* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

Judgment Reserved on: 17.02.2026

% ***Judgment Delivered on: 29.05.2026***

\+ **LPA 52/2025 & CM APPL. 4159/2025**

STATE BANK OF INDIA .....Appellant

versus

HARE RAM SINGH & ANR. .....Respondents

Advocates who appeared in this case

For the Appellant : Mr. Harin P. Raval, Senior Advocate along with Mr. Rajiv Kapur, Mr. Akshit Kapur, Ms. Riya Sood, Ms. Shreya Bansal, Advocates & Mr. Karnik Pandya (Chief Manager) & Mr. H.K. Kataria [Chief Manager (Law)].

For the Respondents : Mr. Ravi Chandra Prakash & Mr. Purushottam S. Tripathi, Advocates for Respondent No.1/Hare Ram Singh.
Mr. Atul Sharma, Mr. Abhinav Sharma, Mr. Ayush Srivastava & Mr. Snehashish, Advocates for Respondent No.2/Reserve Bank of India.

CORAM:
HON'BLE THE CHIEF JUSTICE
HON'BLE MR. JUSTICE TEJAS KARIA

JUDGMENT

TEJAS KARIA, J

1. The present Letters Patent Appeal arises from the judgment dated 18.11.2024 ("**Impugned Judgment**") rendered by the learned Single Judge in W.P.(C) No. 13497/2022 ("**Writ Petition**"), whereby the Writ Petition preferred by Respondent No. 1 was allowed and the order dated 20.10.2021 passed by the Banking Ombudsman of Respondent No. 2, the Reserve Bank of India ("**RBI**"), was set aside, and the Appellant-Bank was directed to pay Respondent No. 1 a sum of ₹2,60,000/- together with interest at the rate of 9% per annum from 18.04.2021, being the date on which the fraud was reported, as well as ₹25,000/- towards litigation costs.

SUBMISSIONS ON BEHALF OF THE APPELLANT

2. The learned Senior Counsel for the Appellant made the following submissions:

2.1 Respondent No. 1 maintains a savings account bearing No. 30051013904 with the Appellant-Bank at its Greater Noida Branch (the "**Bank Account**"). On 18.04.2021, an aggregate sum of ₹2,60,000/- was unauthorisedly withdrawn from the Bank Account by way of two transactions in the sums of ₹1,00,000/- and ₹1,60,000/- respectively ("**Subject Transactions**"). Thereafter, Short Message Service ("**SMS**") alerts in respect of the said transactions were delivered to the mobile number of Respondent No. 1 registered with the Bank Account.

2.2 The Subject Transactions were secured by Two Factor Authentication ("**2FA**") and were carried out using the Internet

Banking ("**INB**") credentials and One Time Passwords ("**OTPs**") transmitted to the registered mobile number of Respondent No. 1.

2.3 Respondent No. 1 contacted the Customer Care Department of the Appellant-Bank alleging that the Subject Transactions were unauthorised and fraudulent, for the purpose of lodging a complaint and seeking blockage of the Bank Account. Thereupon, the Bank Account and the INB facility pertaining thereto were immediately blocked.

2.4 Subsequently, Respondent No. 1 submitted a complaint dated 19.04.2021 / 20.04.2021 to the Branch Manager of the Appellant-Bank at its Greater Noida Branch. Thereafter, the matter was taken up with the INB Department of the Appellant-Bank for obtaining the beneficiary details pertaining to the Subject Transactions. The concerned branch of the Appellant-Bank also requested that a lien be marked, and a hold be placed on the Subject Transactions and sought refund of the disputed amount.

2.5 Thereafter, the INB Department of the Appellant-Bank shared the beneficiary details relating to the Subject Transactions. From the statement of account of the Bank Account, it was found that, on 18.04.2021, the INB profile linked to the Bank Account was accessed using the relevant user ID and password. Upon entry of the OTP transmitted to the mobile number registered with the Bank Account, the first transaction of ₹1,00,000/- was effected to a bank account maintained with

IDFC Bank, and the second transaction of ₹1,60,000/- was effected to One 97 Communications Ltd. (Paytm), being a merchant account. The beneficiary particulars, including the Merchant Code, RRN No. and IP Address, were also furnished by the INB Department.

2.6 As per the details received from the INB Department, Respondent No. 1 received the OTPs for approval of the Subject Transactions and, thereafter, SMS alerts confirming the successful completion of the Subject Transactions were also delivered to Respondent No. 1.

2.7 Upon realising that he had been defrauded, Respondent No. 1 lodged a report on the Online Cyber Crime Portal on 18.04.2021, filed a complaint dated 19.04.2021 at Police Station Hajipur, Vaishali, Bihar, and further registered a grievance in respect of the Subject Transactions under the Centralized Public Grievance Redress and Monitoring System ("**CPGRAMS**").

2.8 Respondent No. 1 further filed a complaint dated 26.04.2021 before the Banking Ombudsman of the RBI ("**BO-RBI**") against the Appellant-Bank in relation to the said matter, to which the Regional Business Office, Sector-51, G.B. Nagar, of the Appellant-Bank submitted its reply dated 20.05.2021.

2.9 Upon receipt of the complaint preferred by Respondent No. 1, a Committee / Competent Authority of the Appellant-Bank was constituted in terms of Circular No. R&DB/DB&NB/IDP-INB/8/2019-20 dated 13.01.2020 to examine the complaint of

Respondent No. 1 and take a decision with respect to the Subject Transactions.

2.10 By decision dated 14.07.2021, the Committee / Competent Authority of the Appellant-Bank rejected the claim of Respondent No. 1 in relation to the Subject Transactions and held, *inter alia*, that the Subject Transactions had been effected through INB; that Respondent No. 1 had received the OTPs for the Subject Transactions on his registered mobile number; that SMS alerts confirming the successful transactions had been sent to the mobile number registered with the Bank Account; and that Respondent No. 1 was an existing INB user who had also undertaken an INB transaction on the date of the Subject Transactions.

2.11 On 26.07.2021, the Chief Manager of the Appellant-Bank, Greater Noida Branch, issued a letter to Respondent No. 1 rejecting his complaint / claim on the ground that the Subject Transactions had taken place through INB; that the OTPs relating to the Subject Transactions had been received on the mobile number registered with the Bank Account; and that, in his complaint to Police Station Hajipur, Vaishali, Bihar, Respondent No. 1 had stated that, upon receiving a call from an unknown number, he accessed a link forwarded by an unknown person, which led to the Subject Transactions.

2.12 Aggrieved by the rejection of his complaint by the Appellant-Bank *vide* letter dated 26.07.2021, Respondent No. 1 approached the BO-RBI by way of complaints dated

06.08.2021 and 31.08.2021 seeking re-investigation of the matter and expeditious disposal of the complaints filed against the Appellant-Bank.

2.13 By order dated 20.10.2021 passed in relation to the complaint dated 26.04.2021, the BO-RBI observed that Respondent No. 1 was a victim of vishing and had been defrauded after clicking on an unknown link and that although the transactions were secured by 2FA by way of OTP, Respondent No. 1 was familiar with the INB application and POS transactions, having used the same earlier, because of that the transaction of ₹1,60,000/- made to One97 Communication was not within the purview of the BO-RBI and that the Appellant-Bank be advised to pay one-third of the disputed amount of ₹1,00,000/-, i.e., ₹33,340/-.

2.14 The BO-RBI, by the said order dated 20.10.2021, further observed that, notwithstanding rejection of the complaint, Respondent No. 1 would remain at liberty to approach a civil court of competent jurisdiction or such other authority in accordance with law for redressal of his grievance. Accordingly, the grievance of Respondent No. 1 was treated as resolved and the complaint was closed under Clause 11(3)(a) of the Banking Ombudsman Scheme, 2006 ("**BOS 2006**") as "*settled by the bank*".

2.15 Consequently, in compliance with the directions issued by the BO-RBI, the Appellant-Bank credited a sum of ₹33,340/- to the account of Respondent No. 1 on 06.10.2021, which amount was accepted by Respondent No. 1 without demur or reservation. It

is, therefore, contended that the doctrine of estoppel would apply in the present case to preclude any further claim.

2.16 Respondent No. 1, thereafter, filed the Writ Petition, *inter alia*, seeking the following reliefs:

> "*(i) Issue writ of mandamus or any other appropriate writ, Order or direction quashing the rejection order dated 26.07.2021 by SBI Branch Greater Noida (Annexure P/8 herein) as violative of Articles 14, 16 and read with Article 300A of the Constitution of India read with RBI Master Circular dated 06.07.2017;*
>
> *(ii) Issue writ of mandamus or any other appropriate writ, Order or directions to the respondents to restore the amount illegally siphoned off from the Petitioner's SBI savings Account bearing No. 30051013904 IFSC Code: SBIN0004324 on 18/4/2021 by unknown 3rd Parties amounting to Rs 2,27,000/- with interest and; "*

2.17 The INB profile of the Bank Account of Respondent No. 1 was successfully logged in at 17:09:55 hours and 17:28:03 hours on 18.04.2021 and the OTPs were successfully delivered to Respondent No. 1's registered mobile number on three occasions at 17:10:18, 17:28:15 and 17:29:42 on 18.04.2021 for approval of transaction of ₹10/-, ₹1,00,000/- and ₹1,00,000/- respectively, which were followed by transaction acknowledgments through SMS, which was based on the documentary evidence produced by the Appellant-Bank and confirmed by the RBI in its written submissions filed in the Writ Petition. Thus, Respondent No. 1, an academician and a highly educated individual was negligent and fell prey to the scamsters.

2.18 Inasmuch as the Subject Transactions were 2FA transactions effected using the INB credentials and OTPs transmitted to the mobile number registered with the Bank Account, the occurrence of the fraud is attributable to the negligence of Respondent No. 1 in clicking upon an unknown link received on his mobile phone, thereby compromising access to the device and facilitating misuse of the OTPs by the cyber fraudster. It is, therefore, submitted that the present case squarely falls within Clause 7(b)(i) of the RBI Circular dated 06.07.2017 titled *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions* ("**2017 RBI Circular**"), and that the Appellant-Bank cannot be held liable for the loss allegedly suffered by Respondent No. 1 on account of his own negligence, which provides as under:

> "***Limited Liability of a Customer***
> ***(a) Zero Liability of a Customer***
> *6. A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:*
> *(i) Contributory fraud / negligence / deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).*
> *(ii) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorized transaction.*
>
> ***(b) Limited Liability of a Customer***
> *7. A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:-*

(i) In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.
(ii) In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value."

2.19 The learned Single Judge failed to appreciate that, in terms of Clause 7(b)(i) of the 2017 RBI Circular, Respondent No. 1 was negligent in safeguarding his confidential and sensitive financial information and in clicking upon the unknown link received on his mobile number. The obligation to maintain the confidentiality of such sensitive financial information and data rests upon the customer. Negligence, in this context, imports the duty of care expected of a person of ordinary prudence. In the present case, Respondent No. 1 failed to exercise due care and caution before clicking upon an unknown link, thereby compromising access to his mobile device and enabling the OTPs and INB credentials, which were within his exclusive knowledge, to be misused by cyber fraudsters.

2.20 The learned Single Judge further failed to appreciate that the OTP, user ID and password are not known to the Appellant-Bank, the same being system-generated and made available to

the account holder at the time of effecting the transaction. No transaction through INB can be carried out without the use of such credentials. Once a customer shares or otherwise compromises such credentials in favour of any third party, the Appellant-Bank cannot be held liable for the consequences thereof.

2.21 Even assuming that Respondent No. 1 was the victim of a phishing attack, *i.e.*, a voice-phishing scam whereby individuals are induced through telephone calls to disclose sensitive banking information, the same occurred on account of Respondent No. 1's own negligence or lack of due caution, without any direct intervention on the part of the Appellant-Bank. Accordingly, the Appellant-Bank could not have been held liable to refund or compensate Respondent No. 1 in terms of Clause 7(b)(i) of the 2017 RBI Circular.

2.22 The Appellant-Bank has consistently issued SMS advisories to its customers cautioning them not to click upon links received from unknown sources, not to download applications from unverified sources, and not to disclose passwords, MPINs, OTPs or other confidential credentials. Similar awareness measures have also been undertaken through electronic media, print media and customer awareness programmes. The 2017 RBI Circular is explicit that, where the loss arises due to the negligence of a customer, the customer is liable to bear the entire loss, and the bank cannot be made responsible for such unauthorised transactions. Since the present case is attributable

to the negligence of Respondent No. 1, the Appellant-Bank cannot be saddled with liability under the 2017 RBI Circular.

2.23 An OTP is a cyber security measure adopted by the Appellant-Bank for every online transaction initiated by a customer. Such OTP is generated and delivered to the customer's registered mobile number, and the transaction is completed only upon entry of the OTP on the relevant platform or payment gateway. This constitutes a secure mode of conducting online transactions unless the recipient compromises the sanctity or confidentiality of the OTP. In the present case, the Subject Transactions were carried out through INB by logging into the Bank Account using the user ID and password and thereafter authorising the transactions through OTP. The loss suffered by Respondent No. 1 is, therefore, stated to have arisen from his own negligence in clicking upon the unknown link received on his mobile number.

2.24 A bank, acting as agent for its customer, cannot ordinarily refuse to process an online transfer where the transaction appears to have been duly authorised by the customer. OTPs delivered to the customer's registered mobile number serve to authenticate a transaction, particularly where the transactions are 2FA transactions carried out using valid INB credentials.

2.25 Further, even if the learned Single Judge was of the view that the BO-RBI had failed to judiciously consider the entire controversy and had overlooked certain material aspects of the matter, the proper course would have been to remit the matter

to the BO-RBI for reconsideration. It was also submitted that a statement had been made on behalf of the BO-RBI expressing its willingness to reconsider and decide the matter afresh, if so directed by this Court.

2.26 The learned Single Judge also failed to appreciate that, prior to the receipt of the complaint by the Customer Care Department for placing the Subject Transactions on hold, the disputed amounts had already been transferred to the beneficiary account. Notwithstanding the same, the Appellant-Bank immediately blocked the Bank Account and deactivated the INB facility operative in relation thereto.

2.27 The learned Single Judge further failed to appreciate that, since the credentials, *viz.* the OTP, user ID and password, had been shared or otherwise compromised by Respondent No. 1 in the course of the telephonic interaction which culminated in the Subject Transactions, Clause 6 of the 2017 RBI Circular pertaining to zero liability of the customer, even where the complaint is made within three days, would have no application, the alleged loss having arisen on account of Respondent No. 1's own negligence.

2.28 The learned Single Judge failed to appreciate that for every transaction, customer receives SMS alerts with transaction details. The said SMS have the following suffix:

> "*If not done by you, forward this SMS from mobile number registered with SBI to 9223008333 to deactivate your user id. You may also call 1-800-111109*"

2.29 The learned Single Judge failed to appreciate the steps taken by the Appellant-Bank on receipt of the complaint received from Respondent No. 1 such as the Bank Account and INB facility therein was blocked, Complaint was taken up with the concerned INB Department for seeking the details of the beneficiary of the Subject Transactions. However, since the transaction of ₹1,60,000/- was made to One97 communication Ltd. which is not under Beneficiary Owner purview and amount was already credited, the Appellant-Bank could not retrieve the said amount. However, for another transaction of ₹1,00,000/-, *vide* order dated 20.10.2021 passed by BO-RBI, the Appellant-Bank was directed to pay 1/3rd of the amount i.e., ₹33,340/, which was paid by the Appellant-Bank.

2.30 Therefore, the Appellant-Bank could not have been held liable to compensate the entire amount of ₹2,60,000/- along with interest at 9% per annum for the loss suffered by Respondent No. 1 due to his own negligence, especially when the Appellant-Bank has paid a part amount of ₹33,340/- as per the directions of the BO-RBI in the order dated 20.10.2021 to avoid further litigation. Respondent No. 1 having accepted the amount as directed by BO-RBI without any reservation, Respondent No. 1 has forgone his right for further litigation. The complaint was accordingly closed by BO-RBI under clause 11(3)(a) of BOS- 06 as '*settled by the bank*'.

2.31 The learned Single Judge failed to appreciate that the Appellant-Bank had adhered to the applicable guidelines and

that its Information Technology Department continuously updates and strengthens its safeguards to address emerging threats and evolving modes of cyber fraud, including phishing attacks, through security features on its digital platforms as well as advisories and notices issued to customers by SMS from time to time. Accordingly, the Appellant-Bank could not have been held deficient in service in the Writ Petition.

2.32 The learned Single Judge further failed to appreciate that, prior to the complaint dated 20.04.2021 made before the Appellant-Bank at its Greater Noida Branch, Respondent No. 1 had already lodged a Cyber Complaint dated 18.04.2021 and a complaint dated 19.04.2021 at Police Station Hajipur, Vaishali, Bihar in relation to the Subject Transactions, both of which were under consideration. The Cyber Crime Cell and Police Station Hajipur, Vaishali, Bihar were, therefore, already seized of the matter and conducting investigation. In the presence of such disputed questions of fact, and when the matter was under investigation by the competent authorities dealing with cyber fraud, the writ court ought not to have intervened and passed the Impugned Judgment. The learned Single Judge also failed to appreciate that the Writ Petition was not maintainable, the controversy involving allegations of cyber fraud by a third-party fraudster necessarily requiring detailed investigation and evidence, including to identify the perpetrator and determine whether Respondent No. 1 had in fact shared the OTPs.

2.33 The learned Single Judge further failed to appreciate that, if Respondent No. 1 was indeed a victim of cyber fraud perpetrated through a phishing attack, the appropriate forum would have been the Controller / Adjudicating Officer under the Information Technology Act, 2000, vested with the power to adjudicate such complaints, with a further statutory right of appeal available before the Appellate Tribunal. Respondent No. 1, therefore, had an efficacious alternative remedy under the statute, and the Writ Petition was not maintainable on that ground as well.

2.34 The reasons set out by the Appellant-Bank in its letter dated 26.07.2021 rejecting the complaint dated 20.04.2021 filed by Respondent No. 1 were not considered by the learned Single Judge, notwithstanding that the same stand recorded in Paragraph No. 5 of the Impugned Judgment. Likewise, the written submissions filed on behalf of the Appellant-Bank were neither dealt with nor considered.

2.35 The learned Single Judge also failed to appreciate that the 2017 RBI Circular had been duly complied with by the Appellant-Bank and that all requisite steps were taken by it. If Respondent No. 1 was defrauded, the same occurred on account of his own negligence, for which the Appellant-Bank could neither have been held liable nor found deficient in service. The decision in ***Tony Enterprises v. RBI*** 2019 SCC OnLine Ker 5366 is, accordingly, inapplicable to the facts and circumstances of the present case.

2.36 The learned Single Judge further failed to appreciate that there was no deficiency or negligence on the part of the Appellant-Bank, and that Respondent No. 1 had shared or otherwise compromised the INB credentials with a third party / fraudster, for which reason the fraud cannot be attributed to the Appellant-Bank. In any event, a sum of ₹33,340/- was paid by the Appellant-Bank to Respondent No. 1, and the remaining loss was liable to be borne by Respondent No. 1 in terms of Clause 7(ii) of the 2017 RBI Circular.

2.37 In the present case, no loss occurred after Respondent No. 1 reported the unauthorised transaction to the Appellant-Bank, Greater Noida Branch, which immediately blocked the Bank Account and deactivated the INB facility in order to prevent any further online transactions. Even under the minimum liability regime contemplated by Clause 7(ii) read with Table 1 of the 2017 RBI Circular, the maximum liability would be ₹25,000/-. The learned Single Judge failed to take this material circumstance into account while fastening liability for the entire loss upon the Appellant-Bank.

2.38 The learned Single Judge also failed to appreciate that, upon receipt of the complaint and having regard to the negligence attributable to Respondent No. 1, a Fraud Case Report ("**FCR**") was prepared. On the basis of the Technical Committee Report, the Appellant-Bank takes a decision as to whether the customer is liable to bear the entire loss arising out of the transaction in

question. In the present case, the recommendation for rejection was approved by the competent authority on 14.07.2021.

2.39 The learned Single Judge did not record any finding as to how the Appellant-Bank had failed to comply with the applicable security guidelines, particularly when, as per the system in place, no withdrawal through an INB transaction can be effected by a third party without the user ID and password. The learned Single Judge further failed to take into account the steps taken by the Appellant-Bank immediately upon receipt of the complaint from Respondent No. 1 and erred in holding that the Appellant-Bank had not acted with urgency, had failed to exercise due care, and had neglected its duty to respond swiftly upon notification of the fraudulent withdrawals.

2.40 The learned Single Judge failed to appreciate that Respondent No. 1 while opting for INB facility had submitted a Form for Online SBI Internet Banking Facility whereby Respondent No. 1 had undertaken that '*I have read and understood the provisions contained in the "Terms of Service (Terms & Conditions) document*" of "*OnlineSBI" and accept them. I agree that the transactions executed over OnlineSBI under my Username and Password will be binding on me*'. Further, under '*Terms of Service (Terms & Conditions) : Online SBI*', it has been categorically stated customer's obligations as under:-

> *"(i) The customer has an obligation to maintain secrecy in regard to Username*
>
> *(ii) & Password registered with the Bank. The bank presupposes that login using valid Username and*

Password is a valid session initiated by none other than the customer.
(iii) Transaction executed through a valid session will be construed by SBI to have emanated from the registered customer and will be binding on him / her.
(iv)The customer will not attempt or permit others to attempt accessing the OnlineSBI through any unlawful means."

Thus, the Appellant-Bank cannot be made liable for any alleged loss caused to Respondent No. 1 through INB transaction.

2.41 The learned Single Judge erred in holding that there is nothing to suggest that Respondent No. 1 shared sensitive financial information and the OTP received on the mobile number registered with the Bank Account and the OTPs received got automatically transmitted to the cyber fraudster who could withdraw the amount from the account of Respondent No. 1. The OTP number cannot be automatically transmitted to the cyber fraudster / third party without the intention of the customer or negligence of the customer. Therefore, the Impugned Judgment deserves to be set aside.

SUBMISSIONS ON BEHALF OF RESPONDENT NO. 1

3. The learned Counsel for Respondent No. 1 made the following submissions:

3.1. Respondent No. 1 is a Professor of Computer Science at GNIOT, Greater Noida. On 18.04.2021, at about 05:15 PM, Respondent No. 1 received an SMS on the mobile number registered with the Bank Account containing a link with the message that, in the event the link was not clicked, the SMS / account service would be

closed. Apprehending disruption of banking services in the prevailing circumstances, Respondent No. 1 clicked upon the said link. Within approximately five minutes thereof, Respondent No. 1 received an SMS from the Appellant-Bank stating that a sum of ₹1,00,000/- had been debited from the Bank Account, together with an intimation that, if the transaction had not been undertaken by him, customer care should be contacted immediately for blocking the account.

3.2. Respondent No. 1 thereupon contacted the Customer Care Number of the Appellant-Bank to report the Subject Transactions. While Respondent No. 1 was still on the call, a further message was received informing him that a sum of ₹1,60,000/- had also been debited from the Bank Account.

3.3. After the unauthorised deduction of an aggregate sum of ₹2,60,000/- from the Bank Account, two OTPs were received by him. According to Respondent No. 1, while it is admitted by the Appellant-Bank that the OTPs were generated and delivered to him, the said OTPs were never shared by him with any person. It is, therefore, contended that the Subject Transactions must have been effected without disclosure of the OTPs, thereby indicating negligence and / or deficiency in service on the part of the Appellant-Bank.

3.4. It is also submitted that, had Respondent No. 1 in fact shared the OTP pertaining to the first transaction and thereafter received the debit message concerning the withdrawal of ₹1,00,000/- from the Bank Account, he would not have disclosed any further OTP in

relation to the subsequent transaction of ₹1,60,000/-. On that basis, it is contended that the Subject Transactions were effected without any sharing of OTPs by Respondent No. 1.

3.5. Respondent No. 1 further submits that he travelled to Noida on 20.04.2021 and, on the same day, lodged a complaint before the Branch Manager of the Appellant-Bank at its Greater Noida Branch seeking restoration of the amount debited from the Bank Account on the ground that the same had occurred due to negligence on the part of the Appellant-Bank. The complaint was, however, rejected by the Appellant-Bank, Greater Noida Branch, on the ground that the transactions had been effected through INB and that the OTPs had been received by Respondent No. 1, though, according to Respondent No. 1, the Appellant-Bank did not state that the OTPs had in fact been shared by him.

3.6. Respondent No. 1 was advised by an official of the Appellant-Bank to lodge an FIR with the concerned police station. Accordingly, on 19.04.2021, Respondent No. 1 approached Industrial Police Station, Paswan Chowk, Hajipur, Vaishali, Bihar, submitted a complaint, and sought registration of an FIR in respect of the unauthorised withdrawals.

3.7. The Impugned Judgment correctly holds that the unauthorised withdrawals of ₹2,60,000/- from the Bank Account occurred on account of failure of the banking security mechanisms and deficiency in service on the part of the Appellant-Bank.

3.8. The learned Single Judge rightly set aside the BO-RBI order dated 20.10.2021, the same having failed to take into account the

material facts and the statutory guidelines governing unauthorised electronic banking transactions.

3.9. The learned Single Judge correctly observed that the Subject Transactions were effected notwithstanding the existence of 2FA; that the banking system maintained by the Appellant-Bank failed to detect suspicious login activity; and that the Appellant-Bank failed to take immediate preventive or remedial measures.

3.10. The banker-customer relationship is both contractual and fiduciary in nature and that the bank owes a corresponding duty of care towards its customer. On that basis, it is contended that the Appellant-Bank was bound to safeguard the interests of Respondent No. 1 in the facts of the present case.

3.11. The allegation of negligence levelled by the Appellant-Bank merely on the basis that Respondent No. 1 clicked upon a malicious link is misconceived. According to Respondent No. 1, modern cyber frauds operate through sophisticated malware capable of accessing data without any voluntary disclosure of OTPs or other credentials. The Appellant-Bank has failed to place any material on record to establish that Respondent No. 1 consciously shared confidential credentials, and that mere generation of OTPs does not, by itself, establish customer authorisation unless it is proved that the customer voluntarily disclosed the same.

3.12. Banks possess superior technological capability and infrastructure to detect suspicious transactions and that the risk arising from technological vulnerabilities cannot be shifted onto customers,

particularly where the fraud occurs within minutes, the customer reports the same immediately, and the bank fails to prevent routing of the transaction. Despite prompt intimation of the fraud, the Appellant-Bank failed to block the beneficiary accounts, initiate chargeback proceedings, or trace the fraudulent transfers. It is, therefore, contended that vulnerabilities in digital banking systems cannot be visited upon an innocent customer and that the Appellant-Bank was obliged to maintain robust fraud detection and prevention mechanisms.

3.13. The technology, by its very nature, is susceptible to vulnerabilities and that online transactions are not immune from compromise. Although the Appellant-Bank may have implemented a secure socket layer connection for online banking purposes, such encryption, according to Respondent No. 1, can still be compromised through various methods, including phishing, trojans, session hijacking and key-logging mechanisms.

3.14. The possibility of hackers obtaining data relating to a banking account while a customer is engaged in an online transaction cannot be ruled out. The bank is in a position to identify fraud risks and devise protective mechanisms, including technologies capable of detecting the location and behaviour of operators. It is, therefore, the responsibility to secure the safety of online banking transactions rests substantially upon the bank.

3.15. The contention of the Appellant-Bank regarding acceptance of the sum of ₹33,340/- is legally untenable. Acceptance of partial compensation pursuant to the BO-RBI directions contained in the

order dated 20.10.2021 cannot extinguish his legal right to seek complete restitution of the allegedly unauthorisedly withdrawn funds.

3.16. The learned Single Judge duly considered the documentary evidence, examined the RBI regulatory framework, and applied the settled legal principles governing the banker-customer fiduciary relationship. On that basis, it is submitted that the Appellant-Bank has failed to demonstrate any legal or factual infirmity in the Impugned Judgment warranting interference in Letters Patent jurisdiction.

3.17. The objection to the maintainability of the Writ Petition was rightly rejected by the learned Single Judge. The Writ Petition was maintainable as the dispute involved alleged violation of statutory RBI guidelines; the BO-RBI order dated 20.10.2021 was vitiated by arbitrariness and non-application of mind; and the matter involved public law elements pertaining to banking regulation and consumer protection. The existence of an alternative remedy does not bar exercise of writ jurisdiction where questions of statutory compliance and fundamental legal principles arise.

3.18. Respondent No. 1 is the victim of a sophisticated cyber fraud and that he acted diligently and promptly upon discovering the same. According to Respondent No. 1, the Appellant-Bank seeks to absolve itself of liability despite the regulatory framework intended to protect customers, thereby undermining consumer protection and public confidence in digital banking systems. In any event, it remains open to the Appellant-Bank to initiate appropriate proceedings against the actual wrongdoers for recovery of the loss,

but Respondent No. 1 ought not to be made to suffer for an alleged systemic failure of the banking mechanism.

3.19. Reliance was placed on ***Tony Enterprises*** (*supra*) to submit that the Appellant-Bank has a remedy by way of filing a civil suit for claiming the loss suffered in the transaction and to recover it from the person responsible.

3.20. The House of Lords in ***London Joint Stock Bank Limited v. Macmillan and Arthur***, 1918 AC 777 has also observed that as the customer and the banker are under a contractual relation, it is obvious that in drawing a cheque the customer is bound to take usual and reasonable precautions to prevent forgery. Crime, is indeed, a very serious matter, but everyone knows that crime is not uncommon. If the cheque is drawn in such a way as to facilitate or almost to invite an increase in the amount by forgery if the cheque should get into the hands of a dishonest person, forgery is not a remote but a very natural consequence of negligence of this description. The learned Lord Chancellor in ***London Joint Stock Bank Limited*** (*supra*) further observed as follows:

> "*Of course the negligence must be in the transaction itself, that is, in the manner in which the cheque is drawn. It would be no defense to the banker, if the forgery had been that of a clerk of a customer, that the latter had taken the clerk into his service without sufficient inquiry as to his character.*"

3.21. Therefore, the present Appeal is misconceived, devoid of merits and liable to be dismissed at the threshold as the learned Single Judge has rightly appreciated the facts, evidence and applicable law while passing the Impugned Judgment.

SUBMISSIONS ON BEHALF OF RESPONDENT NO. 2

4. The learned Counsel for Respondent No. 2 made the following submissions:

4.1. The BO-RBI, by order dated 20.10.2021, observed that Respondent No. 1 had been subjected to vishing and defrauded after clicking upon an unknown link and that, since the Subject Transactions had been effected using the INB credentials and OTPs secured by 2FA, negligence on the part of Respondent No. 1 could not be ruled out.

4.2. The BO-RBI, by order dated 20.10.2021, further observed that the Appellant-Bank had not initiated chargeback proceedings in respect of the transfer of ₹1,00,000/- to the IDFC Bank account and, accordingly, directed the Appellant-Bank to pay Respondent No. 1 one-third of the said amount. It was further observed that, since One97 Communications Ltd. was not covered under the erstwhile Banking Ombudsman Scheme, 2006 ("**BOS 2006**"), the transaction of ₹1,60,000/- in favour of One97 Communications Ltd. was not pursued by the BO-RBI.

4.3. The BO-RBI also recorded that BOS 2006 applied to commercial banks, regional rural banks and scheduled primary co-operative banks, and that One97 Communications Ltd. did not fall within any of the said categories.

4.4. Accordingly, the complaint preferred by Respondent No. 1 was treated as resolved and closed by the BO-RBI on 20.10.2021.

ANALYSIS AND FINDINGS

5. Heard the learned Counsel for the Parties and perused the material placed on record.

6. The principal question that arises for consideration in the present Appeal is whether the learned Single Judge was justified in exercising jurisdiction under Article 226 of the Constitution of India, 1950 ("**Constitution**"), to set aside the order dated 20.10.2021 passed by the BO-RBI and, consequently, to direct the Appellant-Bank to pay Respondent No. 1 a sum of ₹2,60,000/- together with interest at the rate of 9% per annum from 18.04.2021, being the date on which the fraud was reported, on the premise that the Subject Transactions fall within the ambit of "*zero liability*" as contemplated under the 2017 RBI Circular.

7. The material facts, which are largely undisputed, are that Respondent No. 1 admittedly received an SMS containing a link from an unknown source and clicked upon the same. It is equally undisputed that the Subject Transactions were carried out through the INB profile linked to the Bank Account and that the OTPs pertaining thereto were successfully delivered to the mobile number registered with the Bank Account.

8. The learned Single Judge proceeded on the premise that Respondent No. 1 had exercised due caution by not sharing the OTPs and, indeed, had no occasion to do so; and that, if such were the position, it would follow that the 2FA mechanism itself had been breached, thereby indicating deficiency in service on the part of the Appellant-Bank.

9. In our considered opinion, the said approach requires consideration in this Appeal for the following reasons.

9.1. In matters involving digital banking fraud, customer negligence cannot be confined solely to cases of express disclosure of OTPs or passwords. Compromise of such credentials may also occur where a customer interacts with suspicious links or unknown applications, thereby exposing the banking credentials to misuse.

9.2. The 2017 RBI Circular draws a clear distinction between cases involving contributory fraud, negligence or deficiency on the part of the bank and cases where the loss is attributable to negligence on the part of the customer, such as where the customer has shared payment credentials. Clause 6 of the 2017 RBI Circular contemplates "*zero liability*" of the customer where the deficiency lies on the part of the bank or elsewhere in the system, provided the customer notifies the bank of the unauthorised transaction within three working days of receiving the communication regarding such transaction.

9.3. Clause 7(i) of the 2017 RBI Circular, on the other hand, provides that where the loss is occasioned by the negligence of the customer, including by sharing payment credentials, the customer shall bear the entire loss until the unauthorised transaction is reported to the bank.

9.4. Therefore, before liability can be fastened upon the Appellant-Bank, there must exist material indicating a failure of the banking security mechanism or non-compliance with the safeguards prescribed, *inter alia*, under the RBI Circular dated 18.02.2021 titled *Master Direction on Digital Payment Security Controls*, which lays down the necessary guidelines for regulated entities to

establish a robust governance structure and implement minimum standards of security controls for digital payment products and services.

9.5. The expression "*such as where he has shared the payment credentials*" occurring in Clause 7(i) of the 2017 RBI Circular is plainly illustrative and not exhaustive; it does not confine customer negligence only to cases of express disclosure of payment credentials. In the context of digital banking and cyber fraud, negligence may equally arise where a customer, despite repeated advisories and security warnings, accesses suspicious or unknown links, thereby compromising the security of the banking credentials.

9.6. In the present case, Respondent No. 1 admittedly clicked upon a suspicious link received from an unknown person immediately prior to the Subject Transactions. Upon the matter being examined by the INB Department of the Appellant-Bank, it was found that the Subject Transactions were INB transactions secured through 2FA. The BO-RBI, by order dated 20.10.2021, recorded that there had been successful login into the INB profile linked to the Bank Account and that the OTPs were delivered to the mobile number registered with the Bank Account. There is no material presently on record to indicate that the Subject Transactions bypassed the authentication process prescribed by the Appellant-Bank or that there was any established compromise of the banking system of the Appellant-Bank.

9.7. In these circumstances, the learned Single Judge, in exercise of writ jurisdiction, was not justified in presuming deficiency on the part of the Appellant-Bank and in consequently fastening liability upon it.

10. The order dated 20.10.2021 passed by BO-RBI has examined the beneficiary details of the Subject Transactions, including the Merchant Code, RRN No., IP Address and transaction records furnished by the Appellant-Bank, to arrive at the conclusion that the Subject Transactions had been effected through INB and had been rendered possible only after successful login into the INB profile linked to the Bank Account by use of the user ID and password, without any direct intervention on the part of the Appellant-Bank.

11. The BO-RBI, by order dated 20.10.2021, also observed that the Appellant-Bank had failed to initiate chargeback proceedings in respect of the transfer of ₹1,00,000/- made to the IDFC Bank account and, consequently, directed the Appellant-Bank to pay one-third of the said amount to Respondent No. 1. The Appellant-Bank has admittedly complied with the said direction.

12. The learned Single Judge, however, held that, since Respondent No. 1 had denied sharing the OTPs, the liability would necessarily fall upon the Appellant-Bank. Such an interpretation dilutes the operation of Clause 7(i) of the 2017 RBI Circular and the distinction contemplated therein between different categories of unauthorised transactions.

13. The observations in the Impugned Judgment to the effect that Respondent No. 1 "*cannot be said to be negligent in any manner*" and that the Subject Transactions occurred solely on account of deficiency

attributable to the Appellant-Bank are, in our opinion, ordinarily could not have been returned in the absence of any technical or forensic examination and are, moreover, not in consonance with the framework contemplated under the 2017 RBI Circular.

14. It is also material to note that, immediately upon receipt of intimation regarding the Subject Transactions, the Appellant-Bank blocked the INB profile linked to the Bank Account, and no further unauthorised transaction took place after the incident was reported by Respondent No. 1.

15. While exercising jurisdiction under Article 226 of the Constitution, this Court must confine its enquiry to whether the action of the Appellant-Bank suffers from manifest arbitrariness, procedural infirmity, or non-compliance with the framework contemplated under the 2017 RBI Circular.

16. The issues considered by the learned Single Judge, particularly whether the user ID and password of the INB profile linked to the Bank Account or the OTPs were compromised following interaction with a suspicious link received from an unknown source; whether negligence was attributable to Respondent No. 1; whether security protocols such as 2FA or OTP verification had been breached by malware deployed by cyber fraudsters; and whether the security apparatus of the Appellant-Bank failed to detect unusual login activity from a different Internet Protocol Address allegedly used by the fraudsters, are matters that necessarily require technical and forensic examination and adjudication on evidence and could not have been conclusively determined in exercise of writ jurisdiction.

17. The reliance placed by Respondent No. 1 on ***Tony Enterprises*** (*supra*) is not helpful to Respondent No. 1. In ***Tony Enterprises*** (*supra*), the transactions in question were treated as "*prima facie tainted by fraud*" on the

basis of a police investigation establishing SIM swapping and identity theft through fraudulently procured duplicate SIM cards, which were used to access the bank account of the petitioner therein and to effect unauthorised transfers by generating OTPs through such duplicate SIM cards, thereby bringing the transactions within the category of "*disputed transactions*" falling within the sweep of zero liability under the 2017 RBI Circular. In the present case, no such investigative finding has, till date, emerged to establish that the Subject Transactions were carried out through any breach of the Appellant-Bank's system.

18. The observations in ***Tony Enterprises*** (*supra*) to the effect that the bank has a remedy by way of a civil suit to recover the loss suffered in the transaction from the person responsible were rendered in the peculiar facts of that case and cannot be construed to mean that, in every case of an unauthorised electronic banking transaction, the bank must first compensate the customer irrespective of the nature of the transaction or the applicability of the framework under the 2017 RBI Circular. The observations in ***Tony Enterprises*** (*supra*), rendered in the context of a *prima facie* established fraud supported by police investigation, therefore cannot be extended to the facts of the present case.

19. In view of the aforesaid discussion, the present Appeal is allowed, and the Impugned Judgment is set aside.

20. The present Appeal, along with all pending application, stand disposed of in the aforesaid terms.

TEJAS KARIA, J

DEVENDRA KUMAR UPADHYAYA, CJ

MAY 29, 2026/'sms'