



BEFORE THE ADJUDICATING OFFICER

SECRETARY, ELECTRONICS, INFORMATION TECHNOLOGY &
ARTIFICIAL INTELLIGENCE DEPARTMENT,
MANTRALAYA, MUMBAI, MAHARASHTRA.

UNDER THE INFORMATION TECHNOLOGY ACT, 2000

IN

COMPLAINT CASE NUMBER 18 OF 2015

.....
No. DIT-6515/ 1037800/ C.R.-66/ (18/2015)/39 (E-1769359) Reserved on: 06.08.2026

Pronounced on: (Date of Digital Signature)

IN THE MATTER OF,

M/s G.D. Apte & Co.

) ... Complainant

Versus

Bank of India

) ... Respondent No. 1

Idea Cellular Limited

) ... Respondent No. 2

Beneficiary Banks

) ... Respondent No. 3 to 14

Unknown Persons

) ... Respondent No. 15

Appearances:

Adv. Prashant Mali, Mr. Prakash Kulkarni o/b/o. Complainant;

Adv. Pavan K. Barhule, Mr. Suhas Kulkarni o/b/o. Respondent No. 1, Bank of India;

Adv. Mihir Tambe, Adv. Yash Arora i/b. Bharucha and Partners, o/b/o. Respondents No. 2, Idea Cellular Limited (now Vodafone Idea Limited);

Adv. Viswanath Mannadiar, o/b/o. Respondent No. 3, ICICI Bank Limited;

Adv. Devendra Mahadik i/b. Marathe Associates, o/b/o. Respondent No. 4, HDFC Bank Limited;

Adv. Rahul Karnik, Respondent No. 5, Kotak Mahindra Bank Limited;

Adv. R. J. Singh, Respondent No. 6, Central Bank of India, were present

[This document presents the proceedings of a complaint filed by the Complainant for adjudication under Section 46 of The Information Technology Act, 2000 (as amended in 2008) (referred to as the "Act"). The hearings were conducted in accordance with the principles of natural justice and reasonable opportunity, ensuring that both parties, namely the Complainant and the Respondents, were given equal and sufficient opportunities to present and defend their respective cases. After the conclusion of the hearings and the receipt of responses from all parties involved, a decision has been reached, and this order is now being delivered.]

I. THE BRIEF FACTS OF THE CASE, AS STATED BY THE COMPLAINANT, ARE AS FOLLOWS:

1. The present Complaint has been instituted by **M/s. G.D. Apte & Co.**, a partnership firm stated to have been established in the year 1958 and engaged in professional activities including statutory audit, internal audit, taxation and allied services. The

Complainant states that, for approximately ten years preceding the incident in question, it maintained two accounts with **Respondent No. 1 – Bank of India**, Jangli Maharaj Road Branch, Pune, namely **Current Account No. 051820110000041** and **Overdraft Account No. 051827110000015**. The Complainant has approached this Authority alleging, inter alia, failure on the part of the concerned Respondents to adopt and maintain reasonable security practices in relation to its electronic banking facility, resulting in unauthorized access to its banking accounts and consequent unauthorized electronic fund transfers. The Complainant has invoked, inter alia, the provisions of **Sections 43, 43A and 85 of the Information Technology Act, 2000**. The original complaint was presented before this Authority under the Information Technology Act, 2000.

2. It is the specific case of the Complainant that the internet banking facility was not **generally enabled for both the aforesaid accounts**. According to the Complainant, the internet banking facility was specifically opted for in respect of its Current Account No. **051820110000041**, pursuant to a specific resolution duly executed by its partners and submitted to Respondent No. 1 along with the prescribed application for availing internet banking facilities. The Complainant states that the said specific instructions and resolution were initially submitted to Respondent No. 1 on **10 December 2010** and were thereafter submitted/reaffirmed on **13 April 2013**. According to the Complainant, the documents expressly restricted the internet banking facility to the Current Account and did not extend such facility to the **Overdraft Account No. 051827110000015**. The Complainant consequently alleges that any operation of the Overdraft Account through internet banking was outside the authority and mandate furnished by it to Respondent No. 1.
3. Learned Counsel appearing on behalf of the Complainant Mr. Prashant Mali states that it had adopted specific internal security and authorization controls for operation of its internet banking facility. According to the Complainant, the workflow prescribed by it contemplated a **maker-checker mechanism**, under which transactions were to be initiated by the designated accountant/user having lower-level privileges and were thereafter required to be authorized by **any two out of the three partners** having higher-level privileges. Thus, according to the Complainant, a valid transaction required participation of distinct users at the initiation and authorization stages. The Complainant asserts that these controls were consciously incorporated as

an internal safeguard and were intended to prevent unauthorized access or unilateral operation of its banking accounts.

4. The immediate genesis of the dispute, according to the Complainant, lies in an incident concerning mobile number **9011028076**, belonging to/used by Mr. Prakash P. Kulkarni, which was registered with Respondent No. 1 for receipt of SMS alerts and authentication-related communications in connection with the internet banking facility. The Complainant states that it was a Corporate User Group (CUG) customer of **Idea Cellular Ltd.**, with post-paid mobile connections for its partners and employees, and that the aforesaid mobile number was being used for receiving banking alerts and One-Time Passwords (OTPs).
5. According to the Complainant, on **10 March 2015 at approximately 4:30 p.m.**, the said mobile number suddenly became non-functional for both incoming and outgoing communication, although neither Mr. Prakash P. Kulkarni nor any authorized person of the Complainant had requested that the number be barred. Shortly thereafter, at approximately **4:37 p.m.**, a system-generated communication was received stating that a request for barring the mobile number had been successfully processed. The Complainant states that it immediately contacted the customer service centre of **Respondent No. 2 – Idea Cellular Ltd.** and categorically informed the service provider that no such request had been made by the Complainant and that an unauthorized third party might be attempting to misuse the mobile connection. The Complainant further states that it was informed that a complaint regarding loss of the handset/SIM card had been received. The Complainant expressly denied having made any such complaint and informed the service provider that the SIM card had not been lost.
6. Learned Counsel for the Complainant states that, following its communication with Idea Cellular, the mobile number was released at approximately **5:41 p.m.** on 10 March 2015 and a message confirming unbarring of the SIM/mobile number was received. According to the Complainant, it consequently formed a bona fide belief that the alleged unauthorized request had been rejected and that the mobile connection had been restored to its legitimate status. The Complainant further states that, on the following day, i.e. **11 March 2015 at approximately 11:00 a.m.**, the problem of non-functioning of the SIM/mobile connection again arose. Upon contacting the customer service centre, the Complainant states that it was informed that the SIM card might have been damaged and required replacement. Acting upon that representation,

- the Complainant approached the franchisee of Respondent No. 2 and applied for replacement of the SIM card. The connection was thereafter restored on the same day.
7. The Complainant subsequently came to know that, notwithstanding the aforesaid circumstances, a **substitute/duplicate SIM card had allegedly been issued on 10 March 2015 to an unauthorized third party**. The Complainant states that this fact was discovered from the records/logs obtained from the concerned telecom service provider. It is the Complainant's case that the duplicate SIM was issued without any request or authorization from the Complainant and without proper verification of the identity and authority of the person seeking such replacement. The Complainant particularly alleges that this occurred despite the earlier communication to the service provider that the original SIM had not been lost and that an unauthorized person might be attempting to interfere with the mobile connection. The Complainant attributes considerable significance to the duplicate SIM because the registered mobile number was used for receipt of banking alerts and OTPs.
 8. The Complainant states that, on **11 March 2015 at approximately 10:30 a.m.**, its accountant, **Ms. Gauri Joshi**, while checking the balance of the Current Account in the ordinary course, noticed an unusual transaction. An amount of **₹6,60,000/-** had been transferred through RTGS in favour of **Garden Gift Agro Pvt. Ltd.** The accountant immediately brought the transaction to the notice of the partners, who confirmed that the Complainant had neither initiated nor authorized the said transaction. The Complainant states that its representatives immediately contacted the Branch Manager of Respondent No. 1 by telephone and reported the unauthorized RTGS transaction, requesting appropriate action to prevent further unauthorized operations. The Complainant also states that an email was sent to Respondent No. 1 informing it of the unauthorized transaction and requesting immediate credit/reversal of the amount.
 9. Learned Counsel submitted that, at approximately **12:00 noon on 11 March 2015**, its accountant received a telephone call from an official of Respondent No. 1 concerning insufficiency of balance in the Current Account for honouring certain cheques issued by the Complainant. Thereafter, at approximately **3:15 p.m.**, the Complainant deposited **Cheque No. 520626 for ₹2,00,000/-** into its Current Account, the cheque being drawn on its Overdraft Account. The Complainant alleges that the said cheque was not posted by the Bank and that no adequate communication was furnished to it regarding such non-posting and the reasons therefor. Subsequently, at approximately

5:00 p.m., while examining the Overdraft Account to verify the aforesaid transfer of ₹2,00,000/-, the accountant discovered that **12 further RTGS transactions aggregating ₹78,93,000/-** had been effected from the Overdraft Account in favour of various beneficiary accounts situated at different locations.

10. Thus, according to the Complainant, on **11 March 2015**, a total of **13 unauthorized RTGS transactions** were effected from its two accounts: **one transaction of ₹6,60,000/- from the Current Account and twelve transactions aggregating ₹78,93,000/- from the Overdraft Account**, resulting in an aggregate disputed amount of **₹85,53,000/-**. The Complainant maintains that none of these transactions had been initiated, authorized or otherwise instructed by it or its authorized partners/users. It further states that no OTP had been received by it on the registered mobile number in respect of any of the disputed transactions. The Complainant asserts that the disputed transactions occurred during the period in which the registered mobile connection was non-functional and that the funds were thereafter transferred to various third-party beneficiary accounts maintained with different banks and branches across India.
11. Upon discovering the transactions from the Overdraft Account, the Complainant states that it immediately contacted Respondent No. 1 by telephone and informed the Branch Manager of the unauthorized debits. The Complainant further states that two of its partners, along with its accountant, personally attended the branch between approximately **5:30 p.m. and 6:00 p.m.** on the same day and submitted separate written communications in respect of the Current Account and the Overdraft Account, informing the Bank of the unauthorized RTGS transactions and requesting that the amounts be credited back to the respective accounts. The Complainant also states that, on the same day, it approached the police authorities and lodged a **First Information Report with Deccan Gymkhana Police Station, Pune**, in relation to the alleged cyber-fraud and unauthorized transactions.
12. The Complainant further relies upon the manner in which the disputed transactions were allegedly processed through its internet banking credentials and workflow. It asserts that, according to the Bank's own communication dated **12 March 2015**, the disputed RTGS transactions were shown as having been initiated through the user ID associated with Mr. Prakash Kulkarni and authorized by Mr. C. M. Dixit. The Complainant, however, categorically denies that either of them actually initiated or authorized the disputed transactions. In the alternative, and without prejudice to its

primary contention, the Complainant submits that even if the Bank's system records were accepted at face value, the transactions did not conform to the workflow specifically prescribed by the Complainant, since the stipulated combination of one initiator and two separate authorizers was not followed. The Complainant therefore alleges that Respondent No. 1 ought to have detected and rejected the transactions as being inconsistent with the mandate and security parameters prescribed for operation of the account.

13. The Complainant additionally states that it had prescribed a **user-wise RTGS transaction limit of ₹50,00,000/- as the maximum cumulative debit limit in a month**. According to the Complainant, notwithstanding this expressly stipulated limit, RTGS transactions aggregating **₹78,93,000/-** were permitted from the Overdraft Account on a single day. The Complainant relies upon this circumstance as an additional indication that the disputed transactions were materially inconsistent with its established transaction profile and prescribed banking controls. It alleges that Respondent No. 1 ought to have subjected such transactions to appropriate scrutiny, alerts and verification, particularly in view of their unusual velocity, aggregate value and departure from the Complainant's normal transaction pattern.
14. The Complainant also alleges that, after the first unauthorized transaction of ₹6,60,000/- from the Current Account had been brought to the notice of Respondent No. 1, the Bank ought to have exercised enhanced vigilance in relation to the Complainant's other accounts and ought to have examined whether any further unauthorized activity had occurred. According to the Complainant, the subsequent discovery of **12 additional RTGS transactions aggregating ₹78,93,000/- from the Overdraft Account** demonstrated that the earlier alert did not result in adequate protective intervention. The Complainant has further alleged that the Bank failed to employ appropriate real-time fraud analytics, velocity checks and other security mechanisms contemplated under the regulatory framework governing electronic payment transactions.
15. In relation to Respondent No. 2, the Complainant alleges that the unauthorized issuance of the duplicate/substitute SIM constituted a critical link in the chain of events leading to the disputed electronic transactions. According to the Complainant, the telecom service provider ought to have undertaken appropriate verification of the person seeking replacement of the SIM, including verification against the subscriber's records, authorization, identity particulars and other relevant information. The

Complainant contends that, in the circumstances existing on 10 and 11 March 2015, the issuance of the substitute SIM enabled an unauthorized person to receive or intercept banking-related communications, including OTPs and transaction alerts, and thereby facilitated the subsequent unauthorized electronic fund transfers. The Complainant consequently attributes liability to Respondent No. 2 for what it describes as failure to exercise reasonable care and security in relation to the SIM replacement process.

16. The Complainant further states that the disputed funds were transferred to beneficiary accounts maintained with various banks, impleaded as Respondent Nos. 3 to 14, and that one beneficiary account was subsequently identified in connection with the transaction of ₹6,60,000/-. The complaint contains details of the beneficiary accounts and the amounts transferred thereto. According to the Complainant, the beneficiary banks were required to maintain appropriate KYC records and transaction-monitoring mechanisms and, upon receiving information concerning the fraudulent nature of the transactions, were required to take appropriate steps to prevent withdrawal or dissipation of the funds. The Complainant also alleged that the beneficiary accounts and the persons operating them ought to be examined for compliance with applicable banking and KYC requirements.
17. The Complainant states that, following its immediate intimation regarding the Current Account transaction, the amount of ₹6,60,000/- transferred to the beneficiary account of Garden Gift Agro Pvt. Ltd. was frozen by the concerned banking system pursuant to the instructions/alert raised by the Complainant. The complaint accordingly sought, at the initial stage, release of the frozen amount. The Complainant, however, maintained that the remaining disputed amount had resulted in actual financial loss and that the Respondents were liable to compensate it for the loss and consequential hardship caused by the unauthorized electronic transactions.
18. The Complainant has relied upon various regulatory and contractual safeguards, including the **Banking Codes and Standards Board of India (BCSBI) Code of Bank's Commitment to Customers**, the **Reserve Bank of India's RTGS Systems Regulations, 2013**, and the RBI's circular dated **28 February 2013** concerning security and risk-mitigation measures for electronic payment transactions. In particular, the Complainant contends that the applicable regulatory framework contemplated due diligence by the originating member, maker-checker authentication, transaction monitoring and appropriate mechanisms for identifying suspicious or

unusual transactions. It is the Complainant's case that the nature, velocity and aggregate value of the disputed RTGS transactions were sufficiently unusual to warrant intervention or enhanced verification by Respondent No. 1.

19. The Complainant further alleges that the unauthorized transfers caused not merely direct monetary loss but also consequential prejudice to its business operations, working capital position and reputation. It states that the depletion of funds from its Current and Overdraft Accounts adversely affected its ability to conduct its ordinary business and honour its financial commitments. The Complainant has also alleged that the incident resulted in considerable hardship, harassment, mental agony and reputational injury, particularly in view of the alleged publicity surrounding the incident. It therefore sought compensation beyond the principal amount of the disputed transactions.
20. The Complainant states that it addressed communications and complaints to the concerned Respondents and that Respondent No. 1, by communication dated **12 March 2015**, denied responsibility and attributed the incident to alleged compromise/disclosure of user credentials. The Complainant disputes such attribution and maintains that it had exercised due care in relation to its banking credentials and had not shared its password or authorized the disputed transactions. According to the Complainant, the Respondents failed to provide a satisfactory resolution of the grievance, compelling it to invoke the jurisdiction of this Authority under the Information Technology Act, 2000. The Complainant accordingly prayed for appropriate compensation and other consequential reliefs in respect of the alleged contraventions. As set out in its Written Arguments, the Complainant quantified the **disputed amount at ₹64,44,123/-** (Rupees Sixty-Four Lakh Forty-Four Thousand One Hundred and Twenty-Three Only), with the **overall contingent financial liability stated to be ₹76,73,100/-** (Rupees Seventy-Six Lakh Seventy-Three Thousand One Hundred Only), besides interest and costs, as prayed for in the Complaint.

II. SUBMISSIONS AND DEFENSES OF RESPONDENT NO. 1 - BANK OF INDIA :

1. Respondent No. 1 – **Bank of India, Jangli Maharaj Road Branch, Pune**, has disputed the allegations made by the Complainant and has denied any liability in respect of the disputed electronic transactions. The substantive response of

Respondent No. 1 is contained in its communication dated **12 March 2015**, marked in the record as **Annexure 6** (scanned compilation, pp. 43–44). The Bank contended that, upon examination of the transactions at its end, it found no involvement or fault attributable to the Bank and that the transactions had been carried out through the Internet Banking facility purportedly by the authorized/regular users of the Complainant.

2. Respondent No. 1 contended that the disputed **transactions were processed through the maker-checker mechanism** using the relevant login credentials and transaction passwords and were further validated through OTPs sent to **Mobile No. 9011028076** registered with the Bank. On this basis, the Bank contended that the transactions had passed its prescribed authentication process and that no deficiency in its security mechanism could be attributed to it.
3. The Bank further raised the possibility that the **login IDs, login passwords and transaction passwords** of the authorized users of the Complainant may have been shared, revealed or otherwise compromised. It accordingly suggested that an internal inquiry/investigation ought to be undertaken by the Complainant into the manner in which its Internet Banking credentials were allegedly compromised. Thus, the Bank's defence, in substance, was that the available authentication records pointed towards use of valid credentials and authentication factors and that the possibility of compromise of such credentials at the customer/user end could not be ruled out.
4. The Bank further contended that, according to the Complainant's own communication, the disputed transactions had taken place between approximately **9:33 a.m. and 10:15 a.m. on 11 March 2015**. It submitted that, upon logging into the Internet Banking facility, the account balance would ordinarily be displayed on the screen and that the unusual depletion of funds could therefore have been noticed at the earliest stage. The Bank consequently alleged that the Complainant had not promptly informed the Bank and that immediate intimation could have enabled the Bank to take steps for freezing the concerned accounts and thereby mitigating the loss. The Bank specifically referred to the fact that the Complainant's report was received by it only at approximately **6:45 p.m. on 11 March 2015**, by which time, according to the Bank, substantial amounts had already been withdrawn by the beneficiaries.
5. The Bank also sought information from the Complainant as to whether the **STARTOKEN facility** offered by the Bank had been used by its employees/users for Internet Banking transactions. The Bank stated that the STARTOKEN facility

provided an additional authentication/security mechanism for Internet Banking and, by implication, sought to suggest that the availability or non-use of such an additional security facility was a relevant circumstance in determining responsibility for the disputed transactions.

6. At the same time, the Bank stated that, upon receiving information regarding the alleged fraud, it had taken steps to approach the concerned beneficiary banks and requested them to **freeze the available balances in the beneficiary accounts and prevent further withdrawals**. The Bank further stated that it had initiated steps for calling back/recovering the funds transferred through the disputed transactions. It also informed the Complainant that, since the matter was under investigation by the police authorities, the Bank would revert to the Complainant upon further developments.
7. In essence, therefore, the defence of Respondent No. 1 is that the disputed transactions were authenticated through the Bank's prescribed Internet Banking security mechanism, including the **maker-checker process, login credentials, transaction passwords and OTP authentication**; that the possibility of compromise or disclosure of the credentials at the Complainant's/user's end could not be excluded; that the Complainant did not report the transactions to the Bank with sufficient promptness; and that the Bank, upon receiving the complaint, took steps to freeze the beneficiary accounts and seek recovery of the transferred funds. The Bank consequently denied that the disputed transactions were attributable to any failure or deficiency in the security measures maintained by it.

III. SUBMISSIONS AND DEFENSES OF RESPONDENT NO. 2 – IDEA CELLULAR LIMITED. (now VODAFONE IDEA LIMITED):

1. Respondent No. 2, formerly known as **Idea Cellular Limited and now known as Vodafone Idea Limited**, has filed an Affidavit in Reply through its constituted attorney, Ms. Mohana Manjre, disputing the allegations made against it. Respondent No. 2 has denied the allegations in the Complaint and has contended that the Complaint is misconceived, devoid of merit and liable to be dismissed.
2. Respondent No. 2 submitted that the Complainant was **a Corporate User Group ("CUG") subscriber and that Mr. Dhananjay Chinchwadkar**, partner of the Complainant, was the user of Mobile No. **+91 9011028076**. It stated that the said

mobile number had originally been issued on 24.12.2009 after obtaining the requisite Customer Application Form and verification of the identity and address documents. The Customer Application Form and connected documents have been relied upon as **Exhibit 'A' to the Affidavit in Reply.**

3. Respondent No. 2 further submitted that on 10.03.2015 at about 4.37 p.m., a person claiming to be an authorised representative of the Complainant contacted its customer-care service and **requested disconnection of the mobile number on the ground that the SIM card had been misplaced.** According to Respondent No. 2, an SMS acknowledging the request was sent to the mobile number and it was informed that the request could be acted upon only upon the authorised representative visiting its store and completing the requisite formalities. Thereafter, at about 5.40 p.m. on the same day, another representative contacted customer care and informed Respondent No. 2 that the earlier request for disconnection was not required and should not be acted upon. The said communication was duly noted by Respondent No. 2.
4. Respondent No. 2 submitted that at about 7.55 p.m. on 10.03.2015, Mr. Dinesh V. Chinchwadkar, claiming to be an authorised representative of the Complainant, visited its franchise store at S.B. Communications, Pune, and **requested issuance of a replacement SIM card.** He allegedly produced a signed request on the Complainant's letterhead, a self-attested Aadhaar Card and a SIM replacement form stating that the earlier SIM card had been misplaced. Respondent No. 2 submitted that the documents were verified by the store representative and that the replacement SIM was issued and activated only thereafter. The relevant documents are relied upon as **Exhibits 'B' and 'C' to the Affidavit in Reply.**
5. Respondent No. 2 submitted that the person who obtained the replacement SIM had **fraudulently represented himself as an authorised representative** of the Complainant and that Respondent No. 2 itself was a victim of such impersonation/fraud. It further submitted that on 11.03.2015 at about 11.00 a.m., the Complainant approached Respondent No. 2 for issuance of another SIM card and, after verification of the relevant documents, the same was issued. Subsequently, when the Complainant suspected misuse of the mobile number and requested blocking thereof, Respondent No. 2 stated that the mobile number was promptly blocked.
6. Respondent No. 2 further submitted that, **at the relevant time, there were no specific guidelines prescribing the precise procedure for subscriber verification** in cases of duplicate SIM issuance. In the absence of specific directions from the

Department of Telecommunications (“DoT”) or the Telecom Regulatory Authority of India (“TRAI”), it claimed to have adopted reasonable security measures. Reliance was placed upon the order dated 12.04.2012 of the **TDSAT in Cellular Operators Association of India & Ors. v. Department of Telecommunication & Anr.**, annexed as Annexure ‘A’ to the Written Arguments, particularly in relation to the liability of a telecom operator where a third party obtains a connection by using forged documents.

7. Respondent No. 2 submitted that the alleged fraudulent banking transactions could not have been effected merely by obtaining a replacement SIM, as Internet Banking transactions require other confidential credentials, including login ID, password and transaction password. It contended that it neither stores nor has access to the Complainant's banking credentials, account details or transaction passwords and, therefore, any compromise of such confidential information could only have occurred at the end of the Complainant or Respondent No. 1–Bank. It further submitted that the Complainant also received banking-related communications through its registered email address.
8. Respondent No. 2 specifically disputed the applicability of Section 43A of the Information Technology Act, 2000. It submitted that Section 43A applies where a body corporate possesses, handles or deals with sensitive personal data or information in a computer resource under its control and is negligent in maintaining reasonable security practices. According to Respondent No. 2, being a Telecom Service Provider, it did not possess or handle the Complainant's banking credentials or other sensitive financial information and merely provided telecom connectivity for transmission of communications. It therefore contended that no liability under Section 43A could arise against it.
9. Respondent No. 2 also relied upon **Section 79 of the Information Technology Act, 2000**, and submitted that it acted merely as an intermediary in transmitting communications such as SMS/OTP messages. It contended that it did not initiate, select the recipient of, or modify the information contained in such transmission and, therefore, claimed exemption from liability as an intermediary.
10. Respondent No. 2 further submitted that it was not responsible for indefinite retention of historical log records. In this regard, it relied upon the DoT communication dated 21.12.2021, annexed as Annexure ‘B’ to the Written Arguments, concerning retention

of logs, and contended that no adverse inference could be drawn against it merely on account of non-availability of historical records.

11. Respondent No. 2 submitted that there was no proximate nexus between the alleged SIM replacement and the fraudulent banking transactions. It contended that the disputed transactions were undertaken through the Internet Banking facility of Respondent No. 1 and that Respondent No. 2 had neither access to nor control over the Complainant's bank accounts or banking credentials. It further relied upon the investigation by the police authorities and submitted that no liability had been established against it in respect of the alleged fraudulent transactions.
12. Respondent No. 2 further contended that the liability, if any, in respect of unauthorised electronic banking transactions primarily falls for consideration against the concerned banks under the applicable RBI framework. Reliance was placed upon the RBI circulars/guidelines and other documents annexed as Annexures 'C' to 'G' to the Written Arguments, including the provisions relating to customer protection and unauthorised electronic banking transactions. It was submitted that even assuming, without admitting, any deficiency in processing the SIM replacement, such act was too remote to constitute the proximate cause of the alleged loss.
13. Respondent No. 2 also raised an objection regarding jurisdiction. It submitted that subscriber verification and issuance of SIM cards are governed by the telecom regulatory framework, including the **Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933 and the TRAI Act, 1997**, and by directions issued by the DoT. It therefore contended that any alleged non-compliance with subscriber-verification requirements would fall within the domain of the DoT/TDSAT and not within the jurisdiction of the Adjudicating Officer under Section 46 of the Information Technology Act. Reliance was placed upon the judgments cited in its Written Arguments, including **Avishek Goenka v. Union of India & Ors.**
14. Finally, Respondent No. 2 submitted that the Complainant had failed to establish any negligence on its part or any violation of Section 43A of the Information Technology Act. It reiterated that **it had verified the documents presented for replacement of the SIM and had complied with the applicable security requirements, network-security conditions and ISO 27001 standards.** It therefore submitted that no liability for the alleged financial loss could be fastened upon Respondent No. 2 and prayed for dismissal of the Complaint against it.

IV. SUBMISSIONS OF RESPONDENT NOS. 3 TO 14 – BENEFICIARY BANKS AUTHORITY

1. Respondent Nos. 3 to 14 are the banks/branches in whose accounts the disputed RTGS amounts were credited. From the record, it appears that **ICICI Bank**, through Respondent Nos. 3, 5, 10 and 12, filed a written statement in response to the Complaint. The remaining beneficiary banks have primarily been represented in the record through correspondence, account-opening/KYC documents, transaction statements and other documents placed before this Authority.
2. The beneficiary banks, insofar as their respective records are concerned, have essentially relied upon the fact that the disputed amounts were received in the beneficiary accounts through RTGS transactions originating from the Complainant's accounts maintained with Respondent No. 1. The transaction details placed on record show that the amounts were credited to different beneficiary accounts maintained with different banks and at different locations. The Complaint records 12 such transactions from the Overdraft Account, aggregating **₹78,93,000/-**.
3. On the basis of the submissions and documents on record, the beneficiary banks have sought dismissal of the Complaint against them, contending that there is no material on record establishing that they participated in, authorised or facilitated the initiation of the disputed RTGS transactions from the Complainant's accounts or that they were negligent in the maintenance of the beneficiary accounts.

V. ISSUES & FINDINGS OF THE AUTHORITY

1. Upon consideration of the pleadings, documents and material placed on record, the principal issue for determination is whether the unauthorised SIM replacement and the subsequent RTGS transactions resulted from failure of Respondent Nos. 1 and 2 to maintain reasonable security practices and procedures. The record shows that the Complainant's registered mobile number became non-functional on **10.03.2015**, followed by the disputed banking transactions on **11.03.2015**. The Complainant immediately disputed the transactions and called upon the concerned Respondents to take necessary action, as evidenced by **Annexures 1, 2 and 3**.
2. Insofar as Respondent No. 2 is concerned, the material on record shows that a **duplicate SIM was issued in respect of the registered mobile number**, though the Complainant disputed having authorised such replacement. The documents relied upon by the Complainant disclose that the request for replacement was required to be

verified with reference to the subscriber's particulars and authority. The Authority finds that the request and the accompanying documents, including the **letterhead and stamp**, were not adequately cross-verified before issuance of the duplicate SIM. Consequently, Respondent No. 2 failed to exercise the requisite care in permitting a change in the mobile connection which formed part of the authentication mechanism of the Complainant's banking facility.

3. As regards Respondent No. 1, the **Corporate Internet Banking application and the specific resolution forming part of Annexure 5** prescribe the user hierarchy and the maker-checker mechanism. The transaction workflow required initiation by the lower-level user (H2) and authorisation by any two of the three higher-level users (2H1). The same document also records the transaction limits applicable to the users. The Authority therefore finds that these were not merely procedural requirements, but constituted the security controls agreed upon for operation of the Complainant's account.
4. The Bank's own letter dated **12.03.2015**, marked **Annexure 6**, records that the disputed transactions were validated through OTP sent to the registered mobile number and also refers to the maker-checker process. However, when the said document is read with the requirements contained in **Annexure 5**, the record does not establish compliance with the prescribed **H2 + 2H1 authorisation workflow** in respect of the disputed transactions. Further, the disputed RTGS transactions from the Overdraft Account aggregated **₹78,93,000/-**, whereas the transaction limit prescribed in the material relied upon by the Complainant was **₹50,00,000/- per month**. The account statement corroborates the disputed debits.
5. The Authority therefore finds that the two failures occurred at distinct but connected stages of the electronic authentication chain, wherein failure of Respondent No. 2 to adequately verify and authenticate the request for duplicate SIM resulted in loss of effective control over the registered mobile connection, while Respondent No. 1 failed to ensure compliance with the prescribed maker-checker mechanism and transaction-limit controls. The disputed transactions, comprising **₹6,60,000/- from the Current Account and ₹78,93,000/- from the Overdraft Account**, were thereafter immediately disputed by the Complainant through **Annexures 2 and 3**, and the FIR was lodged as **Annexure 4**.
6. In view of the aforesaid documentary evidence and findings, the Authority holds that the acts and omissions of **Respondent Nos. 1 and 2 constitute failure to maintain**

reasonable security practices and procedures, resulting in the unauthorised transactions and consequential loss suffered by the Complainant. The liability of Respondent Nos. 1 and 2 is, accordingly, attracted **under Section 43A of the Information Technology Act, 2000**.

In light of the aforementioned findings, in my considered view, the unauthorised transactions were effected **through the Internet Banking facility maintained and administered by Respondent No. 1**, notwithstanding the specific security architecture agreed with the Complainant under **Annexure 5**, which required the prescribed **H2 + 2H1 maker-checker authorisation** and prescribed a cumulative transaction limit of **₹50,00,000/- per month**. The Bank's own communication dated **12.03.2015**, marked **Annexure 6**, establishes that the disputed transactions were processed through the said Internet Banking facility and were sought to be justified on the basis of OTP, login credentials and maker-checker authentication. However, the record does not establish compliance with the prescribed H2 + 2H1 workflow, nor does it satisfactorily explain how transactions aggregating **₹78,93,000/-**, in excess of the stipulated limit, were permitted to pass through the system. Respondent No. 1, being the entity in control of the relevant banking infrastructure and security controls, must therefore bear the **primary and direct liability for the financial loss resulting from the unauthorised transactions**.

At the same time, the role of Respondent No. 2 cannot be disregarded. The documentary record establishes that the mobile number registered with the Bank became non-functional immediately before the disputed transactions and that a **duplicate SIM was issued upon a request which, according to the Complainant, was unauthorised**. The material placed before the Authority and arguments of the learned council does not satisfactorily demonstrate that Respondent No. 2 adequately verified the authority of the person seeking the duplicate SIM or properly cross-checked the particulars appearing on the request, including the **letterhead and stamp**, before permitting replacement of the SIM. Since the registered mobile number formed part of the authentication mechanism relied upon by Respondent No. 1, this omission materially contributed to the compromise of the security chain. Nevertheless, Respondent No. 2 did not initiate or process the disputed banking transactions and its liability is therefore **contributory and distinct from the primary financial liability of Respondent No. 1**.

The Authority therefore holds that the respective failures of **Respondent Nos. 1 and 2** were **distinct in their nature but interconnected in their effect**, and both materially contributed to the occurrence of the unauthorised electronic transactions. Respondent No. 1, having failed to effectively enforce the prescribed banking authorisation and transaction-limit controls, is liable for the financial loss established in the proceedings, whereas Respondent No. 2 is liable for the security lapse attributable to the SIM replacement process. The respective liability is accordingly determined under Section 43A of the Information Technology Act, 2000, having regard to the nature, extent and evidentiary basis of the individual lapses established against each Respondent.

ORDER

- a) In view of the findings recorded hereinabove, **Respondent No. 1 – Bank of India** is hereby directed to pay to the Complainant a sum of **₹64,44,123/-** (Rupees Sixty-Four Lakh Forty-Four Thousand One Hundred and Twenty-Three Only), being the principal loss established and determined in the present proceedings, together with interest thereon at the rate of **12% per annum**, calculated from the date of contravention until the date of actual payment.
- b) **Respondent No. 2 – Idea Cellular Limited (now Vodafone Idea Limited)** is hereby directed to pay to the Complainant a sum of **₹5,00,000/-** (Rupees Five Lakh Only) as compensation, having regard to the failure established against it in relation to the verification and issuance of the duplicate SIM and its material contribution to the compromise of the authentication channel, as recorded in the findings hereinabove.
- c) The amounts directed to be paid under clauses (a) and (b) above shall be paid to the Complainant within a period of 30 (Thirty) days from the date of this Order.

The order is passed on the date of digital signature, at Mantralaya, Mumbai.

Digitally signed by
VIRENDRA SINGH
Date: 07-09-2026
06:10:04

(Virendra Singh)

Secretary, Electronics, Information Technology
& Artificial Intelligence Department,
Mantralaya, Mumbai – 400 032.