Comments to Draft Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Amendment Directions, 2026, dated 06 March 2026

On 6 March 2026, the Reserve Bank of India (RBI) released the **"Draft Amendment Directions for 'Review of Framework of Limiting Customer Liability in Digital Transactions"** (hereafter "**Amendments**").

The Amendments propose a framework to offer a one-time compensation to victims of small value fraudulent digital transactions. Further, it discusses the distribution of liability among the banks and the RBI, the reporting requirements that customers must satisfy and the obligations of the financial service providers.

In this response, we present four recommendations to the Draft Amendments.

1. **First,** we recommend **progressing to a negligence-based customer liability regime.** The current Amendments seek to make good to every customer who may have fallen prey to a victim fraud. However, they can claim such a compensation only once. Research[1] suggests that Indians encounter fraud attempts multiple times a week, that these attempts are growing more sophisticated, and therefore, it is not unlikely that customers may fall for them more than once. It may be prudent to imagine a compensation framework that factors in customers' role (or negligence), the sophistication of the fraud, the context of the customer (traditional and digital literacy, income levels, post-fraud reporting behaviour) etc. to determine the eligibility and quantum of compensation. Such a framework would compensate the customer when they have been rendered defenseless yet not discourage the customer from exercising caution when transacting online, as an unconditional compensation mechanism might.

   We recommend expanding the scope of negligence for both customer and the providers, identifying parameters that qualify as gross negligence on either side and developing a compensation mechanism that factors and the nature of negligence. Further, when qualifying customer negligence, attention may be paid to the customers' context of literacy, age, savviness in the digital landscape, income-level and sophistication of the fraud. Vulnerable customers may not be expected to meet high standards of attentiveness or defend themselves against frauds that are sophisticated even for the more evolved customers.
2. Second, **identifying authorized but fraudulent (unintended/mistaken/deceitful) transactions as a separate category, outside of the authorized transactions.** Transactions listed out in 4(3A)(i) are bona fide and fall outside the purview of any liability. On the contrary, transactions listed out from 4(3A) (ii) (a)-(c) are fraudulent where the customer may have authorized the transaction but were operating under external influence, coercion, information asymmetry, ignorance or other such contexts. Under the Indian Contract Act[2], such transactions amount to a voidable contract. Separating bonafide transactions from voidable ones is semantically proper. It may also help build more enduring compensation mechanisms, where the eligibility for compensation and its quantum will be determined by the role of the customer and the fraudulent actor. At that point, including authorized bona fide and authorized but unintended transactions in the same definition may be confusing.
3. Third, **streamlining reporting requirements** to make them more customer-centric. Specifically, we recommend doing away with the need to complain to both banks and the national cybercrime portal, instituting multiple reporting channels and raise awareness around the compensation scheme.

---

[1] https://gasa.org/knowledge-base/reports/state-of-scams-in-india-2025
[2] https://www.indiacode.nic.in/bitstream/123456789/2187/2/A187209.pdf

4. Fourth, we highlight the need to **develop complementing infrastructure for the successful execution of the Amendments,** including bolstering complaint acceptance infrastructure and a platform for banks to manage their claims.

I. Introduction

The Draft Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions (from here on, ***Amendments***[3]) come on the heels of the Statement on Developmental and Regulatory Policies, February 2026.[4] That Statement emphasised the need for revisiting the liability framework for electronic transactions to fold in UPI transactions that may have been authorised by the customer unwillingly/mistakenly or under information asymmetry, i.e., fraudulent transactions. The preamble to the Amendments emphasises that they will be reviewed after a year of enforcement, and eventually, the banks will be encouraged to reimburse the compensation without the dominant support of the RBI. Separately, the Statement also announced a discussion paper to explore safeguards to curb digital payment fraud. These developments point to the Amendments being an intermediate solution even as more enduring policies are being considered. To that extent, we welcome the Amendments as striking a balance between safeguarding unsuspecting customers in the event of fraud and, its one-time nature which encourages customers to be vigilant when transacting online. This framework addresses a significant gap, considering that the liability in these transactions was not explicitly defined. Further, it puts India in a minority league of countries that are decidedly tackling the challenge of fraud in electronic transactions. The UK, for instance, notified the Authorised Push Payment Reimbursement Policy[5] in October 2025, to replace its voluntary reimbursement mechanism that compensated customers for authorised but unintended transactions. Similarly, Brazil runs a special refund mechanism (MED)[6] that allows victims of fraud to recover their losses when transacting over PIX, the Brazilian equivalent of UPI.

II. Key recommendations:

1. Moving towards a negligence-based customer liability regime.

We appreciate and welcome the one-time, unconditional compensation offered to the victims of fraud. However, over the longer term, sound customer protection requires empowering the customers to identify, avoid, and report fraud attempts. Thus, over the longer run, compensating customers unconditionally may not incentivise them to be on guard. This may be particularly worrying, given that studies show 75% of Indians have encountered a scam, with nearly 17% encountering a scam multiple times a week, and another 17% encountering a scam once or twice in a month.[8] Therefore, customers' ability to identify and avert these fraud attempts may ultimately be the most potent defense against fraud.

Emerging regulations from other jurisdictions also point in this direction. The UK recognises a standard of gross negligence. When customers are found grossly negligent, they are not entitled to full compensation. The current liability framework also recognises the swiftness of the customers' response as grounds for determining their liability and, by extension, the compensation they are eligible for.

The Amendments offer us an occasion to define our own standards of negligence. The standard may be a function of several factors such as the customers' contribution to the occurrence of fraud, could the customer have reasonably suspected if it were a fraud, their post-fraud behaviour, submitting evidence, adhering to reporting protocols etc. Further, concessions may be made for the elderly, the less literate or new users. Such an approach can instill both discipline and trust in the customer and offer them compensation in circumstances when they are rendered defenseless.

---

[3] https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4922
[4] https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=62171
[5] https://www.psr.org.uk/our-work/app-scams/
[6] https://www.bcb.gov.br/en/financialstability/pixfaqen

In addition to customer-side factors, compensation and liability may also account for provider-side factors. For instance, grievance redress mechanisms that are hard to navigate by design may come in the way of customers raising timely complaints. Similarly, the provider may fail to caution customers when they transact with suspicious numbers, even when the providers have the means to. These lapses on the part of the provider should not come in the way of the customer getting their rightful compensation.

We recommend expanding the scope of negligence for both customer and the providers, identifying parameters that qualify as gross negligence on either side and developing a compensation mechanism that factors and the nature of negligence. Further, when qualifying customer negligence, attention may be paid to the customers' context of literacy, age, savviness in the digital landscape, income-level and sophistication of the fraud. Vulnerable customers may not be expected to meet high standards of attentiveness or defend themselves against frauds that are sophisticated even for the more evolved customers.

2. Identifying authorized but fraudulent (unintended/mistaken/deceitful) transactions as a separate category, outside of the authorized transactions.

The definition of Authorized Electronic Banking Transactions includes two distinct types of transactions. First, as under 4(3A)(i), any transaction willingly and intentionally executed by the customer themselves or by an authorized party on their behalf. Second, as under 4(3A) (ii) (a)-(c), transactions that may have been executed by or on behalf of customers but under coercive or misleading circumstances or unintentionally.

The nature of 'authorization' in these categories is very different. In the former, it is informed, active and intentional, i.e., meeting the requirements of any bona fide contract. In the latter, the authorization is either not intentional or is misguided and undertaken under circumstances of external influence, information asymmetry and even deceit. Contracts undertaken in these circumstances do not have the same legal standing as bona fide contracts. Categorising them both as 'authorised' may be confusing and misleading. On the other hand, decoupling them may have the following benefits:

(i) **Semantic Clarity.** It is important to emphasize that the two types of transactions are intrinsically different. While one meets the muster of a free contract, the other is fraudulent/deceitful or coercive. Under the Indian Contract Act, contracts executed under information asymmetry, external influence or fraudulent pretext are ***voidable,*** i.e., the aggrieved party can refuse to uphold it. Bundling such different transactions under the common definition of 'authorized transaction' diminishes their fundamental difference and may even reduce the significance of a liability framework. We recommend qualifying transactions covered in Section 4 (3A)(ii)(a)-(c) as *authorized but* ***unintended/fraudulent*** transactions.

(ii) **Future-proofing the Amendments.** Further, we imagine the Draft Amendments to be a steppingstone toward a more sustainable compensation regime predicated on customer negligence. In those circumstances, a distinct definition of authorized but fraudulent transactions may offer greater clarity and may even be crucial to a robust compensation framework. Identifying them as distinct may help futureproofing the Amendments.
Further, the liability framework would require several complementing tools. The liability framework will benefit from, for instance, an observatory to record new methods and types of fraud, an exercise to create and revise a taxonomy of fraud to not only help establish liability and negligence but also raise customer awareness. Furthermore, providing a taxonomy for the fraud could be useful in highlighting its distinctiveness, identifying its form, measuring its occurrence, as well as preventing and mitigating the fraud.[7] The identification of separate data points for this fraud could be beneficial for future policies and machine learning systems to prevent and mitigate the fraud. It appears imperative that the Draft Amendments recognise authorized but unintended/fraudulent transactions distinct from authorized transactions. The Amendments may also consider remaining open to revising the *definition of 4 (3A) (ii) to*

[7] https://www.centerforfinancialinclusion.org/article/addressing-fraud-and-scams-for-financial-inclusion-clients-the-case-for-a-victim-centered-approach/

include language that allows financial institutions and law enforcement officials to bring in a wider scope of frauds that occur within the definition of transactions authorized 'unintentionally' by the customer.

The current definition of transactions that were unintentionally authorized (4 (3A) (ii)) is currently limited to three sub-sections separated by an 'or' clause. However, considering the growing scope of fraud seen through the use of complex technical programs and artificial intelligence systems, our knowledge regarding the potentials and possibilities of this type of fraud may be limited. Possible language that could be included in this definition include "or any other fraud that may be authorized by the customer without their consent/ without their knowledge or intention". The flexibility in definition is also seen in the scope of 'unintended transactions' which follows a more principle-level approach (it includes all transactions not authorized by the customer).

3. Streamlining reporting requirements

Under the Amendments, victims of fraudulent transactions involving gross loss of an amount upto INR50,000 are eligible to once in a lifetime compensation under Section 76T in the following circumstances: (i) where the fraud has happened due to their negligence (Section 76N) and (ii) where the fraud arises from a third party breach reported after 5 days (Section 76M). In this section, we make suggestions for enhancing the customer-centricity of the reporting process.

(i) **The customer may report the issue to *either* the ban or the law enforcement agencies (not both)**. The eligibility for compensation under Section 76T is contingent on reporting the fraud within five calendar days to both (i) the concerned bank and (ii) the law enforcement agencies through the National Cyber Crime Reporting (NCRP) Portal or National Cyber Crime Helpline (1930). We believe these dual reporting requirements may be excessive, considering *that existing mechanisms already enable banks and law enforcement agencies to coordinate on reporting of frauds.* The Standard Operating Procedure issued by the Ministry of Home Affairs for NCRP- CFCFRMS, Custody, Restoration of Money and Grievance Redressal, explicitly allows banks to initiate cybercrime reporting on behalf of customers with the purpose to help victims report expeditiously and accurately. Thus, suggesting backend coordination between banks and law enforcement agencies is both feasible and already happening. In such scenario, placing the burden of dual reporting on customers may not yield additional benefits.
Thus, we recommend Draft amendments be revised to allow reporting to either banks or law enforcement agencies to be eligible for compensation under Clause 76T, with first instance of reporting to be treated as the as the relevant timestamp for calculation of five calendar days reporting requirement.

(ii) **Institute multiple, customer-centric reporting channels to reduce the friction that customers experience while reporting.** To improve fraud reporting rates and reduce uncertainty surrounding reporting process, it is essential that customers have multiple avenues available to report in simplified and accessible manner. Specifically, we recommend that victims should be able to:

a. Report frauds at multiple access points including the third-party application provider application, banking application, designated desks at the bank branch, the law enforcement agencies platforms and helpline as well as through physical visit to the police station. Moreover, reporting through any one channel should be sufficient for the purpose of claiming compensation under Clause 76T.

b. Track the status of their complaints, over and above receiving a complaint acknowledgment.

c. Seek assistance easily, in the form of Frequently Asked Questions (FAQs) or option to speak or chat with an agent.

d. Moreover, a customer should also be able to report all kinds of fraudulent transactions (unauthorised as well authorised but unintended ones), including the ones where they may be unsure whether they are eligible for compensation. This would reduce friction at the reporting stage and improve the quality of intelligence flowing into the system. At present, the hesitancy to report when unsure whether a transaction qualifies as a fraud is one of the prominent reasons[8] for underreporting. Thus, lowering the initial barrier will minimize exclusion of eligible cases from the compensation framework.

[8] https://gasa.org/knowledge-base/reports/state-of-scams-in-india-2025

(iii) **Take measures to make customers aware of the compensation mechanism and eligibility for it:** The effectiveness of this one-time compensation mechanism will depend on its uptake among the victims of fraud. In this context, customer awareness regarding the compensation scheme and its eligibility criteria will be a key enabler. We appreciate the emphasis on banks' responsibility to advise customers on reporting to the 1930 helpline of NCRP portal, however, this alone may not suffice.

In addition, other interventions would be required to create awareness about the compensation framework at scale. This may include *regular* campaigns through TV commercials, radio and social media platforms. Behavioural factors are particularly relevant in these campaigns; victims of fraud can experience embarrassment, loss of confidence, hesitation and uncertainty regarding the next steps following an incident. These factors can delay reporting and reduce the likelihood of accessing available remedies. Behavioural science research[9] suggests awareness campaign are most effective when designed to (i) ensure high recall value in the minds of targeted audience; (ii) be comprehensible to the audience and add information that was not known earlier and (iii) enable them to translate awareness through its emotionally resonant messaging.

In the past, under the banner of *RBI Kehta Hai*, several campaigns have been run to educate customers about online frauds, risks of sharing OTPs, passwords and PIN numbers, risks of clicking on unknown links as well as their right to grievance redressal. These campaigns have relied on simple, repeated messaging across multiple channels to improve customer awareness outcomes. We recommend similar emphasis on creating awareness to ensure eligible victims are aware of the compensation mechanisms available to them under Clause 76T and feel confident in accessing them.

4. Develop the infrastructural complementarities needed to execute the Amendments

i. **Bolstering the complaint acceptance infrastructure.** The system can anticipate a rise in incoming complaints on the back of the unconditional compensation. It is worth preparing the system for the surge. In this regard, increasing the complaint-handling capacity at all institutions, simplifying the digital journeys for lodging complaints and ensuring multiple channels to avoid any single channel being overwhelmed will be crucial. This is especially important because lodging complaints within the 'golden hour' help law enforcement agencies track the flow of the disputed sum. Further, technical wrinkles such as mapping the state cybercrime department to the domicile state of the complainant, as opposed to the state in which the fraud occurred may be crucial for complaint registration.[10]

ii. **Instituting internal platform for Banks to settle tripartite claims.** The proposed compensation mechanism implicates three parties: the beneficiary bank, the issuer bank and the RBI. The Amendments further provide for ex-post, quarterly reimbursement of compensation amounts to the banks by the RBI. The success of this compensation mechanism would require a robust operational settlement infrastructure, supported by unambiguous procedural guidance. In this context, we submit that Amendments consider complementing the compensation mechanism with an institutionalised claim management and settlement infrastructure that enables seamless coordination and end-to-end claim management between the regulator and participating banks. We recommend that such an infrastructure and procedural guidance may specifically provide for:

    - *Clarity on inter-bank dispute resolution protocol*: Disputes between the issuer and beneficiary banks are likely to arise on issues such as, (i) the determination of customer negligence, (ii) findings of the investigation (particularly when investigation is undertaken unilaterally), (iii) attribution of fault and consequent quantum of compensation. The absence of a clearly defined inter-bank dispute resolution protocol may undermine the certainity that the compensation framework seeks to establish in the allocation of liability. Internal experience demonstrates the importance of accounting for dispute resolution in the scheme design. For instance, the UK's older Contingent Reimbursement Model Code for Authorised Push Payment Scams, 2019, provided for alternative dispute resolution where payment system providers could not reach a unanimous agreement

[9] https://dvararesearch.com/wp-content/uploads/2023/12/Are-Fraud-awareness-Campaigns-Effective_Policy-Brief.pdf

[10] https://timesofindia.indiatimes.com/business/cybersecurity/jurisdiction-flaw-in-1930-helpline-costs-cyber-fraud-victim-crucial-response-time/articleshow/121391891.cms

regarding allocation, allowing bilateral selection of dispute resolution providers. Under the more recent Authorised Push Payment Reimbursement Policy dispute resolution arrangements are required to be designated in scheme rules, with Pay.UK, the scheme operator being responsible for ensuring that these arrangements are in place and operating effectively. At the domestic front, within the UPI ecosystem, the inter-bank disputes are managed through National Payment Corporation of India (NPCI) 's centralised infrastructure i.e. the Unified Real time Clearing & Settlement (URCS). This portal validates and processes the disputes raised by members. And if dissatisfied with the response of the other bank, the issue can be referred for arbitration to NPCI's Panel for Resolution of Disputes. A similar platform may be needed for banks to settle any disputes.

- *Claim management and coordination infrastructure:* An end-to-end claim management infrastructure and coordination infrastructure would be essential to streamline claims processing, given the tripartite nature of the proposed compensation mechanism involving the regulator, issuer bank and beneficiary bank. We recommend the development of a centralised platform which may have following functionalities:
    - (i) enable standardized claim submission and documentation,
    - facilitate real time tracking of claims by all entities across stages,
    - support routing of claims, including escalation pathways, and provide a formal communication interface between participants, and
    - enable auditability and transparency of the decisions.

Such an infrastructure would support providing compensation to the victims of small-value fraudulent transactions by the bank as well as timely reimbursement of the amount from the regulator. Comparable claim management infrastructures exist in other jurisdictions. For instance, in the UK's Authorised Push Payment Reimbursement Policy regime, a dedicated Reimbursement Claims Management System is available to support Payment System providers in standardised processing and management of claims.
