

Digital Banking in India: Rights, Remedies, and Roadmap to Redressal of Complaints

INTRODUCTION

Digital banking has become part of daily life in India. With 18 billion transactions every month¹, millions of transactions are happening through UPI mechanism and digital platforms. But glitches happen, payments get stuck, fraudsters steal money, hidden charges appear, or recovery agents harass borrowers. In such situations, usually the customer seeks and run for guidance from friends, who may or may not be ideal person to guide. This write up try to demystify the entire ecosystem; the legal backbone that makes every authenticated digital transaction binding, the RBI rules that protect you in case of failure or fraud, the 2025 Digital Lending Directions that curb predatory fintech practices, the escalation ladder from bank to Internal Ombudsman to RBI Integrated Ombudsman and finally the High Court, and most importantly, practical steps one must take immediately to safeguard your money. Armed with the right references and timelines, banking customers can turn RBI's guidelines from mere circulars into enforceable rights.

Digital banking having permeated every corner of daily life, general public relying heavily on convenient, instant transaction modes that have replaced cash and cheques for most routine payments. The most widely used ones include Unified Payments Interface (**UPI**), Immediate Payment Service (**IMPS**), National Electronic Funds Transfer (**NEFT**), Real-Time Gross Settlement (**RTGS**), debit and credit cards (both at points of sale and online), mobile wallets, and internet banking transfers. UPI alone dominates, powering everything from street-vendor QR code scans to utility bill payments and peer-to-peer transfers, often crossing 500 million transactions a day. Card payments remain popular for larger purchases, while NEFT and RTGS handle bigger inter-bank movements, and wallets like Paytm or PhonePe serve users who prefer stored value.

LEGAL FRAMEWORK GOVERNING PAYMENT/ TRANSFERS

These transactions do not happen in a vacuum; they rest on a solid legal foundation that gives them the same enforceability as traditional banking instruments. At the core is the **Payment and Settlement Systems Act, 2007 (PSS Act)**, which empowers the Reserve Bank of India to regulate and supervise all payment systems, authorise payment system operators (like NPCI for UPI), and ensure safety and efficiency. Section 18 of the PSS Act, read with RBI's power under Section 10(2) of the Banking Regulation Act, 1949, allows the central bank to issue directions for electronic fund transfers, making every authorised digital transaction legally binding.

The contractual relationship between the customer and the bank is governed by the **Indian Contract Act, 1872**, a valid account agreement, terms of service accepted during onboarding, and electronic mandates create enforceable obligations. For electronic instructions, the **Information Technology Act, 2000** (as amended) provides the crucial recognition, Section 10A makes digital contracts valid, while Sections 65A and 65B of the **Indian Evidence Act, 1872** ensure that electronic records (transaction logs, OTPs, timestamps) are admissible as evidence without the original paper trail. The RBI's Master Directions on Digital Payment Security Controls (2021) and the recent Reserve Bank of India (Digital Lending) Directions, 2025 further mandate secure authentication (like two-factor for cards and UPI PIN/biometrics), protecting both parties.

¹<https://www.pib.gov.in/PressNoteDetails.aspx?NotelId=154912&ModuleId=3#:~:text=It%20brings%20all%20your%20bank,powerful%20tool%20for%20financial%20inclusion.>

UPI, IMPS, and wallets operate under the RBI's Procedural Guidelines on UPI (2016, updated) and Master Direction on Prepaid Payment Instruments (2021), issued under Section 18 of the PSS Act. NEFT and RTGS fall under the RBI's NEFT/RTGS Procedural Guidelines (updated periodically). Card transactions are regulated by the RBI Master Direction on Credit/Debit Cards (2023) and the Card Network Rules (Visa, Mastercard, RuPay), again authorised under the PSS Act. The relationship is also shaped by the **Banking Regulation Act, 1949** (Sections 6 and 35A for RBI's directive powers) and the Reserve Bank of India Act, 1934 (Section 58 for rulemaking).

In essence, every tap, scan, or click is backed by a chain of statutes that treat electronic instructions as irrevocable once authenticated, protect customer data under the IT Act and SPDI Rules, and give RBI sweeping oversight to penalise failures. This framework has turned digital banking from a convenience into a trusted, legally robust alternative to physical cash, used confidently by hundreds of millions every day.

FAILED TRANSACTIONS

The core rule for failed transactions remains RBI's circular DPSS.CO.PD No.629/02.01.014/2019-20 dated September 20, 2019 – Harmonisation of Turn Around Time (**TAT**) and Customer Compensation for Failed Transactions. It covers every authorised payment system: UPI, IMPS, NEFT, RTGS, cards, wallets, and ATMs. If your account is debited but the beneficiary does not receive the money, the responsible entity must auto-reverse by T+1 (next working day). For card-present transactions at PoS terminals, reversal within T+5. For ATM cash-out failures, the issuer bank must re-credit within 7 working days. Miss the deadline and the bank owes ₹100 per day until fixed – no questions asked, no separate complaint needed.

FRAUD AND UNAUTHORISED TRANSACTIONS

These are governed by RBI circular DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (extended to co-operative banks vide circular dated December 14, 2017). Report within 3 working days and your liability is zero. Report between 4–7 days and it is limited (₹5,000 to ₹25,000 depending on account type). The bank must provide shadow credit within 10 working days and carries the burden of proving customer negligence. Courts have strictly enforced this. In **Hare Ram Singh v. Reserve Bank of India & Ors**². (*Delhi High Court, W.P.(C) 1150/2023, decided on June 13, 2024*, the High Court found that transactions fell under "zero liability" as no customer negligence proven. Bank failed to reverse fraudulent amounts despite prompt reporting. Court quashed Banking Ombudsman's rejection directed full refund with 9% interest from fraud date.

Similarly, In **Jaiprakash Kulkarni v. Banking Ombudsman & Ors.** (*Bombay High Court, WP No. 1150/2023, decided on 13 June 2024*), the High Court held that the bank was liable to refund the entire amount lost in a phishing fraud despite the customer's prompt reporting, as the transaction attracted "zero liability" under RBI's 2017 circular on customer protection. The Banking Ombudsman's order rejecting the complaint was quashed, and the bank was directed to pay the full amount along with interest, reinforcing that the burden of proving customer negligence squarely lies on the bank (para 12 of the circular). This judgment underscores the strict enforceability of RBI's guidelines, making banks primarily responsible for unauthorised electronic transactions unless they conclusively establish contributory fault or delay by the customer.

LATEST FRAMEWORK FOR DIGITAL LENDING – RESERVE BANK OF INDIA (DIGITAL LENDING) DIRECTIONS, 2025

On May 8, 2025, RBI consolidated and strengthened all previous digital lending guidelines by issuing the Reserve Bank of India (Digital Lending) Directions, 2025 vide notification RBI/2025-26/36 DOR.STR.REC.19/21.07.001/2025-26. These Directions came into force immediately (except para 6 effective November 1, 2025 and para 17 effective June 15, 2025) and repealed three earlier circulars: (i) RBI/2019-20/258 dated June 24, 2020, (ii) RBI/2022-23/111 dated September 2, 2022, and (iii) RBI/2023-24/41 dated June 8, 2023 (listed in Annex III of the Directions).

² 2024 SCC OnLine Del 8039

Key protections under the 2025 Directions:

- **Only Regulated Entities (REs):** commercial banks, co-operative banks, NBFCs (including HFCs), and AIFIs, can lend. Fintech apps remain agents called Lending Service Providers (**LSPs**). The RE remains fully liable for all acts of the LSP (para 5(vii)).
- **Key Fact Statement (KFS):** must be provided as per circular DOR.STR.REC.13/13.03.00/2024-25 dated April 15, 2024, showing APR, all fees, and repayment schedule. Penal charges must follow circular DoR.MCS.REC.28/01.01.001/2023-24 dated August 18, 2023 (para 8).
- **Direct flow of funds:** Loan disbursement and repayment must happen only between borrower's and RE's bank accounts, no third-party wallets or LSP accounts (para 9). Fees payable to LSPs must be paid directly by the RE, not charged to borrowers (para 9(iv)).
- **Cooling-off period:** Borrower can exit the loan by paying principal + proportionate APR without penalty during a Board-approved period of at least one day.
- **Data privacy:** Apps cannot access contacts, photos, or call logs. Only one-time access for camera/location/KYC. All data must be stored in India; processing abroad must be deleted within 24 hours.
- **Multiple lender transparency:** When an LSP works with multiple REs, the app must show unbiased digital view of all matching offers with lender name, amount, tenor, APR, EMI, and link to KFS. No dark patterns or promotion of any single lender.
- **Default Loss Guarantee (DLG):** Capped at 5% of the loan portfolio, only in cash/FD/BG form, invocable within 120 days. No DLG for revolving credit or credit cards. RE must recognise NPA irrespective of DLG.
- **Reporting of Digital Lending Apps (DLAs):** All REs must report their own and LSP DLAs on RBI's CIMS portal by June 15, 2025. RBI will publish a public directory.

GRIEVANCE REDRESSAL MECHANISM

Grievance redressal under the 2025 Directions is tighter. Every RE and customer-facing LSP must appoint a Nodal Grievance Redressal Officer (**NGRO**) with details displayed on websites, apps, and KFS (para 11). Complaint lodging facility must be on the app/website. If the RE rejects the complaint, does not reply within 30 days, or the borrower is dissatisfied, the borrower can escalate directly to RBI's Integrated Ombudsman via CMS portal (cms.rbi.org.in) or physical complaint at Chandigarh.

Every bank must have an internal grievance redress mechanism. If a complaint is rejected, the Internal Ombudsman must review it before the rejection becomes final – Master Direction DOR.MCS.REC.3/21.04.018/2023-24 dated December 29, 2023. If the bank does not resolve within 30 days, customers can approach the RBI Integrated Ombudsman Scheme, 2021 (notified vide RBI/2021-22/83 dated November 12, 2021).

In *K. Srinivasan v. Union of India* (Madras High Court, decided on October 25, 2025), the petitioner alleged third degree methods in recovery in violation of Supreme Court direction in *Manager, ICICI Bank Ltd Vs Prakash Kaur and Ors* (Appeal (Crl) No 267 of 2007), under which the Bank was vicariously liable for the action recovery agents. The Court directed the Ombudsman to decide the complaint on merit.

The escalation path for any grievance relating to digital banking is as follows:

- Complain to the bank/NBFC/PSP/LSP and quote the exact RBI circular/Direction.
- If rejected or no reply in 30 days, demand Internal Ombudsman/NGRO review record.
- If still unresolved, file at RBI Integrated Ombudsman (**CMS portal**).
- If Ombudsman order is unreasonable, approach High Court under Article 226.

Many banks now auto-credit the ₹100 per day penalty. Some give shadow credit same day for fraud reports. RBI monitors monthly grievance dashboards and penalises poor performers.

The combined effect of the 2019 TAT circular, 2017 liability circular, 2025 Digital Lending Directions, Internal Ombudsman Master Direction, and consistent court judgments is, if the customer is vigilant and take steps immediately and follow timelines and quote the right rule, the customers would not lose if they. The Supreme Court had laid down that RBI circulars and Directions as binding law. Therefore, the key is knowing your rights and the exact reference, which could help in addressing customer woes.

STAY VIGILANT: ESSENTIAL SAFETY TIPS FOR SAFE DIGITAL BANKING

In an era of digital transactions while the Regulator and Banks have been running customer education programmes and campaign but the rules will work **only if customer act swiftly and prudently**. Customer must educate themselves about the risk associated with digital transactions and follow the rules and safeguards to protect themselves such as the following:

- **Verify before you transfer – every single time**
 - Always double-check the beneficiary's name, account number, and **IFSC code** (find it on the beneficiary's cheque or official bank website; never trust WhatsApp forwards).
 - For large-value RTGS (₹2 lakh and above), remember the beneficiary bank must credit the amount within **30 minutes**; if it fails, the money must return to you within **1 hour**. If it doesn't, immediately raise a dispute quoting RBI's TAT circular (September 20, 2019).
 - Use "Add Beneficiary" with cooling-off period (many banks enforce 30 minutes to 4 hours for new beneficiaries) – treat this as a free safety net, not an inconvenience.
- **Treat OTPs, PINs, CVV, and card details as cash**
 - Never share OTPs, UPI PINs, credit card numbers, expiry dates, or CVV with anyone, not even bank officials calling you. Legitimate banks **never ask** for these over phone or email.
 - Enable transaction alerts instantly; the moment you receive an SMS/email for an unknown transaction, call your bank's 24x7 helpline and block the card/channel immediately.
 - For credit card disputes, you have **60 days** from statement date to file a Cardholder Dispute Form (**CDF**). File online at your bank's portal or send the signed form, delay beyond 60 days weakens your case.
- **Report fraud immediately – every hour counts**
 - RBI's 2017 circular gives you zero liability if you report unauthorised transactions within 3 working days (third-party breach) or if the fault lies with the bank.
 - Even if delayed up to 7 days, your liability is capped. Beyond that, you risk bearing the full loss.
 - First complain to the bank in writing (email counts); if no reply or unsatisfactory reply within 30 days, escalate to RBI Integrated Ombudsman at <https://cms.rbi.org.in> ; it's free and jurisdiction-neutral.
- **Secure your cards and accounts proactively**
 - Use MyCards/ NetBanking to set lower daily limits for ATM, POS, online, and international transactions.
 - Turn off international/online usage when not needed.
 - Immediately hotlist a lost/stolen card via app, netbanking, or phone, do not wait for morning.
 - Register for e-statements and disable physical statements to prevent mail theft.

- **Special care for senior citizens and family add-on cards**

- Banks must provide dedicated counters, door-step services, and automatic senior-citizen status conversion. Insist on these facilities.
- Add-on cardholders enjoy the same rewards but the primary holder is liable, monitor unbilled transactions regularly.

Remember that RBI guidelines are powerful shields, but they activate only when **you act fast, keep records, and stay alert**.

CONCLUSION

RBI has built one of the most robust customer-protection frameworks for digital banking. From auto-reversal with ₹100-per-day penalty for failed transactions to zero liability within three working days for unauthorised transactions, from direct bank-to-bank flows and cooling-off periods under the 2025 Digital Lending Directions to the one-nation-one-ombudsman portal that resolves complaints free of cost, the machinery is in place and courts are enforcing it strictly.

Yet, as recent judgments in ***Jaiprakash Kulkarni (Bombay HC)*** and ***Hare Ram Singh (Delhi HC)*** demonstrate, **banks bear the burden of proof**, and delays or negligence on their part invite judicial wrath, full refunds, and interest. The Supreme Court has repeatedly held that RBI Directions are binding law. What remains is **Customers' vigilance**. Verify beneficiaries, guard OTPs like cash, report fraud instantly, quote the exact circular, and escalate within 30 days. Do this, and the system works overwhelmingly in your favour.

Digital banking is not just convenient, it is now among the safest ways to move money in India, provided you know your rights and act without delay. Stay alert, stay informed, and transact with confidence.

We trust you will find this an interesting read. For any queries or comments on this update, please feel free to contact us at insights@elp-in.com or write to our authors:

Mukesh Chand, Senior Counsel – Email – mukeshchand@elp-in.com

Disclaimer: The information provided in this update is intended for informational purposes only and does not constitute legal opinion or advice.