TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL
NEW DELHI

Dated 4th August 2026

Cyber Appeal No. 10 of 2020

Manvir Singh ...Appellant

Versus

ICICI Bank ...Respondent(s)

BEFORE:

HON'BLE MR. JUSTICE RAM KRISHNA GAUTAM, MEMBER

For Appellant : Ms. Karnika A Seth
Mr. Gurneev Singh, Mr. Garvit Mathur, Advocates

For Respondent(s) : Mr. Anand Shankar Jha,
Ms. Nandika Kaushik, Advocates

JUDGMENT

1. This Cyber Appeal, under section 57 of the Information Technology Act, 2000, (hereinafter referred to as IT Act), has been filed by Manvir Singh, Appellant, against ICICI Bank, Respondent, against impugned Order / Judgment, dated 7th February 2020, passed by Learned Adjudicating Officer, Secretary(Information Technology), Govt. of NCT Delhi, passed in Cyber Complaint no. CC/ITD/31/2016, with a prayer to set aside impugned judgment and order passed by the Learned Adjudicating Authority and allow the prayer made in complaint by way of payment of damages as a

compensation in the tune of Rs. Fifteen lakhs alongwith interest at @ 12% w.e.f. 19th October, 2015 in favour of Appellant, as against respondent with other reliefs, which this Appellate forum deems fit and proper.

2. In brief, the memo of appeal contends that the Appellant Manvir Singhis an Indian National, having Diploma in Marine Engineering, working in Merchant Navy, as seafarer. He travels frequently and is on board cargo ships for long durations, ranging from 4-6 months on sea, due to nature of his job. When he is on sea, there are no signals of terrestrial mobile network and only satellite phone functions and limited internet is available. The Appellant used Globe Mobile SIM, while on ship and could only make or receive SMS and voice on phone call. The Appellant could also access the individual prepaid accounts by logging into Globe ifusion from any computer, connected to the Globe ifusion network, while onboard the ship or via internet. Internet access was available for limited duration, as determined by the management company. The Appellant opened an NRE (Non-Resident External) savings bank account, in the Respondent bank in 2007, bearing account no.017101011602 at its Saket branch, New Delhi. He was issued a debit card no.4554460171001611 by the Respondent Bank. At the time of opening the account the Appellant registered his email id Black05_hawk@yahoo.com and his mobile number 9219695128 for receiving all alerts, linked to

his account and debit card transactions. The Appellant had been using the said debit card for carrying out ATM transactions and online purchases using his 3D secure PIN, CVV and debit card number. At no point of time, the Appellant disclosed or shared his 3D secure pin with anyone. The Appellant was onboard ship from 22nd July, 2015 and signed off from vessel on 17th October, 2015. The last transaction he made with his debit card was to pay Airtel bill on 28th July, 2015 for Rs.375. Thereafter, he was sailing for 3 months and returned on 16th October, 2015 to India. After returning, he checked his account statement for the month of Sept-Oct 2015, and was shocked to learn that 98 unauthorized online transactions were made using his debit card during the said period i.e., from 27th September 2015 to 19th October, 2015, while he was onboard the ship. Since Appellant had not shared or disclosed his 3D secure pin to anyone, this could not have transpired without security breach, on part of the Respondent bank. It meant that financial details of his debit card, CVV number and 3D secure pin were hacked at the Respondent's end. Moreover, for the said unauthorized transactions, the Appellant neither received any OTP, nor other alert by way of SMS or email, to his registered mobile and email address from the respondent bank, which is the mandatory two step verification process, required to be complied with, as per RBI directions, issued under the Payment and Settlement Act, 2007. Appellant used to regularly receive such SMS / email alerts, till the time the said

unauthorized debits took place, from the said saving account. On coming to know of the unauthorized transactions, the Appellant on 19th October, 2015, lodged a complaint with the Respondent bank by email to block his said debit card. He also submitted a hard copy of the complaint alongwith passport and account statement on 23rd October 2015. The Respondent bank registered the complaint of the Appellant and a service reference number SR387346775 was provided to the Appellant. The Appellant, also made a complaint to Police Station Saket, Delhi on 23rd October, 2015 and a FIR no.1383 of 4th November, 2015 was registered, which is still pending investigation. On receiving no response from the Respondent bank, on status of his complaint, the Appellant, on 15th November, 2015, sent a reminder, followed by another email on 23rd November, 2015. The Respondent bank, on 23rd November 2015, intimated Appellant that they will let the Appellant know the status of his complaint by 8th December, 2015, but the Appellant was not done so. Rather, on 21st December, 2015, another service request no. SR392266743 was given by Respondent to Appellant. Vide email, dated 8th March, 2016, the Respondent bank confirmed that INR 6758.78 had been credited to account of Appellant on February 12, 2016, towards disputed transactions raised by appellant and Rs.2449.96 credit was processed on February 9, 2016. Credit processed on October 12, 2015 for Rs.15,908.56.

3. Out of the 98 unauthorized transactions, 81 were credited to the Appellant's account by respondent bank. The Appellant sent an excel sheet to the Respondent by email, showing all those transactions, which were unauthorizedly debited from his account, and are yet to be reversed. But Respondent bank, on 31st March, 2016, blatantly declined its liability to reimburse the remaining unauthorizedly debited amount, on frivolous basis, that the relevant transactions, as stated by Appellant has undergone 2nd level authentication with 3D secure PIN, specifically built in for online transactions done, through merchant websites. However, the 3D secure pin was unauthorizedly accessed and misused by Respondent bank, both for reversed and unreversed debit transactions, as no online debit could occur on any online merchant website without it. Not even this. Even before complainant complained to bank of unauthorized debits, on 7.10.2015, Rs. 72,772.13 was unauthorizedly debited and reversed on the same date (at serial no. 41-42 of **Annexure 8** of the complaint). The Respondent failed to maintain security practices and procedures to maintain secrecy and protect sensitive confidential financial information of the Appellant. Respondent bank systems were faulty and insecure, as is evident from the fact that the debit card of the Appellant had a transaction limit of Rs.2 lakh per day, and the unauthorized transaction reflected online purchases, more than the transaction limit, of a particular day. Hence, the Respondent bank had

violated their own norms and guidelines, but failed to explain how transactions more than permissible limit, were being allowed by its systems. Nor did the Respondent bank ever sent any alert, through email or SMS, on registered mobile and email id of Appellant, when such unauthorized transactions took place, in breach of the mandatory directions of the Reserve Bank of India (RBI). When these unauthorized transactions took place, the bank was obligated to detect abnormal and suspicious activities, which went on for days and bank even failed to send any SMS /email alerts. The total amount of unauthorized transaction during the period from 28th September, 2015 to 17th October, 2015 was of Rs.12,85,381.67, out of which Rs.7,81,771.72, is still to be reversed back in the Appellant's account. Out of 98 transactions, some were reversed automatically by Respondent bank, even before the complaint was lodged, amounting to Rs.3,30,627.51, on 6th June 2016. 49 transactions were reversed amounting to Rs.27,198.48, under the complaint no. SR392266743, filed by Appellant with Respondent on 19.10.2015. Hence, the total amount reversed was Rs.5,03,609.95.

4. The Appellant filed a complaint, on 24th October, 2016, bearing Complaint no. CC/ITD/31/2016, under Section 43, read with Section 46, of the Information Technology Act, 2000 (IT Act) before the Learned Adjudicating Officer, Delhi, for compensation of Rs. 15,00,000 plus interest on Rs.7,81,771.72,with a prayer to

held Respondent bank, to have violated provisions of Section 43 and 43A of the IT Act, 2000. The remaining debited amount of Rs.7,81,771 with interest of 12 % p.a w.e.f. 19.10.2015, and Rs. 5,32,000,towards mental agony and harassment, suffered by appellant - complainant, and cost of litigation in the tune of Rs. 2,50,000, i.e. total damages to the tune of Rs.15 lacs plus interest, was claimed for.

5. The respondent bank, respondent before learned adjudicating authority, after receiving notice of the complaint, filed its written statement/reply, with the preliminary objection, that the complaint is unauthorizedly filed by Hem Chand on behalf of the complainant, and thus, liable to be dismissed. The objection was also with regard to maintainability of this complaint, on the ground that section 43 / 43 A of the IT Act, is not attracted in the given facts of the case of the complainant. Police had investigated this case in pursuance of FIR No. 1383/2015, filed by complainant and none of the officials of the respondent bank were found guilty of any offence. Respondent is not liable to pay any compensation / damages. Complaint is abuse of process of law and filed with oblique motive. Complainant had himself disclosed or shared his 3D secure PIN of his debit card, which is a purely personal and privy to the customer. As per the respondent, they have investigated the matter, and found that the alleged transactions had undergone second level

authentication, with 3D secure PIN, specifically built in for online transaction, done through merchant websites, and apart from the Card Verification Value (CVV) and expiry date on the card, the personal 6 digit 3D secure PIN is also required for effecting the transaction, which is not known to any other person, except the complainant unless compromised otherwise. As the complainant/ card holder is responsible for the security of his card, alongwith his personal 3D secure PIN, the answering bank does not incur any financial liability arising out of misuse of the card.

6. Upon receipt of complaint and further follow up, a sum of Rs. 6758.78 was rolled back which is stated to be bank charges and further transactions were reversed at the merchant level as mentioned in Annexure – 2. The respondent denied any connivance or illegal designs on its part or of its officials. Rather, the complainant himself is responsible for the security of his card,alongwith personal 3D secure PIN and had to ensure its safe keeping. In nutshell, the submission of respondent is that it is not liable to pay any damage/compensation under the provisions of IT Act to the complainant since its employees or bank is not involved in any unauthorized access, deleting, forwarding, tampering with message, chat, hacking or unauthorized transaction etc.

7. This reply of respondent bank was got replied by complainant – appellant and the contention of complaint was reiterated in this replication.

8. Vide impugned order/judgment, learned Adjudicating Officer held that complaint was devoid of any merit and deserves to be dismissed and it was got dismissed. Whereas, the impugned order is contrary to the provisions of law. It was a case of failure of respondent bank to protect personal sensitive information of appellant, which was held at the respondent end causing unauthorized debit in the account of appellant,being maintained in respondent bank, and it was the defiance of provisions of section 43 and 43A of IT Act,2000. As per guidelines of the RBI, and directions given therein, there was a complete defiance of same with regard to appellant's sensitive personal data because of faulty server and system of respondent bank. Under section 43 and 43A of IT Act, 2000, explanation (ii) states reasonable security practices are to be determined by mandatory laws (in absence of agreement, defining the same), which have to be complied with and will determine the reasonable security practices.

9. In present case, the terms of agreement of debit card uses does not define those parameters and mandatory laws of RBI under Payment and Settlement Act,2007 determine the parameters of

reasonable security practices. RBI directions under Payment and Settlement Act,2007 are mandatory laws and its non-compliance has penal and other consequences, such as revocation of license of authorization under Section 8 of the said Act.

10. The Production of ISO 27001, by virtue of a deeming provision under R.8(4) IT (Reasonable Security Practices and Procedures) Rules, 2009 stands rebutted by the evidence produced by the complainant that bank's systems were faulty.But learned Adjudicating Officer failed to consider the evidence on record and he had completely ignored the facts. .Hence, there was every violation of provisions of section 43 of IT Act, 2000, for which complaint was filed before learned Adjudicating Officer, and appeal is before this Appellate Forum.

11. The legal precedent of this Tribunal itself, is the case of Bank of India and other vs Sandeep and others, Cyber Appeal Nos. 3 and 5 of 2018, dated 20.12.2019 of TDSAT Court. Hence, this appeal with above prayer.

12. Learned counsel for respondent bank had rebutted this appeal with same contention, as was before learned Adjudicating Officer and its reply before above forum.

13. Heard learned counsel for both sides and gone through material placed on record.

14. On the very perusal of Impugned Judgment, it is apparent that facts narrated in memo of appeal, were the same, given in memo of complaint, before Learned Adjudicating Officer. The response by Bank was the same one as has been written supra.

15. Learned Adjudicating Officer, after hearing both side, made three issues for determination.

16. First one was, whether the respondent bank has defaulted or compromised, in maintaining reasonable security practices, in any manner whatsoever, as per the mandate under section 43A of the Information Act?

17. Second, whether the respondent bank is liable to compensate to the complainant, under section 43 of the Information Technology Act?

18. Third, whether by not issuing alert messages to the customer / complainant by the Respondent bank, during online transactions, the Respondent has committed default, under the Information Technology Act and thus liable for compensation?

19. The complaint, was filed with specific mention, of left over amount Rs. 7,81,771.72/- (Rupees Seven Lakhs Eighty One Thousand Seven Hundred Seventy One and Seventy Two Paisa Only), which still remained to be re-backed to complainant's account, because of the same being not refunded, out of the total siphoned amount Rs. 12,85,381.67/- (Rupees Twelve Lakhs Eighty Five Thousand Three Hundred Eighty One and Sixty Seven Paisa Only), and the amount refunded from this, in the tune of details given as per Annexure – A to Complaint, leaving balance of Rs. 7,81,771.72/- (Rupees Seven Lakhs Eighty One Thousand Seven Hundred Seventy One and Seventy Two Paisa Only). With this amount, compensation towards mental agony as well as interest, in total 15,00,000/- (Rupees Fifteen Lakhs Only), was claimed as a relief in above complaint.

20. The reply was with same contention, of no fault by Bank Officers or employee. Rather, compromise was said to be made by complainant himself, who had transacted, disputed transactions, by way of 3D secure PIN, and two layer verification, including card verification value (CVV) and date of expiry of card, followed by personal 6 digit 3D secured PIN required for effecting the transactions, and the same could never be under knowledge, of anyone else, unless compromised by the user.

21. This was again rebutted by complainant, and the basic contention was that, it was the lapse of the Bank and its Officers, in maintaining reasonable security practices, where from those details of CVV of card, as well as its expiry date, and 3D secure, 6 digit PIN, could be known to fraudster, for enforcing this transaction, and there was said to be the defiance of guidelines of Reserve Bank of India (RBI) in this regard, specifically mentioning the act and rules i.e. Information Technology (Reasonable Security Practices, Procedure and Sensitive Personal Data or Information) Rules, 2011, framed under the I.T. Act, 2000, as well as the guidelines of RBI given to all its Bank.

22. Learned Adjudicating Officer, after going through Section 43A of Information Technology Act, held that, this provision entitles a complainant, to seek compensation, for failure to protect its data, in a case, where a body corporate possessing, dealing 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, such body corporate shall be liable to pay damages by way of compensation to the person so affected. This provision is with an explanation that 'body corporates' means "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities". The

second explanation to this Section 43A is that "reasonable security practices and procedures" means security practices and procedures, designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practice and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. The third explanation provides that "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

23. In exercise of powers conferred by Section 43A of the Information Technology Act, the Central Government made Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), Rules 2011, for the protection of sensitive personal data of the consumer and reasonable securities practices to safeguard against unauthorized access. Rule 3 defines sensitive personal data or information which Include (i) password, (ii) financial information, such as bank account, debit/credit card and or other payment details etc. Rule 4 directs body corporate having the control of the sensitive data

to provide for policy of privacy and disclosure of information. Rule 8 deals with reasonable security practices, purposes and its compliance including technical, operational and physical control measures. It also mandates that in the event of an information security breach, the body corporate of the person, on its behalf shall be required to demonstrate that they have implemented the security control measures as per their documents information security programme and security policies.

24. The Reserve Bank of India had issued detailed instructions to all the banks on (a) fraud risk management, (b) KYC norms, (c) transaction monitory, (d) dedicated e-mail I.D. and phone number for reporting suspected frauds, (e) mystery shopping and refuse, (f) reporting of fraud, (g) circular, dated July 1, 2010, (h) filing of police complaint by the bank, in the case of fraud committed against their customer, (i) customer awareness etc., in the guidelines on Information security, Electronic Banking, Technology Risk Management and Cyber Frauds in its circular, dated 29.04.2011.

25. RBI Circular 2012-2013 / 424 bearing DPSS(CO)PD1462/02.14.003/ 2012-2013, dated 28-02-2013, is issued under section 18 of Payment & Settlement System Act, 2007, to all Scheduled Commercial banks/ Urban Cooperative Banks/ State Cooperative Bank / District Central Cooperative Bank / Authorised Card

payment Works, directing guidelines on (a) security card payment transaction and (b) securing electronic payment transactions, with further direction to quickly Implement the same. Circular, dated 02.07.2012 of Reserve Bank of India, pertaining to Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/ Combating of Financial Terrorism of (CRT) of obligation of banks under Public Money Laundry Act, 2002 is also there.

26. Section 43 of the Information Technology Act, deals with penalty and compensation for damage of computer, computer system etc. The various forms of damage to compùter such as (a) securing unauthorized access to computer, source, (b) downloading, copying or extracting any data, computer data base or Information from such computer, computer system or computer network, (c) Introducing or causing to be Introduced any computer contamination, (d) causing damages to any computer, computer system or computer network, computer data base or any programme residing In such system, (e) disrupts or causes disruption of any computer, computer system or network, (f) denies or causes the denial of access to any person authorized to access any computer, system or network, (g) to facilitate access any computer, system or network, (g) to facilitate access to computer/ computer system in contravention of the provisions of this Act, Rules or Regulations, (h) tampering with or manipulating any computer, computer system or computer network, (I)

destroy, delete or alter any Information residing In any computer resource or diminishing its value or utility or affecting it injuriously by any means, (j) steal, conceal, destroy or alters or causes any person to steal conceal destroy or alter any computer source code with intention to cause damages.

27. Hence, any person causing damages to the computer, computer system or computer network in the aforesaid manner, is liable to pay damages by way of compensation, to the person so affected.

28. The above interpretation of the provisions of Information Technology Act, as well as the Rules framed thereunder, coupled with the guidelines given by Reserve Bank of India and the definitions given under the explanations of the Section 43A of IT Act, are the legal proposition for adjudging the dispute in the Information Technology Act, either by Adjudicating forum or by Appellate forum.

29. The ground and reasoning in the impugned judgment, is that the very argument of Complainant, present Appellant before Learned Adjudicating Officer, was that the Respondent failed to secure the sensitive personal data, kept under the computer resource of Respondent Bank as of CVV number of the Debit Card of Complainant, the date of its expiry, as well as 3D secure PIN of 6 digit, issued to the Complainant, and this compromise was made

either by insider/ employee of the Bank, or the system might have been hacked/compromised, facilitating leakage of sensitive information, resulting this fraudulent siphoning through 98 unauthorised transactions. For this contention, the Bank's stand was that in the criminal investigation, it was not found that the Bank Officer or Officials were at any fault, and Learned Adjudicating Officer has taken it as a guaranteed one. Whereas, even the finding of a Criminal Court, given in the final Judgment of conviction or acquittal, is not taken to be a proved fact, in adjudication of a Civil matter. Whereas, finding of a Civil Court is an important element in Criminal adjudicating system, but, Learned Adjudicating Officer had taken this very aspect that in Criminal investigation the liability of Bank Officer or Official was not held, hence, it was so.

30. The expected Reasonable Precaution for maintaining Practices and Procedures, for protecting Sensitive Personal Data, or Information lead, the Rules of 2011, has been promulgated under Information Technology Act, written supra. Rule 8 of same, the provision, is of implementation of either IS/ISO/IEC 27001 standard, or the codes of best practices for data protection as approved and notified under sub-rule (3) or Rule 8 as above, and in case of this production of certificate, it shall be deemed to have been complied with the reasonable security practices, provided that, such standard or code of best practices have been certified

or audited on a regular basis by the entities through independent authorities / auditors, duly approved by the Central Government, and this audit shall be carried on by the auditor itself, once a year or as and when the body corporate or person on its behalf undertake significant upgradation of its process and computer resources.

31. In the present case Respondent Bank had placed on record, the certificate of ISO/ IEC 27001/2013 standard, bearing original effective date 09.03.2011 to 09.03.2014, further revised, vide version 2, dated 29.04.2015, and further valid upto 08.03.2017. Hence, during the period of disputed transaction i.e., 27.09.2015 to 19.10.2015, this certificate was of valid effect. Hence, Learned Adjudicating Officer deemed that Respondent Bank had maintained reasonable securities practices, as per the aforesaid law, and that's why no flouting of Section 43A of IT Act or Rules made there under was, held. Whereas, the non-compliance of reasonable security practices was pleaded and proved by way of evidence of complainant, before Learned Adjudicating Officer and the main thrust was with regard to mandatory direction for issuing alert message to its customers on each online ATM transactions by Bank concerned under RBI guidelines, whereas, Respondent Bank had not complied it. It defaulted in this direction. The stand taken by Bank was that the complainant was not registered to sent alert messages on to his mobile number,

during the period when the disputed transactions, were carried out and his telephone number was registered only, subsequent thereto, to sent alert messages. On the contrary, the complainant produced copies of the alert messages, received by the Complainant through e-mail of various dates, prior to the disputed transactions, to butters his submission that the stand taken by the Bank is wrong and the e-mail I.D. alongwith telephone number was already in the data / record of the bank, which it has been using from time to time to send alert messages atleast through e-mail vide some copies produced. This was again pressed by Learned Counsel for Complainant, before Learned Adjudicating Officer that, after the notification, dated 29-03-2011 and 04-08-2011, issued respectively by RBI, as part of security and risk mitigation measures related to usage of debit / credit card, and security issues and risk mitigation measures, related to CNP (Card Not Present) Transaction, it was mandatory to bank respondent to send alert messages, as well as emails informing about transactions, on registered mobile phone as well as emails.

32. This point for determination, raised before Learned Adjudicating officer, was not answered by him, though, he has written this contention and reply in his judgment, but had escaped by saying that "In my considered opinion, the answer will be negative for the reason that the adjudicating authority under the Information Technology Act can direct payment of compensation only in two

situations i.e. either for violation of section 43 or violation of section 43 A of the Information Technology Act. I have already written finding Supra that in the backdrop of facts and circumstances of this case, neither infringement of section 43, nor section 43A of the Information Technology Act is made out. It is the argument of the complainant that by not sending alert messages at the time of transaction, the respondent bank has violated section 43A of the Information Technology Act. In my considered opinion, section 43A can be pressed only where the respondent, being a corporate body, failed to maintain reasonable security practices. However, as per Rule 8 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, once the corporate body produced the requisite certificate of standard 27001, it is deemed to have complied with section 43A of the Information Technology Act, which compliance has been made by the respondent bank vide the requisite valid certificate placed on record. Hence, violation of section 43A of Information Technology Act is ruled out even if respondent bank failed to send alert message to the complainant at the time of online transaction whether using the card or without card i.e. the time of online transaction whether using the card or without card i.e. CNP transaction. At the most these types of default can be termed as deficiency of services on the part of the bank and a customer may seek compensation before other appropriate

forum but atleast not in this forum keeping in view the limited and circumscribed jurisdiction vested upon the adjudicating authority under the Information Technology Act." This finding of learned AO is devoid of any merit. He had failed to interpret law in its correct perspective. 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, with regard to online transaction. And it was guidelines given under section 43 A of the IT Act, as well rules made thereunder in 2011.

33. This Tribunal itself, in its judgment given, in Cyber Appeal No. 1 of 2010 (ICICI Bank vs. Mr. Umashankar Sivasubramanian & Ors.), decided on 10.01.2019, in para 16, has held that :

"16. Although Section 43A creates a special responsibility to protect sensitive personal data or information in a computer resource and creates a liability to pay compensation for certain kind of negligence, the definition of the word "computer" existing from before in the Act is wide enough to include all input, output processing, storage.....(emphasis supplied). The Bank's electronic records in a computer are required to have a safe and secure procedure of access. Under Section 14 it would fall under the term "secured electronic record" and hence, unauthorised access to such records should not have been facilitated by the

Bank by assistance through negligence which is also described in detail by the Adjudicating Officer..... "

34. The mandate of RBI guidelines with regard to SMS alert and email communication of transaction is mandatory to each bank to make compliance. The law laid down by this Tribunal in 2019 SCC online TDSAT 2086 in Cyber Appeal No. 3 of 2018 (Bank of India Vs. Sandeep and Anr.) alongwith Cyber Appeal No. 5 of 2018 (Vodafone Idea Ltd. Vs Sandeep Singhal and Anr), as well as Cyber Appeal No. 8 of 2014 (The Branch Manager, State Bank of India Vs. The Managing Director, Nakoda Chemicals Ltd., this Tribunal had categorically propounded that compliance of sending SMS alert by registering its mobile number as well as email of same, is mandatory for bank, for maintaining its reasonable security practices in internet banking.

35. In the present case, the first stand taken by bank was that the complainant had not registered its registered mobile number for facilities of SMS alert. This was vehemently denied by complainant and was said to be with the same facility and was being provided prior to these disputed transactions. Even before this Appellate forum, learned counsel appearing for bank fairly admitted that if this registered mobile number and email was registered with the bank, then certainly bank was to make the compliance of same. But he took the time to have version of the

bank, but inspite of his all effort, he could not place on record the same thing. Rather, opted to argue on the basis of documents which are available on record.

36. But admittedly, the documents had been filed by complainant appellant, showing his initial opening of this account wherein the registered mobile number, as well as email had been given and got registered with bank, in exercise of above internet banking facility. Hence, this negligence, as well as failure of bank, either through its employee, or officer or by its system, was with specific finding of non sending of SMS alert, as well as emails, for fraudulent transactions, and it 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 43 A of IT Act 2000, was very well maintainable, before learned Adjudicating Officer, but he failed to appreciate it. Hence, this appeal merits to be allowed with cost and the impugned judgment ought to be set aside.

37. The claim made before learned Adjudicating Officer, proved by way of this presentation before learned Adjudicating Officer, on record, as well as the pleadings made before this Appellate Tribunal had proved that Rs. 12,85,381.67 was fraudulently siphoned through 98 transactions, out of which Rs.5,03,609.95, had been returned back, after the due care and caution taken by bank, as well as the system of the bank. But Rs. 7,81,771.72,

rounded at Rs. 7,81,772/-, had not been returned as yet, for which this complaint was filed, and appellant - complainant, is entitled for it for having compensation of its loss. As this money was taken away in the year 2015 and now it is 2026, hence, for this period of litigation, and till actual date of payment, complainant – appellant is entitled for 7% simple interest, over above amount. The mental agony and harassment cost in running from pillar to post, is also to be compensated, by way of awarding, reasonable damages of Rs. 50,000/-, from the bank, in total of remaining amount of Rs. 7,81,772/-, (Rupees Seven Lakhs Eighty One Thousand Seven Hundred Seventy two only),the simple interest over it from the date of complaint, pendente lite and future, till actual date of payment, in the tune of Rs. 7% per annum, over above amount, with a cost of Rs. 50,000/- towards damages, mental agony suffering, is to be paid by bank-respondent ICICI Bank, to appellant – complainant. The same is to be paid within two months from the date of judgment.

38. Hence, with above discussion and mandate, appeal is being allowed.

Formal order/ decree be got prepared by office, accordingly.

Certified to be a True Copy

.....
(Justice Ram Krishana Gautam)
Member

04.08.2026
/NC/