Fountainhead Legal

Technology Law | Data Privacy | Regulatory Strategy

FL FOUNTAINHEAD LEGAL

The RBI's New Customer Protection Framework for Electronic Banking Transactions

What the Directions Say, and Where They Will Break

Why this note exists

Most everywhere we have read a summary of these directions. This is not that.

The Draft Third Amendment Directions introduce a substantially rewritten framework for customer liability in fraudulent electronic banking transactions. On its face, it is a consumer protection measure - and it is. But for General Counsel and compliance heads at commercial banks, digital lenders, payment aggregators, and platform businesses, what matters is not what the framework says. It is where the framework will generate disputes, where the definitions will be contested, and where institutions that have not built the right internal architecture before July 1 will find themselves exposed.

That is what this note addresses.

What the framework actually does

The new Section DA introduces a new liability architecture built around six definitional categories that did not previously exist in this form.

The six new definitions are where the legal work will happen. "Authorised electronic banking transaction," "fraudulent electronic banking transaction," "unauthorised electronic banking transaction," "negligence by a bank," "negligence by a customer," and "third-party breach" are now defined terms and the liability outcome in any given case flows directly from which category a disputed transaction falls into.

On the surface this looks like clarity. In practice it creates a new terrain of interpretive disputes.

Where the framework will break
Five pressure points

Pressure point 1: The "authorised transaction" definition includes transactions executed under coercion or deception

Paragraph 4(3A) defines an authorised electronic banking transaction to include, among other things, a transaction executed by a customer "by granting approval under coercion or duress from the third-party" and a transaction where the customer is "tricked into willingly sending money to a scammer posing as a legitimate recipient."

Read this carefully. These transactions: classic social engineering scenarios, authorised payment frauds, mule account scams are defined as *authorised* transactions. They are simultaneously captured under the definition of "fraudulent electronic banking transaction" at 4(15A), which covers authorised transactions falling under 4(3A)(ii).

This definitional overlap is not an error. It is a deliberate policy choice to extend the framework's reach to authorised payment fraud. But it will generate significant disputes about classification. A bank receiving a complaint about a UPI scam where the customer willingly initiated the transfer will need to determine whether that transaction is an "authorised" transaction under 4(3A)(i), a "fraudulent authorised" transaction under 4(15A), or whether customer negligence under 4(20B) applies to reduce or eliminate liability. These are not the same analysis. Getting the classification wrong at the complaint intake stage has direct consequences under the compensation mechanism.

Pressure point 2: The negligence definitions are drafted at a level of generality that will not survive contact with facts

"Negligence by a bank" under 4(20A) includes "not acting diligently upon a customer notification regarding unauthorised electronic banking transactions or loss of payment instruments." "Negligence by a customer" under 4(20B) includes "not paying attention to specific, directed and clear warnings from the bank that a prospective transaction is likely a scam."

Both definitions use language - "diligently," "specific, directed and clear" - that presupposes a factual assessment rather than providing one. What constitutes "diligent" action on a customer notification will be determined case by case, in complaints before the bank's internal grievance process, then potentially before the Banking Ombudsman, and in contested cases before courts. The same applies to what makes a warning "specific, directed and clear" as opposed to a generic fraud advisory that customers routinely ignore

Banks that have not built internal documentation systems capable of demonstrating, complaint by complaint, that they acted diligently and that their warnings were specific rather than generic, will find the negligence determination consistently going against them.

Pressure point 3: The five-day reporting window is a liability cliff edge

Paragraph 76L gives customers zero liability and full reversal rights where fraud is reported within five calendar days but only for third-party breach cases. Paragraph 76M addresses what happens when the same third-party breach is reported after five calendar days, which triggers the compensation mechanism at 76T rather than automatic zero liability.

Five calendar days is a short window. Fraud is frequently discovered late. Statements are reviewed monthly, elderly customers may not check accounts frequently, and in complex scam architectures the fraud may not be visible until a subsequent transaction triggers recognition. The directions do not address what happens when the customer can demonstrate that the fraud was not discoverable within five days. There is no discovery rule equivalent here.

This is a gap that will generate complaints. GCs at banks need to decide in advance, as part of the policy required under 76A, how they will handle late-reported fraud where delayed discovery is plausible and well-evidenced. Banks that treat the five-day window as a hard cut-off without exercising the discretion available under 76P (which permits waiver of customer liability at the bank's discretion) will generate avoidable disputes.

Pressure point 4: "Third-party breach" pulls payment aggregators and TPAPs into the liability map

The definition of third-party breach at 4(26A) explicitly includes "deficiency on the part of an intermediary such as a Third-Party Application Provider (TPAP), Payment Aggregator (PA), Payment Gateway (PG), Telecom Service Provider (TSP)."

These entities are not regulated banks. They are not directly obligated under the Responsible Business Conduct Directions. But they are now named in the definitions that determine customer liability outcomes. The compensation mechanism at 76T operates regardless of where the deficiency lies in the system.

The practical consequence: a bank compensating a customer for a third-party breach has a potential recourse claim against the TPAP or PA through whose deficiency the breach occurred. That recourse architecture does not exist in these directions - it will need to be built through contract. Banks that have not reviewed their agreements with payment aggregators and TPAPs through this lens before July 1 are creating contingent liability with no recovery path.

Pressure point 5: The board-level policy obligation at 76A is more demanding than it appears

Paragraph 76A requires banks to formulate a policy covering customer protection in electronic banking transactions - defining rights and obligations, complaint timelines, disclosure requirements, and customer awareness mechanisms. The policy must be "transparent, non-discriminatory" and displayed on the bank's website.

The policy becomes the baseline against which the bank's conduct in any individual complaint will be assessed. A policy that is too specific creates a higher standard against which deviations will be measured. A policy that is too vague fails the transparency requirement and provides no cover. Getting this calibration right requires legal input that most internal compliance teams are not positioned to provide without external advisory.

The directions give no timeline for the policy to be put in place beyond the July 1 effective date. Banks that treat this as a post-launch exercise will find themselves in the first wave of complaints without a policy baseline to rely on.

What institutions should be doing now, before July 1st, 2026

Three workstreams need to run in parallel, not sequentially.

First, the classification architecture. Internal teams need a decision framework - not a policy document but a working decision tree, that maps how incoming complaints will be classified across the six definitional categories. This framework needs to be built before complaints arrive, not in response to them.

Second, the contract review. Agreements with payment aggregators, TPAPs, and payment gateways need to be reviewed for recourse provisions that address the third-party breach scenario now defined in the directions. Where those provisions are absent or inadequate, they need to be renegotiated or supplemented before the directions take effect.

Third, the 76A policy. This needs to be drafted with enough specificity to demonstrate compliance with the transparency requirement, and enough flexibility to allow the bank to exercise its discretion under 76P without contradicting its own policy. That balance requires careful drafting and board approval, which takes time.

A NOTE ON THE COMPENSATION MECHANISM

The mechanism at 76T introduces something genuinely novel: the Reserve Bank of India as a contributing party to customer compensation. For losses up to INR 50,000, the RBI contributes 65 percent of the 85 percent compensation payable for smaller claims, with the customer's bank and the beneficiary bank contributing 10 percent each.

This is a mechanism designed to make the compensation framework financially viable for banks while creating a strong incentive for the RBI to push for systemic improvements that reduce the volume of fraud reaching the compensation stage. Institutions that generate high complaint volumes under this framework should expect regulatory scrutiny that extends beyond individual complaint outcomes.

WHAT THIS MEANS FOR NON-BANK FINANCIAL ENTITIES

The directions apply to commercial banks. Small finance banks, payments banks, regional rural banks, and local area banks are explicitly excluded from the scope.

However, the definitional framework (particularly the third-party breach definition) creates indirect obligations for payment aggregators and TPAPs operating within the banking ecosystem. The practical advice for these entities: review your agreements with banking partners now, because those agreements will be the primary instrument through which your exposure under this framework is either managed or left unaddressed.

CLOSING OBSERVATION

The directions represent a significant step toward a more structured customer protection framework for digital banking in India. They also create a more complex liability map than currently exists: one where the outcome in any given dispute depends on definitional classifications that are not yet tested, discretionary standards that are not yet calibrated, and internal policies that most institutions have not yet written.

The institutions that will navigate this framework well are the ones that have built their internal architecture before the first complaint arrives under the new regime. The ones that will not are the ones treating July 1 as a compliance deadline rather than a liability inflection point.

*This note is published by Fountainhead Legal for general informational purposes. It does not constitute legal advice. Fountainhead Legal advises regulated businesses, technology companies, and financial institutions on data governance, digital enforcement, and regulatory risk. Enquiries may be directed through fountainheadlegal.in**

For More Information, Contact

Rashmi Deshpande
Email: rashmi@fountainheadlegal.com
Contact Number: +91 98338 62234

Aarushi Ghai
Email: aarushi@fountainheadlegal.com
Contact Number: +91 91314 15290

Address:
Fountainhead Legal
C - 2106, Oberoi Garden Estate
Chandivali Farm Road, Powai – 400 072

Website: https://fountainheadlegal.com/

LinkedIn:https://www.linkedin.com/company/fountainhead-legal/

FL FOUNTAINHEAD LEGAL