LIABILITY OF THIRD PARTY APPLICATION PROVIDERS IN E-BANKING: A LEGAL FRAMEWORK UNDER RBI GUIDELINES

Anaihya Jena, KIIT School of Law

ABSTRACT

India's digital payments have boomed, with UPI transactions increasing from 1.5 billion to over 14 billion a month since 2020, apps like PhonePe and Google Pay that make banking easy for millions. With this increasing UPI transaction, scams have also increased through third party apps, it's not clear who pays. RBI rules mainly hold banks responsible for unauthorized transactions, giving customers zero blame if they report quickly or if the bank stumbles, while app providers dodge direct fault despite handling logins and approvals. This paper looks at RBI and NPCI rules, plus the 2026 draft changes for better alerts, payouts and calls for fixes like required app checks and shared responsibility borrowing from Europe's PSD2 model to minimise fraud, speed up fixes and keep people trusting digital money without slowing down new tech.

Introduction

India's banking system flipped dramatically around COVID. Pre pandemic, cash was largely used and people prefer visiting banks over online transactions. ATMs and branches handled most transactions with digital payments like net banking fixed at under 10%, held back by less smartphones use and trust issues. Post 2020, UPI exploded from 1.5billion transactions monthly in early 2020 to over 14 billion by 2025, as people preferred contactless transactions as it is easy and convenient which pushed apps like PhonePe into the spotlight, handling 80% of UPI flow.

This shift accelerates for banking to go truly digital across India with mobile apps and UPI now leading quick transfers, bill pays and more. Companies like PhonePe, GPay and others stepped in as middlemen letting users simply tap their phone for transaction between banks. But this created a twisted bond of banks, payment networks, app makers and also phone carriers.

The Reserve Bank of India (RBI), as the primary regulator has issued several guidelines governing electronic payment systems and customer protection. These guidelines ensure security, reliability and consumer protection in digital transactions. Despite these regulatory efforts, ambiguity continues regarding the exact allocation of liability among banks, third party application providers and other intermediaries.

This increasing dependency on technology platforms highlights the need for a clear legal structure that defines the responsibilities of the intermediaries. While banks remain the primary regulated entities within the financial system, third party application providers perform essential operational roles that impact transactions security and consumer protection.

Third Party Application Providers in Digital Banking

Third party application providers (TPAPs) are technology platforms that enable customers to initiate digital banking transaction through mobile applications without which users access banking services such as fund transfers, bill payments and merchant transactions.

To simplify these application gives a simple screen to link your bank account, punch in PIN or biometrics and send cash instantly no branch visits needed. In UPI, they bridge to a sponsor bank that handles the actual money shift. Within the UPI ecosystem, TPAPs act as intermediaries between customers and Payment Service Providers (PSP) banks.

Unlike banks, the TPAPs do not hold customer's deposits or directly manage funds, they're more like tech supporters managing the forepart of logins and approvals. However, they remain essential to the digital payment process because they control the interface through which authentication, transaction initiations and user interaction occur.

RBI and National Payments Corporation of India (NPCI), the regulatory bodies keep them in check through partnerships and also have expanded the role of third party applications within the digital payments ecosystem. Applications need NPCI approval and a bank tie-up to join UPI. Lately, rules let wallets like Paytm route UPI too, widening their reach but blurring lines on who's watching what.

This expansion of functionality has increased the operational significance of TPAPs while simultaneously raising questions about their legal accountability in the event of system failures, security breaches or unauthorised transaction.

Roles and Responsibilities of TPAP (Third Party Application Providers)

- TPAP is a service provider and participates in UPI through PSP Bank
- It is responsible to comply with all the requirements prescribed by PSP Bank and NPCI in relation to TPAP's participation in UPI
- It ensures that its systems are adequately secured to function on the UPI platform
- It is responsible to comply with all the applicable laws, rules, regulations and guidelines etc. prescribed by any statutory or regulatory authority in relation to UPI and TPAP's participation on the UPI platform including all circulars and guidelines issued by NPCI in this regard
- TPAP has to store all the payments data including UPI Transaction Data collected by TPAP for the purpose of facilitating UPI transactions, only in India
- Facilitates RBI, NPCI and other agencies nominated by RBI/ NPCI, to access the data, information, systems of TPAP and carry out audits of TPAP as and when required by RBI and NPCI.

- TPAP shall facilitate the end user customer with an option of to raise grievance through the TPAP's UPI app, email, messaging platform, IVR etc. for redressal of customer grievances.

Main Regulatory Authority in India

1. **Reserve Bank of India**

RBI regulates digital payment systems under the the Payment and Settlement Systems Act, 2007, which lets it set standards for all payment intermediaries. This include directions on prepaid instruments, payment gateways, customer safeguards for unauthorized debits and bank cyber rules. This empowers the central bank to supervise payment system operates and establish regulatory standards governing electronic transactions.

Several RBI guidelines shape how third party application providers operates, even if they target banks and payments setups more directly, including

- Master directions on prepaid Payments Instruments
- Guidelines on Payment Aggregators and Payment Gateways
- Customer protection limiting liability of customers in unauthorised electronic banking transactions
- Cyber security framework for banks

These regulatory primarily focus on banks and payments system operators rather than technology platforms. As result TPAPs providers are often indirectly regulated through their partnership with banks and payment network.

The RBI has introduced strict new draft guidelines for digital banking, slated for implementation on July 1, 2026, which significantly tighten customer liability rules for electronic transactions. The proposed rules, which amended the 2017 customer liability policy are developed to boost consumer protection against online fraud, covering UPI, card transactions and net banking.

Proposed 2026 RBI Guidelines

1. Zero Liability Mandate: The Customers will have zero liability and guaranteed reversal of funds in cases of bank negligence, such as security lapses or failure to send alerts.

2. Third Party Breaches: If fraud results from third party breach and is reported within 5 days (previously it was 3days), the customer has zero liability.

3. Mandatory Alerts: banks must send instant SMS alerts for all transactions exceeding 500 rupees.

4. Small Value Fraud Compensation: This will cover up to 85% of net losses (Maximum Rs. 25,000) for scams up to Rs 50,000, provided it is reported within 5days, allowing for compensation even if customer was partially tricked.

5. Bank Accountability: The burden of proof foe showing customer negligence lies with the bank, which must resolve complaints within 30 days.

2. National Payments Corporation of India (NCPI)

NPCI is an umbrella organisation for operating retail payments and settlement systems in India. It is an initiative of the RBI and the India Bank's Association (IBA), established under the provisions of the Payments and Settlement Systems Act, 2007 with the objective of creating a strong, secure and efficient payment and settlement infrastructure in India. in the context of its utility oriented objectives, NPCI has been incorporated as a not for profit company under Section 8 of the Companies Act, 2013. It works as fundamental network provider for entire banking system providing both physical and electronic payment and settlement systems. NCPI is mainly focused on driving innovation in retail payment systems through the adoption of technology by such means enhancing operational efficiency and expanding the reach of payment systems nationally.

Roles and Responsibilities of NPCI

- NPCI owns and operates the Unified Payments Interface (UPI) platform

- Prescribes rules, regulations, guidelines and the respective roles, responsibilities and liabilities of the participants, with respect to UPI. This also includes transaction processing and settlement, dispute management and clearing cutoffs for settlement.

- NPCI approves the participation of Issuer Banks, PSP Banks, Third Party Application Providers (TPAP) and Prepaid Payment Instrument issuers (PPIs) in UPI

- It provides a safe, secure and efficient UPI system and network

- Provides online transaction routing, processing and settlement services to members participating in UPI

- NPCI can, either directly or through a third party, conduct audit on UPI participants and call for data, information and records, in relation to their participation in UPI

- Provides the banks participating in UPI access to system where they can download reports, raise chargebacks, update the status of UPI transactions etc.

3. Payment Service Provider (PSP)

It is a third party company also a known as merchant service provider that authorise businesses to securely accept various electronic payments such as credit cards, debit cards, UPI and bank transfer both online and offline. They act as an intermediary between consumers and merchants combining payment methods.

Roles and Responsibilities of Payment Service Provider (PSP Bank)

- PSP Bank is a member of UPI and connects to the UPI platform for providing UPI payment facility to the PSP Bank and Third Party Application Providers (TPAP) which in turn enables the end user customers / merchants

- It is either through its own app or TPAP's app, on-boards and registers the end-user customers on UPI and links their bank accounts to their respective UPI ID.

- It is responsible for authentication of the end user customer at the time of registration of such customer, either through its own app or TPAP's app

- PSP Bank engages and on boards the TPAPs to make the TPAP's UPI app available to the end-user customers

- It has to ensure that TPAP and its systems are adequately secured to function on UPI platform

- It is responsible to ensure that UPI app and systems of TPAP are audited to safeguard security and integrity of the data and information of the end-user customer including UPI transaction data as well as UPI app security

- PSP Bank has to store all the payments data including UPI Transaction Data collected for the purpose of facilitating UPI transactions, only in India

- PSP Bank is responsible to give all UPI customers an option to choose any bank account from the list of Banks available on UPI platform for linking with the customer's UPI ID.

- Responsible to put in place a grievance redressal mechanism for resolving complaints and disputes raised by the end-user customer

Allocation of Liability in e-Banking Transactions

1. The Hierarchy of Liability

The RBI currently follows a fault based system. Liability is determined by where the security "leak" occurred and how quickly you reported it.

- Zero Liability for Customers:

    1. Bank Negligence: If the bank is at fault (e.g., a system hack or internal fraud), the customer pays nothing, regardless of when they report it.

    2. Third-Party Breach: If a breach happens in the system (not the bank's fault, but not the customer's either), and the customer reports it within 3 working days, they have zero liability.

- Limited Liability (The "Delay" Penalty): If you report a third party breach within 4 to

7 working days, your liability is capped based on your account type:

1. Basic Savings Deposit Accounts: Max Rs. 5,000.
2. Savings, Current Accounts or Credit Cards (Limit more than 5L): Max 10,000.
3. Credit Cards (Limit less than 5L) or MSME Accounts: Max 25,000.

- Full Liability (The "Negligence" Factor): If the bank can prove you were negligent such as the person himself has shared the OTP or PIN, person bears the full loss until you report it. Once the person reports it, any further transactions are the bank's responsibility.

2. The "Application" Dynamic: Middlemen & Intermediaries

While many users interact only with applications like GPay, PhonePe or mobile banking apps, the legal "buck" almost always stops with the bank.

- Bank as the Legal Shield: Under current norms, the bank is the Regulated Entity. If a third party application has a security glitch like a weak API, the bank is usually held responsible for the intermediated transaction.
- Shadow Reversals: In many cases, banks perform a shadow reversal (temporarily crediting your account) within 10 days of a report while they investigate the application's failure privately.
- Intermediary Accountability: New rules make it harder for apps to hide. While the bank remains responsible to you, the application must prove clean hands that their systems didn't facilitate the fraud to avoid being penalized by the bank or the regulator later.

Legal Challenges in Determining TPAP Liability

1. Technological Intermediation

TPAPs function as technological intermediaries, not financial institutions. Their main role is to help user interaction with banking system. This raises questions regarding how they should be classified for liability purposes as service providers, intermediaries or financial entities.

2. Data Protection and Privacy Concerns

Third party applications collect and process a lot of user data, including transaction history and personal information. If this data is misused or compromised, it could lead to financial losses and privacy violations.

3. Cybersecurity Risks

Phishing, malware, SIM swaps hit apps first. When such vulnerabilities originate from weakness in application security, determining liability becomes complex.

Dispute Resolution Mechanisms

The dispute resolution process in digital payments generally involves banks, payment network and application providers. The lack of a clear and defined liability framework can delay dispute resolution and undermine consumer protection.

- The victim must report the unauthorised or fraudulent transaction to the bank or the third party application provider (TPAP) within 3 to 10 days through banking applications, Interactive Voice Response (IVR) systems, SMS or online grievance portals. After filing the complaint, a unique complaint reference number is generated for tracking purposes.

  Under Section 35A of the Banking Regulation Act, 1949, it is the duty of banks to provide grievance redress mechanism, which allows the RBI to issue directions to banks in the public interest. The timeline for customer reporting and zero liability protections are regulated by the 2017 RBI circular concerning customer protection and limiting customer liability in authorised e banking transactions.

- Once a complaint is received, the bank is required to verify the transaction and decide if it was caused by a system failure, technical error or fraudulent activity. Bank must require to comply with timeline prescribed by the RBI under the “Harmonisation of Turn Around Time (TAT) and Customer Compensation for Failed Transactions Using Authorised Payment Systems” circular (2019) for failed transaction.

  In cases involving UPI payments, the bank works with the counterparty bank and the

National Payments Corporation of India, which manages the Unified Payments Interface under the regulatory supervision of the RBI.

The regulatory basis for such oversight stems from Section 18 read with Section 10(2) of the Payment and Settlement Systems Act, 2007, which empowers the RBI to regulate and supervise payment systems in India.

- If the issue remains unresolved at the bank level, the complaint may be forwarded to the Online Dispute Resolution (ODR) mechanism managed by the National Payments Corporation of India. the Payment Settlement Systems Act, 2007, which gives the RBI statutory authority to regulate electronic payment infrastructure and settlement arrangements, governs this dispute resolution system.

- If still the complaint is not resolved within 30 days, the customer may approach the Ombudsman Scheme for Digital Transactions or Integrated Ombudsman Scheme, 2021 administered by the Reserve Bank of India. Section 35A of the Banking Regulation Act of 1949 and the Reserve Bank of India Act, 1934's supervisory powers of the RBI provide the Ombudsman mechanism its statutory authority. The Ombudsman has authority to order compensation and corrective majors if service deficiencies or grievance handling delays are found.

Regulatory Gaps

- Even with this organised grievance procedure in place, there are still practical issues. Investigation and dispute resolution fragmentation caused by the involvement of banks, NPCI and TPAPs. Moreover, banks and third party intermediaries are not clearly assigned liabilities under the current regulatory frameworks under the Payment and Settlement Systems Act, 2007 and RBI circulars, especially when it comes to application level vulnerabilities or data breaches. This uncertainty often leads to disagreements over accountability and may out the onus of demonstrating fault on the client.

Comparative Regulatory Approaches

The European Union has established one of the most comprehensive legal structure regulating digital payment platform and the role of third party technology providers. The main law

governing this area is the Payment services Directive (PSD2) which creates a consistent regulatory framework for electronic payments across EU member states. PSD2 acknowledges the increasing importance of fintech companies and officially includes third party payment service providers within regulated financial system.

Under PSD2, two major categories of third party providers are recognised;

- Payment Initiation Service Providers (PISPs), which allows users to start payments directly from their bank through external applications.

- Account Information Service Providers (AISPs) which collects financial data from multiple accounts. These entities need to secure regulatory approval and comply with operational, cybersecurity and governance standards similar to those imposed on financial institutions.

The directive implements Strong Customer Authentication (SCA), which mandates multi factor authentication to improve transaction security and lower the risks of frauds. Mainly, PSD2 sets up a clear liability framework for liabilities by assigning responsibility between banks and third party providers in cases of unauthorised transactions or system failures. If a security breach or system failure happens in a third party provider's system that provider may be held financially liable.

In total, the European Union model offers clear legal recognition and regulatory supervision of technology intermediaries ensuring that responsibility for digital payment failures in digital transactions is distributed among all. This framework provides useful guidance for regions aiming to strengthen accountability and consumer protection in digital banking system.

Conclusion

Digital payments in India have changed how everyone handle money. Apps like PhonePe and Google Pay are now part of daily life for millions of people. While these apps make banking much faster, the legal rules haven't fully kept up with how they work.

Right now, if a scam or a technical error happens, the bank is almost always the one held responsible. This creates a big gap because the apps are the ones managing the screens where we type our PINs and approve payments. It doesn't seem fair for banks to carry all the blame

while the app providers have very little direct responsibility when their own systems fail.

The upcoming 2026 regulations represent a positive move as they offer customers greater safeguards and quicker refund processes. However, they still don't clearly state what the app providers must do to keep data safe. When examining how Europe approaches this issue, they enforce stricter security regulations on these applications and share the financial losses if fraud occurs on their platforms.

For people to keep trusting digital money, India needs to update its laws. We need to make sure that apps are audited just as strictly as banks and that they are held accountable when things go wrong. Making the apps share the responsibility won't slow down technology; it will just make the whole system safer and fairer for everyone.

Reference

1. https://www.thehindubusinessline.com/blexplainer/electronic-banking-frauds-what-frauds-are-covered-how-much-will-be-compensated-how-to-claim-your-refund/article70726036.ece

2. https://paytm.com/blog/payments/upi/roles-and-responsibilities-of-npci-psp-and-tpap-in-upi/

3. https://ssrana.in/articles/rbi-issues-circular-limiting-liability-of-customers/

4. https://www.thehindubusinessline.com/blexplainer/electronic-banking-frauds-what-frauds-are-covered-how-much-will-be-compensated-how-to-claim-your-refund/article70726036.ece

5. https://ssrana.in/articles/rbi-issues-circular-limiting-liability-of-customers/

6. https://www.ijfmr.com/research-paper.php?id=55593