435594?utm_source
- Lexology. (2025, October 6). RBI (Authentication Mechanisms for Digital Payments Transactions) Directions 2025: Balancing privacy and security in digital payment. Lexology. <https://www.lexology.com>
- Ministry of Finance, Government of India. (2024). Central Payment Fraud Information Registry (CPFIR): Overview. Department of Financial Services. <https://rbi.org.in>
- Ministry of Finance, Government of India. (2025a). UPI fraud trend data FY 2024-25. Lok Sabha statement by MoS Finance, 15 December 2025. https://sansad.in/getFile/loksabhaquestions/annex/186/AU2481_5blzKk.pdf
- MHA (Ministry of Home Affairs), Government of India. (2025a). Lok Sabha Unstarred Question No. 432, 2 December 2025: Cases of Cybercrime. <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/432.pdf>
- MHA (Ministry of Home Affairs), Government of India. (2026a). Rajya Sabha Unstarred Question No. 1349, 11 February 2026: Sharp rise in cyber and financial frauds. <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/RS11022026/1349.pdf>
- National Crime Records Bureau. (2023). Crime in India 2022. Ministry of Home Affairs, Government of India. <https://ncrb.gov.in>
- Ministry of Finance, Government of India. (2025). Lok Sabha Unstarred Question No. 2481: UPI Domestic Payment Frauds During the Last Five Financial Years (Answered on 16 December 2025). Parliament of India. https://sansad.in/getFile/loksabhaquestions/annex/186/AU2481_5blzKk.pdf
- NABARD (National Bank for Agriculture and Rural Development). (2024). All India Rural Financial Inclusion Survey (NAFIS) 2021-22. Department of Economic Analysis & Research, NABARD, Mumbai. <https://www.nabard.org>
- Observer Research Foundation (ORF). (2026, January 20). Digital deception in rural India and the AI counter-offensive. ORF Expert Speak. <https://www.orfonline.org>
- Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, 18(4), 329–340. https://www.sciencedirect.com/science/article/pii/S2214845017301503?utm_source
- OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. https://www.oecd.org/en/publications/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en.html?utm_source
- PIB (Press Information Bureau). (2025a). Pradhan Mantri Jan Dhan Yojana: Progress Report, August 2025. Ministry of Finance, Government of India. <https://www.pib.gov.in>
- PIB (Press Information Bureau). (2025b). Cybercrime statistics and I4C awareness initiatives. Ministry of Home Affairs, Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2153524>
- PIB (Press Information Bureau). (2025c). Curbing Cyber Frauds in Digital India - Special Feature, October 2025. Ministry of Information & Broadcasting, Government of India. <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/oct/doc2025108660701.pdf>
- PIB (Press Information Bureau). (2025d). Digital Payment Transactions Surge with Over 18,000 Crore Transactions in 2024-25. Ministry of Finance, Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2110405>
- Reserve Bank of India. (2024). Report on Currency and Finance 2023-24: India's Digital Revolution. RBI, Mumbai. <https://www.rbi.org.in>
- Reserve Bank of India. (2025a). Financial Inclusion Index for the year ending March 2025. RBI, July 2025. <https://www.rbi.org.in>
- Reserve Bank of India. (2025b). National Strategy

for Financial Inclusion (NSFI): 2025-2030. RBI, 1 December 2025. <https://www.rbi.org.in>

Reserve Bank of India. (2025c). Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025. RBI, 25 September

2025. <https://www.rbi.org.in>

Reserve Bank of India. (2026a). Digital payments awareness programme with CSC e-Governance Services. RBI. <https://www.rbi.org.in>



BANK QUEST THEMES

The themes for upcoming Issues of “Bank Quest” are identified as:

1. July-September 2026: Enhancing Customer Service through Capacity Building in the Banking Sector

Sub-themes: Employees as drivers of Customer Service Excellence; Customer service; Customer engagement; Customer acquisition and retention in digital era; Customer protection; Complaint management; Grievance redressal; Employee engagement; Training, skill development and technology adoption in employees; Ethics and compliance

2. October-December 2026: Credit Inclusion: Bridging the credit gap

Sub-themes: Role of data and emerging technologies in enabling credit access; Fintech & NBFCs ecosystem in credit delivery; Digital lending; Microfinance; MSME financing; Embedded finance; Financing of emerging sectors

3. January-March 2027: Rural banking, Co-operative Banking and NBFCs in Indian Financial system

Sub-themes: Role and importance of regional rural banks, co-operative banks and NBFCs; Challenges of regional rural banks, co-operative banks and NBFCs; Rural banking; Technology adoption; Business Correspondents & Financial inclusion

4. April-June 2027: Risk management in banks

Sub-themes: Different types of risks in banking sector and their management; Cyber risks; Climate related risks; Operational risks; Unsecured loans; Early-warning signals; Compliance