



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE RISE OF INVISIBLE BANKING: A LEGAL ANALYSIS

Utkal Sinha

“Invisible Banking, Visible Data: Should Invisible Banking Face Stronger Privacy Rules?”

BACKGROUND/ FACTS

In today’s digital India, we often use online payment apps for buying insurance to claim a credit offer - all without ever opening a traditional banking app. This scenario is an example of Invisible banking, where credit, payments, or insurance is delivered through non-financial apps so smoothly that the customer doesn't notice the regulated bank or NBFC handling the transaction.

This concept is called embedded finance, built through Banking-as-a-service (BaaS) arrangements where a licensed lender exposes its balance sheet through APIs while a fintech or platform keeps all the customer attention. But the real question that arises is: Can India’s data protection laws keep pace with this tangled web of companies moving our data around?

The convenience comes with a trade-off that customers aren’t aware of. A single transaction may involve a platform, a fintech company, a bank or NBFC, payment service providers, or other tech or service partners. Each participant may handle data differently, including collecting, processing, storing, or transmitting information. This data becomes significant when it goes beyond a name or mobile number to include spending patterns, creditworthiness, transactions, and preferences. The traditional boundary between a “banking service” and a digital service is harder to identify as financial services become increasingly embedded into everyday digital experiences.¹

¹ Sauradeep Bag, Embedded Finance in India: Opportunities and Challenges, ORF Issue Brief No. 851, Observer Research Foundation (Dec. 19, 2025) [<https://www.orfonline.org/research/embedded-finance-in-india-opportunities-and-challenges>]

India has regulations governing different parts of this ecosystem, but the question is whether these rules provide to guarantee the same level of transparency, control, and accountability when financial services operate in the background. So, invisible banking isn't just about technological convenience- it's about privacy, consent, consumer protection, and regulatory responsibility.

LEGAL FRAMEWORK

India doesn't have a single clear law that specifically regulates "invisible banking" or embedded finance. However, that doesn't mean the sector operates in a legal vacuum. Different parts of digital finance services are governed through data-protection law, RBI regulations, and sector-specific financial frameworks.

The Digital Personal Data Protection Act, 2023² provides the broader legal framework for processing digital personal data. It's relevant for fintechs and digital platforms that collect or process customers' data. This Act sets obligations for processing personal data to respect individuals' rights over their data. However, it is a general data-protection law and doesn't specifically address the complex relationships involved in embedded finance.

The RBI (Digital Lending) Directions,³ 2025 provide more detailed and specific safeguards for digital lending. These guidelines regulate the relationship between regulated entities, such as banks and NBFCs, and third-party entities such as Lending Service Providers. The framework requires data collection to be strictly need-based and supported by prior and explicit consent. The rules also restrict regulated entities from accessing certain mobile-phone resources and oversee their service providers.

Another layer of protection comes from the Account Aggregator framework.⁴ This system enables sharing of financial information between the parties based on the customer's instruction and explicit consent. This attempts to give customers real control over the movement of their financial information.

Recently, the Delhi High Court considered a public interest petition concerning the protection of borrowers' data through digital lending applications. In the case of Himakshi Bhargav v.

² Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 2–8

³ Reserve Bank of India, Reserve Bank of India (Digital Lending) Directions, 2025 (May 8, 2025)

⁴ Department of Financial Services, Ministry of Finance, Government of India, Account Aggregator Framework [<https://financialservices.gov.in/account-aggregator-framework>]

Union of India & Ors. (2026)⁵, the court recognised the RBI's Digital Lending Directions, 2025, as providing measures to address the protection of borrowers' data and required the RBI to show the steps taken to enforce these safeguards.

Therefore, India already has several laws and regulatory mechanisms relevant to invisible banking. But the difficulty lies in their scattered nature. A single digital financial transaction may involve data protection, banking, lending, payments, and multiple intermediaries at the same time. The real challenge is that when responsibility is divided among entities, accountability lies with whom for protecting consumers' data and ensuring meaningful consent.

BODY

India's digital finance ecosystem has grown at an extraordinary scale. In FY 2025-26, UPI handled over 24,000 crore transactions, with a total value exceeding ₹314 lakh crore. By June 2026, more than 55 crore users were onboarded on UPI.⁶ These figures demonstrate how digital payments and financial transactions have integrated into everyday life.

India has developed several legal safeguards for digital finance and data protection, but invisible banking is growing so rapidly that the existing frameworks can't bind legal obligations. The issue is not regarding the regulated financial service, but the real concern is whether consumers remain informed, protected, and accountable for their data when these services run silently in the background.

ARGUMENTS

Invisible banking and embedded finance provide convenience - faster payments and quick access to credit but this seamless customer experience should not result in invisible accountability. Embedded finance undoubtedly offers important benefits that are integrated into the platforms that consumers already use. However, convenience cannot justify uncertainty about who collects, processes, or protects a customer's financial information.

The Government and RBI have made efforts against fake and illegal lending applications, and RBI provides a public directory of Digital Lending Apps associated with its regulated entities to help customers verify whether the app relates to a regulated lender.⁷ By July 2026, the

⁵ Himakshi Bhargav v. Union of India & Ors., W.P.(C) No. 118/2026, ¶¶ 3–6 (Delhi High Ct. Jan. 7, 2026)

⁶ Press Information Bureau, Ministry of Finance, nearly 55.49 Crore Users Onboarded on UPI as in June 2026 (July 20, 2026) [<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2286608®=48&lang=2>]

⁷ Reserve Bank of India (Digital Lending) Directions, 2025, ¶ 17 (May 8, 2025)

Government blocked 87 illegal lending apps under the Information Technology Act, following proper procedures.⁸

EVIDENCE

The risk associated with financial data isn't just hypothetical theory. In July 2026, Bank of Baroda⁹ confirmed a cybersecurity incident where an employee's email account was compromised, after which customer information and internal documents ended up on the dark web. Reports indicated that the compromised data included customer identity documents, loan-related information and internal records.

This incident is significant because it shows how sensitive financial data is. A digital finance ecosystem doesn't just process payment information, but it also holds identity documents, credit, loan details and payment patterns of the customer, and these information's are capable of exposing an individual's financial life.¹⁰

Similarly, in 2024, a security incident involving Signzy-a company working with banks and fintechs on digital identity verification, faced a security breach, which demonstrates how risks affecting a technology service provider can potentially affect a wider financial ecosystem.¹¹

CONCLUSION

Invisible Banking is likely to become a larger part of India's digital economy, but its invisibility should never extend to consumer rights, data protection or accountability. India's existing laws provide important safeguards, yet the rise of fintechs, banks, NBFCs, and tech companies shows the need for greater regulatory coordination and transparency.

The aim isn't to slow financial institutions, but to ensure that convenience doesn't come at the cost of privacy. Customers deserve to know who handles their data, why it is being used, and who is responsible when something goes wrong. Ultimately, the success of invisible banking

⁸ Press Release, Ministry of Finance, Government of India, Government and RBI Strengthen Digital Lending Ecosystem Through New Regulatory Framework, Digital Lending App Directory and Enhanced Customer Safeguards (July 21, 2026) [<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2287195&lang=2®=48>]

⁹ Reuters, Customer Data from India's Bank of Baroda Leaked Online, Source and Researcher Say (July 27, 2026) [<https://www.reuters.com/business/media-telecom/customer-data-indias-bank-baroda-leaked-online-source-researcher-say-2026-07-27/>]

¹⁰ Reserve Bank of India, Chapter V: Digitalisation—Tackling Emerging Risks and Challenges (July 29, 2024) [https://systemhealth.rbi.org.in/Scripts/PublicationsView.aspx_id%3D22461.html]

¹¹ Jagmeet Singh & Manish Singh, Indian Online ID Verification Firm Signzy Confirms Security Incident, TechCrunch (Dec. 2, 2024) [<https://techcrunch.com/2024/12/02/indian-online-id-verification-firm-signzy-confirms-security-incident/>]

should not be measured only by how effortlessly a financial service works, but also by how securely and fairly it operates behind the scenes.