INDIALAW

BANKING AND FINANCE

Allahabad High Court Clarifies Bank Liability in Cases of Alleged Unauthorized Electronic Transactions: A Case Defining Customer Responsibility

AUTHOR Shrishail Kittad, Divy Lotia

PUBLISHED 7 October 2025

Introduction

In the evolving digital landscape, where financial transactions are increasingly conducted through online banking systems, the issue of liability in cases of unauthorized electronic transactions has gained immense judicial attention. The Allahabad High Court in Suresh Chandra Singh Negi and Another v. Bank of Baroda and Others (Writ-C No. 24192 of 2022, decided on July 17, 2025) examined whether a bank can be held liable to refund amounts alleged to have been fraudulently transferred when the evidence demonstrates that the customer's own credentials and devices were used. The Court, comprising Justice Shekhar B. Saraf and Justice Praveen Kumar Giri, addressed the intricate question of responsibility under the Reserve Bank of India's 2017 Circular on "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," providing critical clarification on the extent of both customer and bank liability in digital banking operations.

Table of contents

Factual Background

The petitioners, a father and son duo, were proprietors of two separate transformer fabrication businesses and maintained individual cash credit accounts with the Bank of Baroda. These accounts, having credit limits of ?1.20 crores and ?1.30 crores respectively, were operated with active internet banking facilities. On June 19, 2022, petitioner no. 1 transferred ?37,85,000 to petitioner no. 2's account, which was subsequently transferred to an unknown third-party account. Claiming that the transaction was unauthorized and fraudulent, petitioner no. 2 lodged a complaint with the Cyber Crime Police Station, Civil Lines, on June 21, 2022. Petitioner no. 1 also reported the incident to the Bank of Baroda. When no remedial action was taken, the petitioners approached the Allahabad High Court under Article 226 of the Constitution of India, seeking a writ of mandamus directing the Bank of Baroda and the Reserve Bank of India to restore the alleged embezzled amount of ?38,78,000 with 24% penal interest.

Contentions of the Petitioners

The petitioners argued that they had been victims of a sophisticated cyber fraud despite maintaining proper vigilance. They claimed that their SIM card was blocked during the time of the transactions, which prevented them from receiving OTPs or SMS alerts, thereby enabling unauthorized transfers from their account. The petitioners emphasized that they had duly informed the bank and the police within three days, in line with the RBI's guidelines on customer protection.

Their primary reliance was placed on the RBI Circular No. RBI/2017-2018/15, DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017, which mandates that if a customer notifies the bank of an unauthorized electronic transaction within three working days, the bank must restore the debited amount without delay and without any liability on the part of the customer. They further contended that as per the same circular, the burden of proof lies entirely on the bank to establish the customer's liability in such cases.

To reinforce their claim, the petitioners relied upon judicial precedents including State Bank of India v. Pallabh Bhowmick & Ors. (SLP No. 30677 of 2024), where the Supreme Court observed that banks must adopt robust technological measures to prevent fraudulent withdrawals, and Jaiprakash Kulkarni & Ors. v. The Banking Ombudsman & Ors., 2024 SCC OnLine Bom 1666, wherein the Bombay High Court held that if an account holder promptly reports an unauthorized withdrawal and no negligence is established, the bank is obligated to refund the amount.

Contentions of the Respondents

The Bank of Baroda contested the claim and asserted that the alleged transactions were initiated by the petitioners themselves using their own login credentials and registered mobile devices. The bank argued that petitioner no. 1 voluntarily transferred the funds to petitioner no. 2, who in turn transferred them to accounts that had been added as beneficiaries by him on June 18, 2022, one day prior to the transactions in question.

The Bank produced detailed evidence demonstrating that the transactions were executed through the same device, the same IP address, and the same registered mobile number used by the petitioners for regular banking activities. The bank also produced logs showing that OTPs were generated and used from the petitioner's registered mobile number and that petitioner no. 2 changed his internet banking password after completing the transfers. Since password changes require prior knowledge of the existing password, this act, according to the bank, confirmed that the petitioners themselves carried out the transactions. The respondents therefore argued that the narrative of cyber fraud was an afterthought devised to avoid personal accountability.

Judicial Analysis and Findings

After thoroughly examining the records, the Allahabad High Court concluded that the evidence overwhelmingly indicated that the disputed transactions were carried out by the petitioners themselves. The Court observed that the funds were transferred after the petitioners logged into their internet banking account, generated OTPs, and approved the transfers to accounts that had been added by petitioner no. 2 as beneficiaries. The IP address and device data corroborated that the same system was used throughout.

Furthermore, the Court noted that the petitioners received SMS alerts about the transactions at 12:44 p.m. on June 19, 2022, but chose not to report the issue immediately, instead lodging a cyber complaint the next day and an FIR only on June 21. This delay was considered inconsistent with the behavior of genuine victims of cyber fraud and was held to weaken their credibility. The Court therefore held that the plea of cyber fraud was a concocted story and that the petitioners' conduct revealed negligence and possible concealment.

Analysis of the RBI Circular

The Court then turned its attention to the RBI Circular on "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions." Under Clause 6(a) of the circular, a customer is entitled to zero liability if the unauthorized transaction occurs due to the bank's negligence or due to a third-party breach where neither the bank nor the customer is at fault, provided it is reported within three working days. Under Clause 7(b), however, a customer bears full or partial liability when the loss occurs due to his own negligence, such as sharing credentials or failing to secure devices, or when there is a delay in reporting the unauthorized transaction. The circular further provides that if the delay exceeds seven working days, the customer's liability shall be determined in accordance with the bank's board-approved policy.

The Court reaffirmed that although the burden of proof lies upon the bank to establish customer liability, the Bank of Baroda had successfully discharged this burden through documentary and technical evidence including account statements, beneficiary addition records, and IP logs. It further observed that the circular is designed as a protective mechanism to ensure that genuine victims of cyber fraud are safeguarded and that customers are educated about the risks of digital transactions. However, the Court clarified that the circular cannot be invoked as a means to mask personal mistakes or deliberate fund transfers as fraudulent activity.

Evaluation of Precedents

In addressing the precedents relied upon by the petitioners, the Court clarified that the ruling in Pallabh Bhowmick was not applicable since that case involved clear third-party fraud and prompt reporting by the account holder, whereas in the present case, the transactions were executed by the petitioners themselves. Similarly, the decision of the Bombay High Court in Jaiprakash Kulkarni was distinguished on the ground that in that case, the petitioner did not receive any alerts regarding the addition of new beneficiaries, demonstrating an external breach. In contrast, the present matter involved transactions approved from the petitioners registered devices and accounts. Hence, neither precedent provided any relief to the petitioners.

Court's Decision

Based on the detailed technical evidence and the conduct of the petitioners, the Court held that there was no unauthorized or fraudulent withdrawal of funds. It concluded that the transactions were knowingly and deliberately executed by the petitioners and that there was gross negligence on their part. The plea of cyber fraud was found to be unsubstantiated, and the claim for refund under the RBI circular was rejected.

The Court emphasized that the RBI circular's intent is to function as a shield for customers genuinely affected by unauthorized digital transactions, not as a sword to escape the consequences of their own negligence or misuse. Consequently, the writ petition was dismissed, and no direction was issued to the Bank of Baroda or the Reserve Bank of India for restoration of the funds.

Conclusion

The Allahabad High Court's decision in Suresh Chandra Singh Negi v. Bank of Baroda reinforces the principle that digital vigilance is a shared responsibility between financial institutions and customers. While the judiciary continues to uphold customer protection against external cyber frauds, this case underscores that such protection is not absolute. When transactions are proven to have been executed using the customer's own devices, credentials, and OTPs, the liability cannot be shifted to the bank under the guise of fraud.

The author concurs with the Court's reasoning and finds the judgment consistent with judicial precedents emphasizing both technological accountability and human diligence. The decision rightfully prevents misuse of consumer protection provisions and draws a clear line between genuine cyber fraud and cases stemming from customer negligence. As India advances toward a fully digitized financial ecosystem, this judgment serves as an important precedent balancing the dual imperatives of consumer security and personal responsibility in electronic banking.

For further details write to contact@indialaw.in

Related Practice Areas

Banking & Finance