A customer has zero liability in cases of unauthorized electronic banking transactions arising out of a third-party breach where the deficiency lies neither with the bank nor with the customer but elsewhere in the system, provided the customer notifies the bank within three working days of receiving communication regarding the unauthorized transaction

The **Bombay High Court** in the case of **Subodh C. Korde vs Union of India [Writ Petition No. 11990 of 2023] dated April 06, 2026**, has held that writ petition under Article 226 of the Constitution of India is maintainable against a private scheduled bank for the enforcement of the Reserve Bank of India's circulars and guidelines issued in the public interest, as the bank discharges a public function when acting in a capacity that involves public interest and the protection of customers in electronic banking.

The Court also clarified that under the RBI Circular dated 06/07/2017, a customer has zero liability in cases of unauthorized electronic banking transactions arising out of a third-party breach where the deficiency lies neither with the bank nor with the customer but elsewhere in the system, provided the customer notifies the bank within three working days of receiving communication regarding the unauthorized transaction.

Thus, the Court ruled that the burden of proving customer liability or negligence in unauthorized electronic banking transactions rests strictly on the bank, and the bank cannot absolve itself of liability merely by claiming that OTPs were generated and sent, without conclusively establishing the customer's complicity or negligence in sharing the credentials.

The High Court observed that while HDFC Bank may not be a 'State' or its instrumentality under Article 12 of the Constitution, a writ petition under Article 226 is maintainable against it because the Bank discharges a public function when it implements the guidelines formulated by the Reserve Bank of India (RBI) under Section 35A of the Banking Regulation Act for the protection of customers in electronic banking transactions.

The Court observed that the RBI Circular dated 06/07/2017 on 'Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' is independent of any criminal investigation to be conducted to establish any cyber-crime, as the RBI intended to protect the customer who has suffered financial loss on account of fraudulent or unauthorized electronic banking transactions.

Further, the Court noted that the burden of proving the customer's liability in case of unauthorized electronic banking transactions lies entirely on the bank. Since the Bank failed to establish that the Petitioner was careless or negligent, or that he had shared the password or OTP with anyone, the Court observed that the Petitioner was a victim of a SIM swapping fraud, which is a sophisticated form of identity theft where fraudsters take over a victim's phone number, resulting in the OTPs and banking alerts being received on a cloned/duplicate SIM in the hands of the fraudster.

The Court noted that the Bank's internal investigation report clearly admitted that the transactions were not alerted because the risk score was 691, and the alert was declined

despite the IP location of the disputed transactions (Chennai) being different from the genuine transaction IP location of the customer (Pune).

Since the Bank did not produce a single original log of sending messages or e-mails and its receipt by the Petitioner, but merely placed excerpts from the Log Book of a private agency to urge that the Bank had sent OTPs and e-mails, the Court concluded that since the fault lies neither with the Bank nor with the customer, but elsewhere in the system (third-party breach), and the customer notified the bank promptly, the clause fixing 'zero liability' on the customer gets triggered, entitling the Petitioner to a full refund.