



BEFORE THE ADJUDICATING OFFICER

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

UNDER THE INFORMATION TECHNOLOGY ACT, 2000

IN

COMPLAINT CASE NUMBER 05 OF 2020

.....
No. DIT- 2020/C.R. 41/ (05/2020)/S- 2/39/ (E- 1641916)

Reserved on: 26.08.2026

Pronounced on: (Date of Digital Signature)

IN THE MATTER OF,

The Kolhapur Urban Co-Operative Bank Limited) ... Complainant

Versus

HDFC Bank Limited & Others) ... Respondent

Appearances:

Adv. Samadhan Patil, Mr. Harishchandra Gat o/b/o. Complainant;

Adv. Partha Pati, Adv. Janhavi Jadhav i/b. Abhay Nevagi & Associates o/b/o. Respondent

No. 1, HDFC Bank Limited,

Mr. Atish Mhetre, Police Sub- Inspector i/b. Inspector of Police, Shahupuri Police Station, Kolhapur, were present.

[This Complaint has been filed under Section 46 of the Information Technology Act, 2000 (Hereinafter 'Act'), invoking Sections 43(a), 43(g) and 43A thereof. The parties were heard at length over the course of the enquiry. Pleadings, documents, affidavits, a computer forensics report, the report of the investigating agency and written submissions were taken on record. Both sides were afforded full and equal opportunity to lead material, to meet the case of the other, and to address this Authority on facts and law, consistent with the requirements of natural justice and the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003. The matter was reserved for orders on 26.08.2026. This Order is pronounced on the date of its digital signature.]

I. FACTS OF THE CASE

1. The Complainant is a primary urban co- operative bank at Kolhapur. It held two accounts with Respondent No. 1 and operated them through Respondent No. 1's internet banking platform, E- Net, for two purposes and two only - RTGS and NEFT. On 19.04.2019, which was Good Friday and a bank holiday, thirty- four transactions were put

through those two accounts in a single day. Every one of them was an **IMPS** transaction. The Complainant says it had never subscribed to IMPS, had never performed an IMPS transaction on that platform in seven years, and was not present in its own premises on the day. ₹67,88,041/- left its accounts.

2. The question in this Complaint is therefore a narrow one, and it is not whether a fraud occurred - that much is common ground. It is whether a bank which provides an electronic payment platform to another bank discharges its obligation under Section 43A of the Act when that platform processes thirty- four transactions, on a banking holiday, through a channel the customer never subscribed to, to beneficiaries never before transacted with, from network addresses the customer had never used, without generating a single alert, block, or additional verification at any point in the sequence.

II. POINTS FOR DETERMINATION

3. Upon consideration of the pleadings, the documents and the submissions, the following points arise for determination and are answered as indicated. The reasons follow in Part XII

Sr. No.	Point	Finding
(i)	<i>Whether this Authority has jurisdiction to entertain and adjudicate this Complaint.</i>	Affirmative
(ii)	<i>Whether the thirty- four transactions effected on 19.04.2019 from Account Nos. 01640380000253 and 01640380000305 were authorised by the Complainant.</i>	Negative. They were unauthorised.
(iii)	<i>Whether the IMPS channel, through which every one of the disputed transactions was routed, had been subscribed to by, or authorised by, the Complainant.</i>	Negative
(iv)	<i>Whether Respondent No. 1 was, on 19.04.2019, a body corporate possessing, dealing with or handling sensitive personal data or information in a computer resource owned, controlled or operated by it, within Section 43A of the Act.</i>	Affirmative
(v)	<i>Whether Respondent No. 1 was negligent in implementing and maintaining reasonable security practices and procedures in relation to that computer resource.</i>	Affirmative
(vi)	<i>Whether such negligence caused wrongful loss to the Complainant, and in what sum.</i>	Affirmative. ₹65,98,041/-
(vii)	<i>Whether any part of the loss is attributable to the act or omission of the Complainant.</i>	Negative

Sr. No.	Point	Finding
(viii)	<i>What final order ought to be passed in the present Complaint?</i>	<i>As in Part XV</i>

III. SUBMISSIONS OF THE COMPLAINANT

4. The Complainant, The Kolhapur Urban Co- operative Bank Ltd., is a society registered under the Maharashtra Co- operative Societies Act, 1960 and a banking company within the meaning of the Banking Regulation Act, 1949, holding RBI Licence No. UBD MH 686/P/29/86, with its registered office at 514, 'D' Ward, Gangawesh, Kolhapur – 416002.
5. Respondent No. 1, HDFC Bank Ltd., is a company incorporated under the Companies Act, 1956 and a banking company within the Banking Regulation Act, 1949, with its registered office at Senapati Bapat Marg, Lower Parel, Mumbai – 400013, and a branch at Shahupuri, Kolhapur.
6. Respondent Nos. 2 to 11 are the banks with which the beneficiary accounts were maintained - Canara Bank, Bank of Baroda, Union Bank of India, Punjab National Bank, Central Bank of India, ICICI Bank, Kotak Mahindra Bank, Oriental Bank of Commerce, Federal Bank and Allahabad Bank. Respondent Nos. 12 to 18 are the individual account-holders into whose accounts the disputed funds were credited - Durjan Ramsay Bhokta, Sarojbai Dhurelal Dhakad, Khomdram Jecky, Dharmendra Sudarshan Prasad Pandey, Salim Shabrati Shaikh, Isak Ansari alias Munna and Dhurelal Daulatramji Dhakad.
7. The documents which define the relationship are four, and it is necessary to be exact about what each one covers:
 - (a) **Exhibit "K"** - the E- Net Agreement, undated and stamped 27.06.2012, for Corporate Internet Banking Service, expressly for NEFT and RTGS.
 - (b) **Exhibit "J"** - Agreement dated 13.09.2012 between the Complainant and Respondent No. 1 for sub- membership to the Centralised Payment Systems of the Reserve Bank of India
 - (c) **Exhibit "L"** - Application dated 17.02.2017 by the Complainant to avail of online RTGS and NEFT facility, as detailed in the payment options of that application.
 - (d) **Exhibit "N"** - documents relating to settlement Account No. 01640380000305, a settlement account used for settling IMPS, POS, ATM and NACH services which the Complainant availed from NPCI directly, and not from Respondent No. 1.
8. Not one of these four instruments provides for the Complainant availing an IMPS facility from Respondent No. 1. That is a matter of the documents, not of assertion, and it is the foundation of the finding at Point (iii) below.

IV. FACTS NOT IN DISPUTE

9. The following are either admitted or are not in contest, and the Complaint may be approached on this footing:

(a) The two accounts in question were maintained by the Complainant with Respondent No. 1.

(b) On 19.04.2019, twenty- eight transactions aggregating ₹55,98,041/- were debited from Account No. 01640380000253, and six transactions aggregating ₹11,90,000/- were debited from Account No. 01640380000305 - thirty- four in all, aggregating ₹67,88,041/.

(c) Every one of the thirty- four was an IMPS transaction, executed through E- Net. This is not the Complainant's assertion. It is Respondent No. 1's own statement at the time of Argument and also in w.r.t. RBI Holiday list of 2019 in its letter dated 25.04.2019 (Exhibit "E"), by which it furnished details of the operation of the accounts on 19.04.2019 and of the thirty- four reported transactions.

(d) 19.04.2019 was Good Friday and a bank holiday.

(e) The funds were credited to accounts maintained with Respondent Nos. 2 to 11 in the names of Respondent Nos. 12 to 18.

(f) ₹1,90,000/- has been recovered. ₹65,98,041/- has not.

(g) The transactions were disputed by the Complainant to Respondent No. 1 on 20.04.2019 (Exhibit "C"), application filled to the police the same day (Exhibit "D"), and an FIR bearing No. 0254 of 2019 was registered at Shahupuri Police Station, Kolhapur on 21.04.2019 (Exhibit "P").

V. THE CASE OF THE COMPLAINANT

The Complainant's case, shorn of repetition, is this.

10. Complainant stated that, they subscribed to RTGS and NEFT. It never subscribed to IMPS from Respondent No. 1, never gave permission for IMPS to be enabled on either account, and has not to date carried out a single IMPS transaction with Respondent No. 1. A properly configured system ought to have declined an IMPS request originating on its profile, because IMPS was not a service it had subscribed for. In the case of the settlement account, the position is stronger still a settlement account should never process a customer- generated IMPS request at all.
11. IMPS transactions on the platform required neither digital certificate authorisation nor maker- checker authorisation. The security measures Respondent No. 1 relies upon were therefore not engaged by the very transactions which caused the loss. Separately, the digital signature certificate issued to the Complainant was not fully secure, being capable of being copied from the machines on which it was installed.
12. On the day of the incident, the three designated computers at the Complainant's premises were switched off. CCTV recordings show that bank personnel were not present. It was a bank holiday. The IP addresses from which the disputed transactions were initiated are different from the Complainant's external IP addresses.

13. Respondent No. 1's own IP logs show (i) suspicious login attempts on 02, 16 and 18 April 2019, undetected; (ii) login and access from two different IP addresses in two different cities at the same time on 02.04.2019, undetected; and (iii) access at 20:01 hours on 18.04.2019, after banking hours, undetected.
14. When the IMPS transactions were permitted, Respondent No. 1 sent no intimation to the registered email address or telephone number when beneficiaries were added; sent no OTP to the registered email address or telephone number; and raised no alert although the transactions were initiated from irregular MAC identifiers and an irregular browser. It has not disclosed where any OTP was sent, or to which number, or whether it tallied with the credentials furnished by the Complainant.
15. The Complainant availed sub- membership relying on Respondent No. 1's representation that E- Net was a fully secured, internet- based, real- time electronic delivery channel, and that Respondent No. 1 had deployed the strongest security measures for digital payment transactions in the country. Respondent No. 1 being in a dominant position and in full control of E- Net, it was for Respondent No. 1 to configure the system - to track IP addresses and MAC identifiers from which transactions would be initiated, to track the browsers used, to confine transactions to business hours, to cap transaction values and beneficiary numbers, to limit beneficiaries addable in a day, to alert on beneficiary addition, to run velocity checks, to detect cyber intrusions promptly, and to maintain a robust monitoring process for unusual activity patterns. It was equally for Respondent No. 1 to inform and educate the Complainant of any security measure it expected the Complainant to observe.
16. Respondent No. 1 furnished no information regarding the security controls and risk-management framework by which its E- Net system was capable of detecting unauthorised or irregular transactions.
17. The Complainant accordingly alleges failure by Respondent Nos. 1 to 11 to implement reasonable security practices and to exercise due diligence under the Act and the RBI directions, and unauthorised access to and debiting of its accounts by Respondent Nos. 12 to 18. It seeks compensation.

VI. THE CASE OF RESPONDENT NO. 1

18. Learned Advocate Mr. Partha Pati for Respondent No. 1 denies negligence and denies any failure to maintain reasonable security practices. Its case may be stated under six heads.
19. The rights and obligations of the parties were governed by the Agreement for Sub-Membership to the Centralised Payment Systems of the Reserve Bank of India. The Complainant was duly onboarded and the requisite applications, user details, access rights and transaction permissions were duly provided and configured.
20. IMPS was available as part of "other payment services". Respondent No. 1 relied in this regard on a Board Resolution of the Complainant.

21. The system incorporated multiple layers - User ID and password, digital certificate, encryption and other access controls - and transactions were required to pass through the prescribed authentication process. The disputed transactions did so.
22. Respondent No. 1 relies on its ISO 27001 certification, PCI- DSS compliance, periodic internal and external audits, information- security policies, privilege- based access controls, and continuous monitoring through Security Information and Event Management (SIEM).
23. The contractual framework placed responsibility for the confidentiality and safe custody of User IDs, passwords and digital certificates upon the Complainant, and the Complainant's own systems, configuration, access arrangements, cyber- security controls, fraud- monitoring and application- to- application authentication were relevant to the enquiry. The learned counsel for Respondent No.1 further stated that,
24. The Complainant never communicated its static public IP addresses to Respondent No. 1 by a separate letter, and furnished IP details for the first time on 20.08.2019.
25. It contends that the mere occurrence of unauthorised transactions does not establish deficiency in its systems, that the identity and conduct of the person who actually used the credentials requires examination, and that the Complaint against it be dismissed.
26. The R2 to R1 are the beneficiary basic where the funds are credited and 12 to 18 the AC holders.

VII. PROCEDURAL HISTORY

27. The Complaint was presented in 2020. It came up for preliminary hearing on 16.12.2021, when the Complainant appeared through Adv. Vaishali Bhagwat and Respondent No. 1 through Adv. Partha Pati and Mr. Ashutosh Marathe. Three weeks were granted to Respondent No. 1 to file its reply.
28. On 03.02.2022, Respondent No. 1 filed limited affidavit in reply.
29. On **25.06.2026**, after hearing both sides, this Authority put four specific questions to Respondent No. 1, set out at paragraph 56 below. The Atish Mhatre (Police Sub-Inspector) from Shahupuri Police Station, Kolhapur, was present and the progress report of the Police Inspector (No. 6909/2026 dated 24.06.2026) was taken on record.
30. On **16.07.2026**, arguments were advanced by Respondent No. 1. The Roznama records that the questions put on 25.06.2026 had not been satisfactorily answered by Respondent No.1. Further opportunity was granted to obtain instructions.
31. On **06.08.2026**, Respondent No. 1 tendered a reply to the queries. The Roznama records that satisfactory answers to the questions posed at the earlier hearings had not been furnished, and that the question of **IP whitelisting** remained. The Complainant was directed to place further material on that question, and did so by its submission dated 11.08.2026, verified on affidavit by Shri. Harishchandra Sudhakar Gat and notarised the same day. The final written submission of Respondent No. 1 was filed beyond the time granted; it has nonetheless been read and taken into consideration in the interest of justice.
32. The matter was reserved on 26.08.2026.

VIII. THE MATERIAL ON RECORD

33. The findings which follow rest on the following material, all of which forms part of the record:

- (a) Statements of account of the two accounts - **Exhibits "A" and "B"**;
- (b) The Complainant's letter to Respondent No. 1 dated 20.04.2019 - **Exhibit "C"**;
- (c) Application to the Police Inspector, Shahupuri Police Station dated 20.04.2019 - **Exhibit "D"**; FIR No. 0254 dated 21.04.2019 - **Exhibit "P"**;
- (d) Respondent No. 1's letter dated 25.04.2019 with log details - **Exhibit "E"**;
- (e) The Complainant's letter dated 16.05.2019 - **Exhibit "F"**; Respondent No. 1's reply dated 27.05.2019 - **Exhibit "G"**;
- (f) Letter from the Police dated 15.07.2020 - **Exhibit "H"**;
- (g) Letter from the Reserve Bank of India dated 12.02.2019 - **Exhibit "I"**;
- (h) The four instruments at paragraph 7 - **Exhibits "J", "K", "L" and "N"**; sample RTGS/NEFT form - **Exhibit "M"**; UAT sign- off and Go- Live letter dated 17.01.2018 to NPCI - **Exhibit "O"**;
- (i) Correspondence with the regulator and CERT- In: letter dated 22.04.2019 to the Principal Chief General Manager, RBI - **Exhibit "R"**; intimation to the cyber security cell of the RBI dated 30.04.2019 - **Exhibit "S"**; email dated 16.05.2019 to CERT- In - **Exhibit "T"**;
- (j) **Computer Forensics Report - Exhibit "V"**;
- (k) Email dated 03.05.2019 from Respondent No. 1 regarding additional enhancement of the E- Net set- up - **Exhibit "W"**;
- (l) Letter from Maharashtra Cyber - **Exhibit "X"**; the Complainant's letter dated 27.05.2019 to Maharashtra Cyber - **Exhibit "Y"**; Interim report dated 15.10.2019 - **Exhibit "Z"**;
- (m) The progress report of the Police Inspector, Shahupuri Police Station (No. 6909/2026 dated 24.06.2026), and the oral submission of the Mr. Atish Mhetre, Police Sub- Inspector, Shahupuri Police Station recorded on 25.06.2026;
- (n) The Complainant's submission dated 11.08.2026 on static public IP addresses, on affidavit, with Annexure A (emails dated 12.10.2017 and 12.04.2018 to 16.04.2018 to NPCI/NACH with the NACH Access Request Form) and Annexure B (RBI Circular dated 22.04.2025 on domain migration);
- (o) The account- opening and KYC documents produced by Respondent No. 1, including Board Resolution No. 10(9)/2012- 13 dated 01.01.2013.

IX. THE LEGAL FRAMEWORK

34. Section 43A of the Act provides that where a body corporate, possessing, dealing with or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures, and thereby causes wrongful loss or wrongful gain to

any person, it shall be liable to pay damages by way of compensation. Section 43(a) and 43(g) provide for liability where a person, without permission of the owner or person in charge of a computer resource, accesses it, or provides assistance to any person to facilitate access in contravention of the Act. Section 46 confers the power of adjudication; Section 46(1A) fixes the pecuniary limit at ₹5 crore; Section 46(5) vests the powers of a civil court. Section 47 prescribes the factors governing quantum.

35. Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 enumerates what constitutes sensitive personal data or information, and includes **password** and **financial information such as bank account details**. Rule 8 defines reasonable security practices and procedures. It is necessary to be precise about what Rule 8 requires: a documented security programme and policies containing managerial, technical, operational and physical security control measures commensurate with the information being protected; IS/ISO/IEC 27001 is a recognised standard; and, critically, the standard must be **certified or audited on a regular basis by an independent auditor duly approved by the Central Government, such audit being carried out at least once a year or as and when the body corporate undertakes significant upgradation of its process and computer resource**. Rule 8 further provides that the body corporate seeking to rely on such practices must be able to demonstrate that it has implemented them.

36. **The regulatory framework in force on 19.04.2019 -**

a. RBI Circular DPSS(CO)PD.1462/02.14.003/2012- 13 dated 28.02.2013, issued under Section 18 of the Payment and Settlement Systems Act, 2007 and addressed to scheduled commercial banks and urban co- operative banks alike, directs the securing of electronic payment transactions.

b. RBI Circular DBS.CO.ITC.BC.No.6/31.02.008/2010- 11 dated 29.04.2011, implementing the recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, and the Cyber Security Framework in Banks, DBS.CO/CSITE/BC.11/33.01.001/2015- 16 dated 02.06.2016, prescribe the standard of care expected. These directions were in force and applicable to Respondent No. 1 on 19.04.2019, the date of the incident, and it is that standard, not the position as it may stand today, by which Respondent No. 1's conduct on that date falls to be judged.

X. FINDINGS

Point (i) - Jurisdiction

37. The Complainant's accounts were maintained with a branch of Respondent No. 1 within the State of Maharashtra, and the electronic banking facility was availed and operated from Kolhapur. The claim as finally pressed is ₹65,98,041/- , well within the limit of ₹5 crore under Section 46(1A). The Complaint is founded on Sections 43 and 43A, matters expressly assigned to the Adjudicating Officer by Section 46(1). By Section 46(5) this Authority is vested with the powers of a civil court for the purposes of the enquiry. The objection to jurisdiction raised on behalf of Respondent No. 1 by its

affidavit in reply dated 03.02.2022 was considered and does not survive scrutiny for the reasons recorded above; Section 46(1) expressly assigns matters under Sections 43 and 43A to the Adjudicating Officer, and Section 61 of the Act ousts the jurisdiction of the civil court in respect of such matters. **Point (i) is answered in the affirmative.**

Point (ii) - Were the transactions authorised by Complainant?

38. The Complainant has denied authorisation from the first moment and has never wavered. The denial is not a litigation posture adopted after reflection; it is documented in real time. On **20.04.2019** it wrote to Respondent No. 1 (Exhibit "C") and asked for the debit transactions in both accounts to be frozen. On the **same day** it applied to the Police Inspector, Shahupuri Police Station (Exhibit "D"). On **21.04.2019** FIR No. 0254 of 2019 was registered (Exhibit "P"). On **22.04.2019** it wrote to the Principal Chief General Manager of the Reserve Bank of India (Exhibit "R"); on **30.04.2019** it intimated the cyber security cell of the RBI (Exhibit "S"); on **16.05.2019** it informed CERT- In (Exhibit "T").
39. A party which has fabricated a dispute does not, within seventy- two hours, lay the matter before its own regulator, the national computer emergency response team and the police. The contemporaneity, the consistency and the sheer breadth of the reporting are themselves evidence of the genuineness of the denial.
40. To that is added the material on where the Complainant's officers were. The three designated computers at its premises were switched off. CCTV recordings show that its personnel were not present. The day was a bank holiday. And the Police Representative stated before this Authority on 25.06.2026 that the IP addresses from which the disputed transactions were carried out were **not located in Kolhapur**, whereas the concerned Maker and Checker **were present in Kolhapur City** on the date of the incident.
41. Respondent No. 1 offers nothing against this beyond the proposition that the system accepted the credentials. That proposition is addressed at Point (v) and does not survive. The standard of proof in these proceedings is the preponderance of probabilities (*Dr. N.G. Dastane v. S. Dastane*, (1975) 2 SCC 326), and it is amply met. **Point (ii) is answered in the negative: the thirty- four transactions were unauthorised.**

Point (iii) - Was IMPS ever subscribed to or authorised?

42. This is the point on which this Complaint principally turns, and it can be decided on the evidence on record.
43. Every one of the thirty- four disputed transactions was an IMPS transaction. That is not the Complainant's characterization. It is Respondent No. 1's own, stated in its letter of 25.04.2019 (Exhibit "E"), by which it furnished details of the operation of the accounts on 19.04.2019 and confirmed that the transactions were executed through E- Net using the IMPS mode.
44. The instruments between the parties have been set out at paragraph 7. The E- Net Agreement (Exhibit "K") is for **NEFT and RTGS**. The application of 17.02.2017 (Exhibit "L") is to avail **online RTGS and NEFT**. The sub- membership agreement (Exhibit "J") concerns the Centralised Payment Systems of the Reserve Bank. The settlement account (Exhibit "N") existed to settle IMPS, POS, ATM and NACH services

which the Complainant took **from NPCI directly**. None of them enables an IMPS facility from Respondent No. 1 to the Complainant. The Complainant asserts, and Respondent No. 1 has not controverted with any record of its own, that in the entire period of the relationship it never once performed an IMPS transaction on the E- Net platform. If that is so - and Respondent No. 1's transaction logs would settle it conclusively - then the first IMPS transaction ever performed on this profile was the fraud, and the thirty- fourth was too.

45. Respondent No. 1's answer is that IMPS was available as one of the "other payment services", relying on a Board Resolution of the Complainant. That answer fails twice over.
46. *First*, when the question was put at the hearing of 16.12.2021 whether the Board Resolution formed part of the Agreement, the answer given on behalf of Respondent No. 1 was that **it did not**; the expression relied upon was described as a residuary word. A residuary expression in an agreement which nowhere mentions IMPS cannot be the vehicle by which an entire payment channel is brought into existence on a customer's profile.
47. *Second*, and more fundamentally, the Board Resolution is on this record. Board Resolution No. 10(9)/2012- 13, passed on 01.01.2013, records the Chairman informing the Board of the proposal to avail the **ATM Sponsor Bank facility**, and resolves that consent be given to open and operate a current account with HDFC Bank Ltd. **for ATM Sponsor Bank facility**. It authorises four named officials to execute the necessary facility documents and to operate the account jointly. It says nothing whatever about IMPS. Respondent No. 1 has thus produced, from its own files, the very instrument which refutes the defence it built upon it.
48. It follows that IMPS was enabled on the Complainant's two accounts without any mandate from the Complainant. In the case of Account No. 01640380000305 the position is worse: that was a settlement account, and a settlement account has no business processing a customer- generated IMPS instruction at all. A banker may debit its customer's account only in accordance with the customer's mandate, and where a debit is made otherwise, the loss falls on the banker (*Canara Bank v. Canara Sales Corporation*, (1987) 2 SCC 666). **Point (iii) is answered in the negative.**

Point (iv) - **Are the ingredients of Section 43A made out?**

49. Before negligence is reached, the statutory threshold must be established, and this Authority is conscious that it is a threshold on which appellate scrutiny has fastened. In *ICICI Bank Ltd. v. Saurabh Ravi Shankar Jain*, 2019 SCC Online TDSAT 3480, the Hon'ble Tribunal held that the jurisdiction under Section 43A read with Section 46 is confined to a body corporate possessing, dealing with or handling sensitive personal data or information in a computer resource which it owns, controls or operates, and to negligence by such body corporate in implementing and maintaining reasonable security practices within Section 43A read with Rule 8 of the 2011 Rules. Each ingredient is therefore examined separately.

50. Respondent No. 1 is a banking company incorporated under the Companies Act. It falls squarely within the Explanation to Section 43A. This is not in dispute.
51. E- Net is Respondent No. 1's platform. Respondent No. 1's own defence - that it deployed digital certificates, privilege- based access controls and SIEM monitoring across that platform - is itself an assertion of ownership and control. A party cannot claim the benefit of controls it administers while disclaiming the resource on which they run.
52. This requires precision, because the account- holder here is itself a body corporate. The credentials through which E- Net was accessed were the User IDs, passwords and digital certificates issued to the Complainant's designated Maker and Checker - **natural persons**, identified on the platform as 'TIWARE KOUCBK' and 'SHILPA KOUCBK'. "Password" is expressly enumerated in Rule 3 of the 2011 Rules, and financial information such as bank account details is enumerated alongside it. Respondent No. 1 possessed, dealt with and handled that information within its computer resource for the purpose of authenticating every transaction on the Complainant's accounts. That the account- holder is a co- operative bank does not alter the character of the credentials of the individuals authorised to operate the account, nor of the financial information held in respect of those accounts. **Point (iv) is answered in the affirmative.**

Point (v) - Negligence in maintaining reasonable security practices

53. Respondent No. 1's defence rests on two pillars: certification, and successful authentication. Neither bears the weight placed on it.
54. Rule 8 does not equate certification with compliance. It requires that the practices be implemented in fact, that the body corporate be able to **demonstrate** implementation, and that the standard be audited by a Central Government- approved independent auditor at least annually and on every significant upgradation of the process or computer resource. A certificate establishes that a framework was documented. It does not establish that the particular control which ought to have interdicted thirty- four IMPS transfers on a bank holiday was configured and operating on 19.04.2019. Respondent No. 1 has produced no audit report, no control- testing record, and no alert log referable to these transactions.
55. Authentication and authorisation are not the same thing. Authentication establishes that a system accepted credentials; authorisation establishes that the account- holder gave the mandate. Where the very allegation is that the credentials were compromised, proof of successful authentication proves the point in issue only by assuming it. But in this case the argument has a further and fatal difficulty. On the Complainant's case, which Respondent No. 1 has not met with any record of its own, **IMPS transactions on this platform required neither digital certificate authorisation nor maker- checker authorisation.** If that is so, then the two controls Respondent No. 1 principally relies upon were not engaged by the transactions which caused the loss. A bank cannot defend a breach by pointing to safeguards which the breach bypassed.
56. In the course of the hearings this Authority put to Respondent No. 1 specific questions on matters lying exclusively within its knowledge, possession and technical control:
- Why the registered contact particulars of the Complainant had not been updated in its records

- b. Why no alert was generated or escalated although access and transactions originated from IP addresses situated in cities other than the Complainant's place of operation
 - c. The nature and content of the emails referred to in the Maharashtra Cyber report, stated to have been sent and thereafter deleted
 - d. Whether IP whitelisting was configured on the Complainant's E- Net profile, and on what parameters
57. These were not peripheral questions. Each went to whether a control existed, and if it existed, why it did not operate. Respondent No. 1 was granted three successive opportunities - 25.06.2026, 16.07.2026 and 06.08.2026 - and its written submission, though filed out of time, was received and read. The material was not furnished.
58. The E- Net access logs, authentication records, source IP data, MAC identifiers, browser signatures, alert configuration and SIEM output are within the exclusive knowledge and possession of Respondent No. 1 within Section 109 of Bhartiya Sakshya Adhiniyam, 2023 and are the best evidence on precisely the questions in issue. Where a party in possession of the best evidence withholds it, an adverse inference may be drawn notwithstanding the burden of proof. This Authority draws that inference and holds that, had the records been produced, they would not have supported the case that effective alerting, anomaly detection and access control were in operation on 19.04.2019.
59. **The specific failures.** Setting aside the adverse inference and confining attention to what is affirmatively on the record, the following failures are established:
- (a) **An unsubscribed channel was enabled.** IMPS was operative on two accounts for which no IMPS mandate existed (Point (iii)). A system properly configured to the services actually subscribed for would have declined the very first request.
 - (b) **A settlement account processed a customer- initiated IMPS instruction.** Account No. 01640380000305 existed to settle obligations with NPCI. Six customer- type IMPS debits on such an account ought to have been structurally impossible.
 - (c) **Anomalous access went undetected across three weeks.** Respondent No. 1's own logs record suspicious login attempts on 02, 16 and 18 April 2019; simultaneous login from two different IP addresses in two different cities on 02.04.2019; and access at 20:01 hours, after banking hours, on 18.04.2019. Simultaneous authenticated sessions from two cities is not a subtle signal requiring sophisticated analytics. It is a physical impossibility for a single set of credentials, and any functioning monitoring system flags it.
 - (d) **No alert of any kind was raised.** No intimation on beneficiary addition; no OTP to the registered email or telephone; no transaction alert; no alert on the irregular MAC identifiers or the irregular browser. Respondent No. 1 has not disclosed to what number or address any OTP was sent, or whether it tallied with the credentials on its record. The Hon'ble Tribunal has held in *Manvir Singh v. ICICI Bank Ltd., Cyber Appeal No. 10 of 2020* decided 04.08.2026, that failure to issue alerts in respect of fraudulent transactions is a failure of the security practices imposed on banks by the RBI through its circulars, sounding in Section 43A.

(e) **No velocity or value control operated.** Thirty- four transfers aggregating ₹67,88,041/- were permitted to pass in sequence on a single day, to beneficiaries not previously transacted with. The securing of electronic payment transactions directed by RBI Circular DPSS (CO) PD.1462/02.14.003/2012- 13 dated 28.02.2013 contemplates precisely such caps, beneficiary limits, beneficiary- addition alerts and velocity checks.

(f) IMPS operates around the clock, and this Authority does not suggest that the holiday made the transactions technically impossible. That is not the point. The point is that thirty- four high- value transfers from a co- operative bank's corporate accounts, on Good Friday, through a channel never before used on that profile, constitute a transaction pattern which departs from the customer's established profile in every measurable respect at once. The function of anomaly detection is to notice exactly that.

(g) **Contact particulars were not maintained.** The failure to keep registered contact details current is not a clerical matter. It is the failure of the link by which any alert, had one been generated, would have reached the customer.

60. Respondent No. 1's contention is that the Complainant never communicated its static public IP addresses by separate letter and furnished them for the first time on 20.08.2019. On the material placed on affidavit on 11.08.2026, the following emerges. The Complainant held two static public IP addresses - **117.218.170.63** and **203.192.231.88** - for its head office internet connectivity, and had communicated them to NPCI/NACH by email as early as 12.10.2017 and again in April 2018, with the NACH Access Request Form recording the public IP range. That is contemporaneous documentary evidence, generated well before the incident and for an unrelated purpose, that these were the addresses from which the Complainant's traffic originated.
61. But the whitelisting contention is, with respect, beside the point, and it is important to say why. The Complainant's answer - that at the relevant time the E- Net registration form contained no field in which a static IP address could be declared, and that such a field was added only on 20.08.2019 as a subsequent security precaution which Respondent No. 1 accepted - is itself telling. If the platform provided no means of declaring an IP address for whitelisting, the absence of a declaration cannot be laid at the customer's door; and if IP- based access control was a control Respondent No. 1 considered necessary, the absence of any mechanism to configure it was Respondent No. 1's deficiency, not the Complainant's default. A service provider cannot fail to offer a control and then rely upon the customer's failure to invoke it.
62. In any event, the question was never whether a letter was written. The question is from which IP addresses the disputed transactions were actually initiated - and the answer to that lies in Respondent No. 1's own E- Net audit logs, which record the source IP of every transaction, genuine and disputed alike. A comparison of the source IPs of the Complainant's successful transactions before the incident with those of the thirty- four disputed transactions would have settled the matter objectively in a single exercise. Respondent No. 1 has not produced that comparison. The Maharashtra Cyber Police and the forensic auditor have recorded that the source IP addresses appearing in the fraudulent transactions do not belong to the Complainant, and the Police sub- inspector stated before this Authority that those IP addresses were not located in Kolhapur.

63. Two entries on the record are of significance, and this Authority relies on them for a limited purpose only. On **02.05.2019**, within a fortnight of the incident, Respondent No. 1 took steps to issue a more secure digital signature certificate with tokens, and on **03.05.2019** it wrote regarding additional enhancement of the E- Net set- up (Exhibit "W"). This Authority does not treat remedial action as an admission of liability; a prudent institution improves its systems after an incident and should not be discouraged from doing so. The limited and legitimate inference is as to **feasibility**: the enhancements adopted within a fortnight were available to be adopted before, and their adoption immediately afterwards indicates that the pre- existing configuration was capable of improvement in exactly the respects in which it had just failed.
64. Taking the record as a whole - the enabling of an unsubscribed channel, the processing of customer IMPS instructions on a settlement account, the bypassing of the digital certificate and maker- checker controls, three weeks of undetected anomalous access including physically impossible concurrent sessions, the complete absence of alerts, the absence of velocity and value controls, the failure to maintain contact particulars, the absence of any mechanism by which IP whitelisting could be configured, and the failure to produce the logs which alone could have answered any of it - this Authority holds that Respondent No. 1 was negligent in implementing and maintaining reasonable security practices and procedures in relation to the computer resource it owned, controlled and operated. **Point (v) is answered in the affirmative.**

Point (vi) - **Wrongful loss and causation**

65. The nexus is direct and requires little elaboration. The unauthorised transactions were initiated on, authenticated by, and processed through the computer resource of Respondent No. 1. Every control which might have interdicted them was either absent, unconfigured or inoperative. The funds left the Complainant's accounts and were credited to accounts held by Respondent Nos. 12 to 18 with Respondent Nos. 2 to 11. The loss is the direct and proximate consequence of the negligence found at Point (v). The quantum is dealt with below under 'Quantum'. **Point (vi) is answered in the affirmative.**

Point (vii) - **Contributory negligence**

66. This Authority has considered of its own motion whether any part of the loss is attributable to the Complainant, because a finding under Section 43A does not absolve a customer of its own obligations of custody and care.
67. Four circumstances are decisive against such a finding.
- i. The three designated computers at the Complainant's premises were switched off on the day of the incident, and CCTV recordings show that its personnel were not present. (As per Mr. Atish Mhetre, Police Sub- Inspector, Shahupuri Police Station, Kolhapur stated on record)
 - ii. The originating IP addresses were not located in Kolhapur, whereas the Maker and the Checker were present in Kolhapur City. (As per Mr. Atish Mhetre, Police Sub- Inspector, Shahupuri Police Station, Kolhapur stated on record)

iii. The Complainant detected the debits, reported them to Respondent No. 1, applied to the police, and thereafter informed the Reserve Bank and CERT- In, all within days.

iv. And most significantly, the channel through which the money left was one the Complainant had never subscribed to and had no means of controlling; a customer cannot be expected to guard a door it did not know existed and could not have closed.

68. Nor can the Complainant be faulted for the custody of credentials on the footing that credentials were accepted. On the material discussed at paragraph 55, the IMPS channel did not require the digital certificate or maker- checker authorisation at all. Beyond the assertion that its system accepted credentials, Respondent No. 1 has placed nothing to suggest that the Complainant parted with, shared, or negligently exposed them. **Point (vii) is answered in the negative. No apportionment arises.**

XI. RELEVANT JUDICIAL PRECEDENTS

Before recording my considered view, it is appropriate to set out the authorities which have guided the findings above.

69. In *ICICI Bank Ltd. v. Saurabh Ravi Shankar Jain*, 2019 SCC OnLine TDSAT 3480, Decided on 24.09.2019 the Hon'ble Tribunal held that the jurisdiction under Section 43A read with Section 46 is confined to a body corporate possessing, dealing with or handling sensitive personal data or information in a computer resource which it owns, controls or operates, and to negligence in implementing and maintaining reasonable security practices within Section 43A read with Rule 8 of the 2011 Rules. This Authority has tested each ingredient separately at Point (iv) above rather than assuming it.
70. In *ICICI Bank Ltd. v. Umashankar Sivasubramanian & Ors.*, *Cyber Appeal No. 1 of 2010*, decided 10.01.2019, and affirmed by the Hon'ble Madras High Court in *ICICI Bank Ltd. v. Umashankar Sivasubramanian*, C.M.A. No. 2863 of 2019, decided 09.11.2022, the Hon'ble Tribunal held, at paragraph 16, that a bank's failure to secure its electronic records amounts to negligent assistance facilitating unauthorised access under Section 43(g), and that this liability arises irrespective of whether the customer's own credentials were used to effect the fraudulent transaction.
71. In *Sri Basaveshwara Pattana Sahakara Bank Niyamitha v. Canara Bank & Connected Matter*, *Karnataka High Court*, decided 08.06.2026 (Neutral Citation: 2026:KHC:25587), a primary urban co-operative bank suffered seven unauthorised RTGS/NEFT transactions aggregating ₹87.70 lakh after its internet banking authentication mechanism was compromised. The Hon'ble High Court held in paragraph 25.44, that

"...The standard of care applicable to a licensed public utility service provider is higher than that applicable to an ordinary commercial entity, precisely because public utility service providers occupy a position of trust and their failures can cause widespread harm."

The principle is of general application: liability attaches to the party which controls the authentication gateway and fails to safeguard it.

72. In *Manvir Singh v. ICICI Bank Ltd.*, *Cyber Appeal No. 10 of 2020*, decided 04.08.2026, the Hon'ble Tribunal considered and reversed a finding of an Adjudicating

Officer that production of an ISO/IEC 27001 certificate under Rule 8(4) of the 2011 Rules deems compliance with Section 43A notwithstanding a proved and admitted failure to issue transaction alerts. The Tribunal held, at paragraph 32, that

"... Merely by producing a certificate under Rule 8, the defiance, which is apparent and admitted today with regard to non sending of SMS alert, through cell phone, registered as well as email was there, and it was mandated by the RBI to be taken by each bank."

The Tribunal further held, at paragraph 36, that this failure

"...was failure of due and expected security practices, imposed upon the bank by RBI, through its above circular, and for this loss has been suffered by complainant appellant, for which claim under section 43A of IT Act 2000, was very well maintainable."

XII. IN MY CONSIDERED VIEW

73. Reduced to its essentials, my conclusion rests on seven propositions, each of which is established on the record and arguments advanced:

(a) The thirty- four transactions of 19.04.2019 were not authorised by the Complainant.

(b) Every one of them was routed through IMPS - a channel the Complainant never subscribed to from Respondent No. 1, which no instrument between the parties provides for, and which the Board Resolution relied upon by Respondent No. 1 does not mention. **(c)** A payment channel enabled on a customer's account without the customer's mandate is the service provider's responsibility from the moment it is enabled. Every transaction through it is unauthorised at inception. That is enough, by itself, to fix Respondent No. 1 with liability for the consequences.

(d) The controls Respondent No. 1 relies upon - the digital certificate and maker-checker authorisation - were, on this record, not engaged by IMPS transactions at all. A defence founded on safeguards the breach bypassed is no defence.

(e) Nothing in Respondent No. 1's system noticed anything: not three weeks of anomalous access, not concurrent authenticated sessions from two cities, not access after banking hours, not thirty- four transfers on a banking holiday to beneficiaries never before paid, not a single one of them. No alert, no OTP, no beneficiary-addition intimation, no velocity check, no block. A security architecture is to be judged by what it detects, not by what it certifies.

(f) The records which alone could have shown otherwise - the E- Net logs, the source IPs, the alert configuration, the SIEM output - were exclusively within Respondent No. 1's possession, were specifically called for on three occasions, and were not produced. The inference follows.

(g) The Complainant did nothing to bring the loss upon itself. Its premises were empty, its terminals were off, its officers were in Kolhapur while the money was moving from elsewhere, and it raised the alarm with its bank very next day and subsequently with the police, its regulator and CERT- In within days

74. I am accordingly of the view that Respondent No. 1 failed to implement and maintain reasonable security practices and procedures in relation to a computer resource which it owned, controlled and operated, and that such failure caused wrongful loss to the Complainant. Liability under **Section 43A of the Information Technology Act, 2000** is attracted.
75. I record, so that there is no misunderstanding of the basis of this Order, that the finding is **not** that Respondent No. 1 is liable because a fraud occurred on its platform. No system is impregnable, and liability under Section 43A does not follow from the fact of a breach.

The finding is that a channel was opened without mandate, that the controls which existed did not apply to it, that no control which did apply detected anything over a period of three weeks culminating in thirty- four transactions in one day, and that the evidence which might have shown otherwise was withheld. It is the conjunction of these, and not the occurrence of the fraud, which constitutes the negligence.

XIII. QUANTUM

76. Section 47 requires this Authority, in adjudging the quantum of compensation, to have due regard to the amount of gain of unfair advantage wherever quantifiable, the amount of loss caused, and the repetitive nature of the default.
77. **Amount of unfair advantage.** ₹67,88,041/- was transferred to beneficiaries to whom the Complainant owed nothing. The gain is quantifiable and co- extensive with the loss.
78. **Amount of loss.** From the statements of account at Exhibits "A" and "B":

Account	Transactions	Amount
01640380000253	28 IMPS	₹55,98,041/-
01640380000305	6 IMPS	₹11,90,000/-
	Total	₹67,88,041/-
	<i>Less recovered</i>	<i>(₹1,90,000/-)</i>
	Unrecovered principal	₹65,98,041/-

79. The Complaint as instituted claimed a larger sum, comprising the principal together with interest and incidental claims. The claim was subsequently confined to the fraudulent transactions established on the record, and the unrecovered principal now

pressed is ₹65,98,041/- . That figure is arithmetically verifiable from Exhibits "A" and "B" and has not been disputed by any Respondent.

80. The default was not a single lapse. Suspicious access on 02, 16 and 18 April passed unnoticed; concurrent sessions from two cities passed unnoticed; after- hours access passed unnoticed; and then thirty- four transactions were permitted to pass in sequence on a single day without one of them triggering an alert, a block or a step- up verification. The controls did not fail once. They were absent throughout.
81. Interest is directed from 19.04.2019, being the date on which the Complainant was deprived of the use of the funds. Interest so awarded is not punitive. It is the normal accretion on capital and compensates a party for being kept out of money to which it was legitimately entitled. The Complainant is a co- operative bank, and the sum withheld was deployable funds of which it was deprived for over seven years. The rate of 12% per annum is a reasonable measure of that deprivation.

ORDER

In view of the findings recorded above (from paragraph 1 to 81), it is ordered as follows:

1. Respondent No. 1, HDFC Bank Limited, shall pay to the Complainant, The Kolhapur Urban Co- operative Bank Limited, the unrecovered principal sum of **₹65,98,041/- (Rupees Sixty- five Lakh Ninety- eight Thousand and Forty- one only)**, together with interest thereon at the rate of **12% (twelve per cent) per annum** from **19.04.2019**, being the date on which the disputed transactions were effected, until the date of actual payment.
2. The said amount shall be paid within a period of **30 (thirty) days** from the date of this Order.
3. Any person aggrieved by this Order may prefer an appeal under Section 57 of the Information Technology Act, 2000 to the Telecom Disputes Settlement and Appellate Tribunal, New Delhi, within the period prescribed.

This Order is passed on the date of digital signature, at Mantralaya, Mumbai.

Digitally signed by
VIRENDRA SINGH
Date: 05-10-2026
16:29:42

(Virendra Singh)

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