

TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL

NEW DELHI

Dated 25th September 2024

Cyber Appeal No. 14 of 2015

State Bank of Patiala Aliganj Branch Lucknow ...Petitioner(s)

Vs.

Suhas Enterprises And Others ...Respondent(s)

Cyber Appeal No. 16 of 2015

Vodafone Idea Ltd. ...Petitioner(s)

Vs.

Union of India And Others ...Respondent(s)

Cyber Appeal No. 18 of 2015

Dhanlaxmi Bank Limited ...Petitioner(s)

Vs.

Rajesh Aggarwal And Others ...Respondent(s)

Cyber Appeal No. 22 of 2015

State Bank Of India And Anr ...Petitioner(s)

Vs.

Suhas Enterprises And Others ...Respondent(s)

BEFORE:

HON'BLE MR. JUSTICE RAM KRISHNA GAUTAM, MEMBER

Cyber Appeal No. 14 of 2015

For Appellant : Mr. Rajiv Kapur & Ms Riya Sood

For Respondents : Mrs Yugandhara Pawar Jha, Mr Kunal Verma,

Ms Lavanya Dhawan, Mr Shivraj Pawar & Mr Ritik
Gupta For R-1 For Suhas Enterprises

Mr Meet Malhotra, Sr. Adv., Alongwith Mr Jaiyesh
Bakhshi, Mr Ravi Tyagi, Ms Manmilan Sidhu, Ms Ria
Chanda, Ms Bhumika Bhatnagar, Mr Mayank Mishra,
Ms Pallak Singh For Vodafone Idea Ltd. For R-4

Cyber Appeal No. 16 of 2015

For Appellant : Mr.Meet Malhotra, Sr Adv., Alongwith Mr Jaiyesh
Bakhshi, Mr Ravi Tyagi, Mr Mayank Mishra, Ms Pallak
Singh, Ms. Manmilan Sidhu, Ms Ria Chanda & Ms
Bhumika Bhatnagar

For Respondents : Mrs Yugandhara Pawar Jha, Mr Kunal Verma,

Ms Lavanya Dhawan, Mr Shivraj Pawar & Mr Ritik
Gupta for R-2 For Suhaas Enterprises Mr Gautam
Kumar For Dhanlaxmi Bank

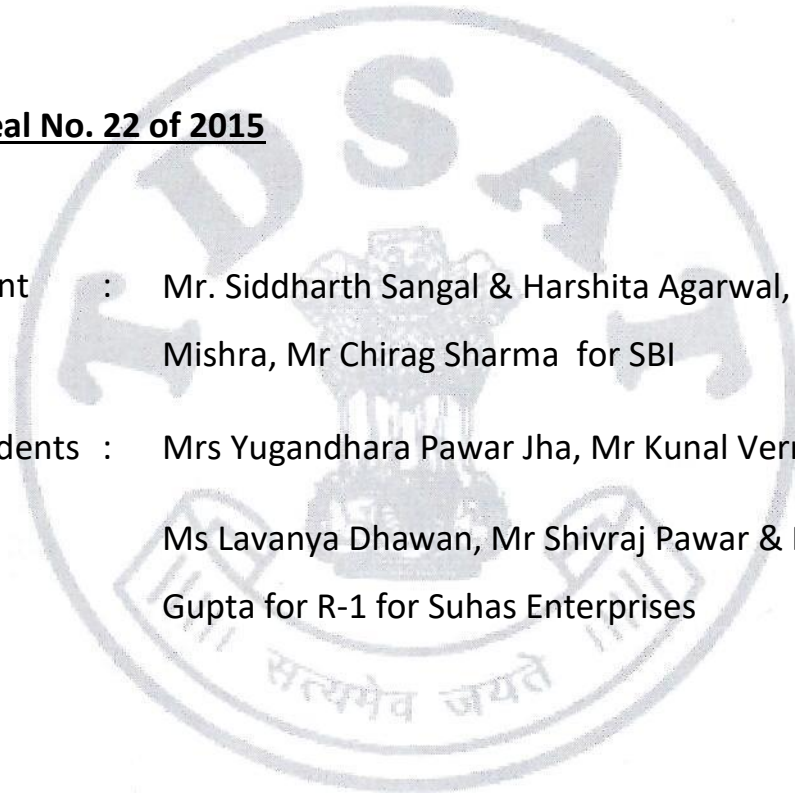
Cyber Appeal No. 18 of 2015

For Appellant : Mr. Gautam Kumar for Dhanlaxmi Bank

For Respondents : Mr. Meet Malhotra, Sr. Adv., Alongwith Mr Jaiyesh Bakhshi, Mr Ravi Tyagi, Mr Mayank Mishra, Mr Pallak Singh, Ms Manmilan Sidhu, Ms Ria Chanda & Ms Bhumika Bhatnagar for Vodafone Idea Ltd.
Mrs Yugandhara Pawar Jha, Mr Kunal Verma,
Ms Lavanya Dhawan, Mr Shivraj Pawar & Mr Ritik Gupta for R-2 for Suhas Enterprises

Cyber Appeal No. 22 of 2015

For Appellant : Mr. Siddharth Sangal & Harshita Agarwal, Ms Richa Mishra, Mr Chirag Sharma for SBI
For Respondents : Mrs Yugandhara Pawar Jha, Mr Kunal Verma,
Ms Lavanya Dhawan, Mr Shivraj Pawar & Mr Ritik Gupta for R-1 for Suhas Enterprises



JUDGMENT

1. This **Cyber Appeal No. 14 of 2015**, by State Bank of Patiala (now State Bank of India), Aliganj Lucknow Branch, against M/s Suhas Enterprises, Registered Partnership Firm, through its authorised partner, Mr. Suhas Mankame, complainant – Respondent No. 1, Bank of Maharashtra, Head Office, as well as Bank of Maharashtra, through its Branch Manager, Mr. Prakash Chittodkar, respondent nos. 2 and 3, Vodafone Essar Limited, respondent no. 4, Dhanlaxmi Bank Ltd. Branch – Jaipur, through its Branch Manager, Mr. Anup Nair as well as Dhanlaxmi Bank, Head Office, respondent no. 5 (A & B), State Bank of India, its General Manager as well as Branch Manager, respondent no. 6(A & B), Punjab National Bank, Head Office as well as its Branch Manager, respondent no. 7 (A & B), under Section 57 of the Information Technology Act, 2000, against Order dated 12.01.2015, passed in Cyber Complaint No. 26 of 2013, by Adjudicating Officer(AO), Shri Rajesh Aggarwal, Principal Secretary, Information Technology, Government of Maharashtra, Mumbai, under section 43, 43A, 46, 61, 72A, read with section 85 of IT Act, 2000, is with this contention that Mr. Saurabh Pandey, on 15.4.2013, got opened his savings Bank A/c No. 55144678983, at appellant Bank Branch State Bank of Patiala,

Aliganj Branch, Lucknow, after complying with KYC norms, laid down by Reserve Bank of India, by producing his proof of identity i.e. PAN Card bearing No. BXHPP9737Q, and proof of address i.e. Voter Identity Card bearing EPIC No. TDQ0307096, together with a photograph of him. These documents are Annexure A1 (colly.) to the memo of Appeal.

2. As per directions of circular letter No. GB S&P/50 of 2007-08 dated 9.2.2008, the requisite compliance of proof of identity and proof of address was got complied with, then after account was got opened validly. There had been transaction of deposit of Rs. 1000/- on 15.4.2013, and thereafter, account operated by Shri Pandey on 17.7.2013, for the first time. Copy of Statement of above Account is Annexure A-4 to the memo of Appeal. On 17.7.2013, a request through email from Bank of Maharashtra through Shri Anil K Popli, Senior Manager RTGS, Treasury and International Banking Division, Mumbai, was received by appellant bank to put hold the account No. 55144678983 of Shri Saurabh Pandey.
3. However, multiple withdrawal transactions in the tune of Rs.7,40,000/- had already been taken place before the receipt of

information from Bank of Maharashtra on 17.7.2013 and after receipt of this information the remaining amount of Rs. Two lakhs only was kept on hold. On 31.7.2013, Mr. D S Arve, Police Inspector, Dattawadi Police Station, Pune City, Maharashtra, requested appellant bank to furnish information under section 91, CrPC, 1973. It was replied by a letter dated 25.10.2013. M/s Suhas Enterprises, complainant, through its authorised person i.e. Respondent No. 1 / complainant, filed a complaint dated 22.11.2013, bearing number 26 of 2013, before Shri Rajesh Aggarwal, Principal Secretary, Information Technology, Government of Maharashtra, Mumbai, Adjudicating Officer, under section 43, 43A, 46, 61, 72A read with section 85 of IT Act, 2000, against Bank of Maharashtra, respondent nos. 2 and 3, and M/s Vodafone Essar Limited, respondent no. 4, for claim of compensation, wherein, vide interim order, dated 14.10.2013, it was held that complainant, respondent no. 1 was having his Cash Credit Account bearing no. 60129897006, with Bank of Maharashtra, having its branch at Sinhagad Road, Pune, i.e respondent no. 3. Complainant / respondent no. 1 received a call from respondent no. 3, Security Operation Centre, on 17.7.2013 that large amounts were taken out from its above bank account, through online transfers. Whereupon

complainant / respondent no. 1 visited respondent bank No. 3, Branch Manager and requested him to freeze its account, as well as account where money has been illegally transferred. Then it was apprised by Complainant / respondent no. 1 that on 17.7.2013, some unknown persons had got deactivated his mobile number 9158000825 and got a new SIM card from Cell operating company, respondent no. 4 Vodafone Essar Ltd., without due verification and information to complainant/respondent no. 1, and during the course of investigation, it was found that many of the accounts into which the fraudulent transactions transferred, were got frozen.

4. Bank of Maharashtra was directed to deposit frozen amounts within 7 days of the order. It was further held, vide interim order dated 29.10.2013, that alleged fraudulent transferred amounts of complainant / respondent no. 1, were illegally transferred to several bank accounts opened with Dhanlaxmi Bank, State Bank of India, as well as the appellant bank, wherein remaining balance amount was frozen. Learned Adjudicating Officer released all the amounts pertaining to the disputed transaction to the accounts of complainant/respondent no. 1 and appellant too remitted Rs. Two lakhs to the

account of complainant / respondent no. 1. By way of amendment application, pleadings of petition/complaint was got amended wherein, appellant as well as Dhanlakshmi Bank, State Bank of India, Punjab National Bank, were got added as respondents. Notices were got issued on 19.11.2023. Replies were got filed and after hearing, impugned order under appeal, dated 12.1.2015 was got passed, which has been assailed in this appeal, with contention that impugned order is misconceived, untenable in the eyes of law, is with no reasons, nor with any appreciation of fact and law. Appellant Bank had opened savings bank account of Mr. Saurabh Pandey, after full compliance of guidelines and norms, given with regard to KYC. The requisite documents, valid for proof of identity and proof of address, were taken with photographs of account holder and after due verification, it was got opened. Legislative intent of Section 43A of IT Act, was with regard to responsibility for safeguarding any sensitive personal data, to be handled with regard to particular person, affected thereat. But appellant bank cannot be held responsible for the sensitive personal data of the complainant / respondent no. 1, for which he was having no data, nor it got arrayed as a party initially. No finding with regard to responsibility of appellant is there. Mere finding of non adherence

with KYC norm with regard to money mule account, in order to prevent cyber crime, by appellant bank, may not be a basis of impugned order, for making payment of compensation in the tune of Rs. 7.5 lakhs, ordered in impugned order.

5. The direction was for making payment within four weeks of judgment.

Whereas, section 57(3) of IT, 2000, itself provides for 45 days for appeal, that too after the date of communication of the order. Hence, in that appeal period, compulsive coercive order may not be passed. Order itself is erroneous on this alone ground. More so, complainant / respondent no. 1 was under knowledge of its all banking credentials, but it failed to make it secret, rather, it was made available to others, which resulted this siphoning of money from his account. There was no defiance of any circular by appellant bank, nor there had been any reason given in the impugned judgment. Hence, this appeal with above prayer for setting aside the impugned order.

6. **Cyber Appeal No. 16 of 2015**, was filed by 'Vodafone Cellular Limited' against Union of India and Others against same impugned order dated 12th January 2015, passed in same Complaint No. 26 of 2013, under

Section 57 of IT Act, 2000, within jurisdiction of this Tribunal, as well as under limitation period, provided for this Appeal, assailing the same impugned order of Adjudicating Officer, with this contention, that present Appellant is a Public Limited Company, incorporated under the provisions of the Companies Act, 1956, having its registered Office at Vodafone Cellular Limited, 1045/ 1046, Avinashi Road, Coimbatore – 641018, with a circle office at The Metropolitan Building, Wakdewadi, SY No. 21, F.P. No. 27, Old Pune, Mumbai Highway, Shivajinagar, Pune 411003. It is in the business of providing telecom service, as licensed telecom service provider, having license under Unified Access Service, post migration from CMTS under new No. 842-1019/ 2008-AS-IV w.e.f. 6th November 2008, for the entire state of Maharashtra & Goa, excluding Mumbai. Ms. Mohanna Manjre, the Authorized Representative of Appellant Company, had filed this appeal against the impugned order, dated 12.01.2015 of Ld. Adjudicating Officer, Principle Secretary, Information Technology, Government of Maharashtra, Shri Rajesh Aggarwal, passed in Complaint No. 26/2013, whereby, Appellant was directed to make payment of compensation, in the tune of Rs. 10 Lakhs, to the Complainant, who is Respondent No. 2 in this Appeal. Complainant

i.e., Respondent No. 2 of this Appeal, is registered as a subscriber of Appellant, as an individual subscriber on 29th July 2009, by way of customer agreement form dated 29th July 2009, **Annexure 3**, and the documents submitted **Annexure 4**, to memo of appeal. There is no agreement, in between Respondent No. 3 and 4, or any other bank as well as Appellant.

7. An application was made by Respondent No. 2, through its authorized representative, for a post-paid corporate connection number 9158000825, in the name of Respondent No. 2. On 04.05.2013, an Agreement of Franchise, was entered, in between, the Petitioner and Hi-Tech Cellular, Pune, for providing the Company's service of an initial period of 04 years, on an exclusive basis, and this Franchisee under the agreement, was to be responsible for abiding prevailing Laws, Acts and Legislation, Rules framed thereunder. As per agreement, Franchisee shall also develop and maintain customer competence and satisfaction.
8. Certain person, holding himself as the Authorized Representative of Complainant, Suhas Enterprises, Respondent No. 2 of present Appeal, visited Hi-Tech Cellular at Shop No. 2 and 3, Ramrajya Building,

Opposite City Bank, Near Carnival Restaurant, College Road, Nashik 422005, which was a Franchisee store of Appellant, on 15th July 2013, with a request for replacement of SIM Card. Upon receipt of SIM replacement request, in the prescribed form, alongwith with the requisite documents of subscriber, annexed as **Annexure 6** to memo of appeal, the request was duly processed and a new SIM bearing No. 9158000825 was got issued to that person, who visited the store. This SIM was got activated at 11:56:52 AM IST on 17th July 2013. This Person was complained to be an imposter by Complainant, Respondent No. 2, who visited the Vodafone Store at Hirabaug, Pune on 17th July 2013, with a request for replacement of the SIM, and upon receipt of the SIM replacement request in the prescribed form alongwith requisite documents of subscriber, Annexure 7 to memo of appeal, the request was duly processed and a new SIM bearing number 9158000825, was got issued to Complainant and this SIM was got activated at 14:31:50 P.M. IST on 17th July 2013.

9. Respondent No. 2/ Complainant lodged an FIR No. 174 of 2014 with Datta Wadi Police Station on 25.07.2013 under Section 420 & 34 of I.P.C. A complaint was also got filed by Complainant Respondent No. 2

of Appeal, before Ld. Adjudicating Officer, as Complaint No. 26 of 2013, under Section 43, 43A, 46, 61 and 72, read with Section 85 of IT Act 2000, against Respondent No. 3 and 4 alongwith Appellant.

10. On 9th October 2013, Appellant, through its letter requested Cyber Cell, Pune and Datta Wadi Police Inspector to take appropriate action against the imposter for that fraud. Appellant co-operated in the investigation of that Cyber fraud by Inspector concerned. A request under Section 91 of Code of Criminal Procedure, 1973, for producing few of documents was received from Datta Wadi Police Station, Pune, and it was replied appropriately. The Complaint, filed before Adjudicating Officer, was also replied by Appellant. A preliminary objection, regarding the maintainability of above Complaint against the Appellant, was also raised there at.

11. Adjudicating Officer, Principal Secretary, Information Technology, Government of Maharashtra, passed impugned order, dated 12.01.2015, directing Appellant to pay compensation, in the tune of Rs. 10,00,000/- (Rupees Ten Lakhs only) within a month and in case of failure, with compound interest at the rate of 12%, to be compounded monthly.

12. Writ Petition (Civil) No. 1641 of 2015, was filed before Hon'ble High Court of Delhi, by Appellant, wherein, vide order dated 23.02.2015, Impugned Order was got stayed on 23.02.2015. The Impugned Order dated 12th January 2015, is without reason, appreciation of facts and law, and is beyond the contention of complaint. The jurisdiction of Adjudicating Officer, under Section 43A, read with Section 46, of Information Technology Act, was restricted to claims involving :

- (i) body corporate possessing, handling and dealing in sensitive personal data or information in a computer resource, which it owns, controls or operates and
- (ii) negligence by such body corporate in implementing and maintaining reasonable security practices and procedures (as prescribed by Section 43A of Information Technology Act, 2000 read with Rule 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, in respect of such computer resource which owns, controls or operates.

13. In the instant case, Appellant, being a Cellular Service provider, was not handling the sensitive personal information, the unauthorized

access of which caused the wrongful loss to Respondent No. 2, nor it was negligent in implementing and maintaining reasonable security practices and procedures, as prescribed by Section 43A of the Act, read with Rule 8 therein, in respect of any computer resource, which it owns, controls or operates. But, it was not appreciated by Ld. Adjudicating Officer. To bring a case in respect of Section 43A of IT Act, Complainant must show that there is sensitive personal data or information, being possessed handled or dealt with by Appellant, whereas, it was categorically stated that it does not possess, handle or deal with any sensitive personal data or information. Therefore, Section 43A of the Act was having with no obligation vis-à-vis cellular company Appellant is concerned. As per Indian Telegraph Act, 1885, Indian Wireless Telegraphy Act, 1933 and as per Column 2 of the License Agreement, for provision of Unified Access Service, dated 6th November, 2011, granted by the Department of Telecom to Appellant, the scope of the services, the Appellant is entitled to provide is collection, carriage, transmission and delivery of voice and/or non-voice messages over the Licensee's network, in the designated Service Area. Hence, the role of Telecommunication Service Provider, is restricted to providing access to its network, to the subscribers of such

Telecom Service Provider, to transmit messages in real time and other than in relation to a transit nary period. Such messages are not saved or stored on any computer resources. The Appellant does not have any access to the content of the message (voice or text), being transmitted over its network and it neither stores, nor possesses, nor handles, nor deals with the contents of above messages, which are being transmitted over its network. Unless specifically being directed and instructed by Government of India, under Section 5 of the Indian Telegraph Act, 1885, the Appellant has no access or right to intercept, in any manner, whatsoever, in respect of the messages or the content thereof, which are being transmitted on its network. Hence, question with regard to sensitive personal data or information, never arises in the course of Appellant's function to provide the Services, under the License granted to it, by the Department of Telecommunications. There were guidelines and directions, issued by Telecommunication Department, for observing, before issuing any mobile connection or its activation, in circular dated 9th August, 2012, which is **Annexure - 16** to the memo of Appeal. Accordingly, there is two tier mechanism, namely, Retailer/Franchisee and Distributor. The role and

responsibility of the Retailer/Franchisee and the Distributor are clearly elucidated therein.

14. This all was adequately complied by Appellant. For seeking an order of compensation, under Section 43 of the Act, the Complainant must specifically identify the sensitive personal data or information, which is possessed, handled or dealt with, by Cellular Telecom Company i.e., Appellant. But, it was not proved so. But Adjudicating Officer failed to appreciate. On the contrary, Complainant had specifically admitted that the only inconvenience caused to him, was the alleged non-receipt of intimation of the transfer of money from alleged bank account of complainant with bank - **Respondent no. 4**. In the light of same, Adjudicating Officer had failed to bring out any finding on the exact nature of sensitive personal data or information relating to Appellant to cause alleged loss. The only personal data or information, and the unauthorized access in Bank account, resulting wrongful loss to complainant was the one time password communicated to Complainant by bank. It was the negligence of the Complainant itself, which resulted such fraudulent transaction from his account. There was no contention with regard to negligence in implementing and

maintaining the reasonable security practices and procedure, as was prescribed by Section 43A of the Act, read with Rule 8 of the Rules, by Appellant. In its capacity as a Telecommunication Service Provider, the only computer resource owned, controlled and operated by Appellant is its equipment, hardware, software, switches, junctions installed at switching centers, transmission centers, network operation and control/ management centers, base stations, cell sites, radio transmitters, media gateway controller, soft switches, call controller etc. Whereas, under Section 43A of the Information Technology Act, 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 practices and procedures, as may be prescribed by Central Government, in consultation with such professional bodies or associations, as it may deem fit.

15. So far as Appellant is concern, Clause 46.1A of the License Agreement for provision of Unified Access Service, dated 6th November 2011, granted by the Department of Telecom, to all Unified Access Service Licensees, as notified by the Department of Telecommunications, vide its letter dated 31st May 2011, mandate the implementation of the ISO 27001, Standard for Network Security. Hence, it was being obeyed by Appellant and it does not include the subscribers verification process, at the time of issuance or re-issuance of SIM Cards. Provisioned ISO Standard 27001 for Network Security, had been observed and this was observed by Appellant all the time.

16. Respondent No. 2 i.e., Complainant had himself stated in its pleading before Ld. Adjudicating Officer, that the only inconvenience caused to him on the account of deactivation of the Telecom Services to the SIM Card, inserted in the handheld device of the Complainant was to make enable to receive intimation at the time of alleged unauthorized transfer of funds from the bank accounts of Complainant, maintained with Respondent No. 4 bank. It is not the Complainant's case that such non intimation, resulted in siphoning of money or unauthorized access to the Complainant's account. It was the contributory negligence of

Complainant, which resulted such fraud, because of leak of mobile password, user id, password, One Time Password and other security layers applied by banks, while offering internet banking service, and this was not appreciated by Ld. Adjudicating Officer, while apportioning and imposing amount of compensation, in the impugned order. Hence, this appeal, with above prayer, for setting aside Impugned Order.

17. **Cyber Appeal No. 18 of 2015** had been filed by Appellant, Dhanlaxmi Bank Limited, through its authorized signatory versus Shri Rajesh Aggarwal and others, against the same impugned order, dated 12.01.2015, of Mr Rajesh Agarwal, Adjudicating Officer & Principal Secretary, Information Technology, Government of Maharashtra, passed in same complaint, between same parties, whereby, Appellant-Dhanlaxmi Bank, was directed to make payment of Rs. 18.00 Lakhs (Rupees Eighteen Lakhs only), by way of compensation, to Complainant, M/s Suhas Enterprises, within a month, failing which a compound interest @ 12%, to be compounded monthly was to be paid.

18. In brief, the contention of this Appellant was that Adjudicating Officer was not with jurisdiction to entertain complaint under Section 72 of the Information Technology Act, 2000, and to adjudicate under Section 46 of IT Act. No unauthorized person, in the present case, has secured access to any electronic record, book, register, correspondence, information document or other material of the appellant's bank, Jaipur Branch, nor disclosed the same to any other person. Neither Appellant Bank was involved in such activities. Hence, there was no jurisdiction to adjudicate against Appellant. Appellant Bank had never breached, the confidentiality and privacy of Complainant, as it was never being a bonafide account holder of the applicant bank branch at Jaipur, nor the complainant or the Bank of Maharashtra, Pune, had ever passed and/or shared any data/information of its own account holders with the Applicant and as such, the Adjudicating Officer had wrongly entertained the Complaint of Complainant, M/s Suhas Enterprises, under Section 72 of the Act, against the appellant bank. Appellant Bank was having possession, dealing and handling sensitive personal data and information of its own account holders, and it was never negligent in implementing and maintaining reasonable security practices and procedures, with regard

to those information. Hence, it never caused any wrongful loss, or gain to any person, and was never liable to be adjudged by Adjudicating Officer, vide Impugned Order under Section 43A of the Act, nor it may ever be held, responsible to make payment of compensation or damages to complainant. The Complainant had never been a bonafide account holder of the Appellant Bank. Appellant bank had neither been involved in handling any sensitive and/or personal information, and/or data of the complainant. Therefore, the question of failure to protect any of the data/information of the Complainant, by the Appellant Bank didn't arise, under any stretch of imagination for attracting Section 43A, of the IT Act, 2000 for any wrongful loss to the Complainant or gainful to someone else. That neither the Complainant, nor the Adjudicating Officer could establish the breach or contravention on the part of Appellant Bank. By allowing its bonafide Account Holder, to withdraw the money, standing to his credit in the account of Appellant Bank, ensuring the due process on the day of incidence on 17th July 2013, neither the Appellant Bank had violated, nor disregarded any of the relevant rules regulations and procedures, issued by the Reserve Bank of India in such a case.

19. In brief, the fact was that on 8th September 2012, one Irfaan Ansari had approached Appellant's Jaipur Branch, for opening a current account. He applied to open the current account in the prescribed form of the Appellant's Bank, Jaipur Branch and submitted his photograph, photocopy of each of his PAN Card No. AXIPA739R, Ration Card for supporting documents, with a self drawn cheque from his own account with another bank, Karur Vysya Bank. After due scrutiny and verification with the originals, his current account, bearing no. 021806700001020 with Jaipur Branch of Dhanlaxmi Bank, was got opened on 17th September 2012 and cheque book containing cheque No. 210551 to 210570 was got issued. Before all this opening and issuing, KYC norms and guidelines of RBI were fully complied with.
20. This client was a premium customer of Appellant Bank since opening of above account. He got opened Saving Bank Account bearing No. 021801400006999, in the month of November, 2012. This too was got opened under good faith and strict adherence with KYC norms. This account was with ATM / NEFT facility. This Irfaan Ansari, during his visit in July, 2013 had informed the Branch Operation Manager of the Appellant Bank's Jaipur Branch, that he would be expecting credit on

15.07.2013 and 16.07.2013, some outstanding/ pending amount from Pune, against sale of consignments on account of his various customers, which was due for a considerable period. On 17th July 2013, the said Irfaan Ansari, again came to the Bank and enquired about the credit of some amount in his account from Pune, and it was found that an amount of Rs. 30.00 Lakhs (Rupees Thirty Lakhs Only) was credited to his account, through Internet banking RTGS, from Bank of Maharashtra, Pune at 12.16 P.M. with narration as M/s Suhas Enterprises and subsequently, this Irfaan Ansari was allowed to withdraw Rs. 20.00 Lakhs (Rupees Twenty Lakhs Only) on the same day by using cheque No. 210552, after verifying his PAN card and obtaining a purpose letter from him.

21. Further transactions were made by Irfaan Ansari subsequently, and those were also in good faith and strict adherence with the practice and procedure. But on the same day on 17th July 2013 at 2.45 P.M. information with regard to receipt of Rs. 30.00 Lakhs (Rupees Thirty Lakhs Only), in the account of Irfaan Ansari reported to be fraudulent by the Bank of Maharashtra, Pune and a request for freezing the same was received. Though, no written request or communication was

there till above time, but immediately on receipt of the phone call, the Appellant bank marked debit freeze on both the accounts of Irfaan Ansari i.e. current as well as saving, and only Rs. 4.00 Lakhs (Rupees Four Lakhs Only) could be saved, which was available at that time. RTGS Cell of the Appellant Bank received an email from RTGS Cell of Bank of Maharashtra on instructions from their Hi- Tech Agri Branch, Pune at 3.09 P.M on 17th July 2013 about the above fraudulent transfer of Rs. 30.00 Lakhs (Rupees Thirty Lakhs Only) from their branch to the account of Irfaan Ansari, by a fraudster and the RTGS Cell of the Appellant bank forwarded the said Email to them at 3.17 P.M, and thus, before receipt of any information on the suspicious nature of the transaction, the customer, Irfaan Ansari could manage to withdraw Rs. 26.00 Lakhs (Rupees Twenty Six Lakhs Only), as stated above.

22.The complaint before Adjudicating Officer by Complainant under Section 46 of IT Act, 2000, was against unknown imposter, having unauthorized access, penetration to their bank account maintained in Bank of Maharashtra, Hi- Tech Agri Branch, Pune. On 17th July 2013 and got siphoned fraudulently Rs. 79,26,000.00 (Rupees Seventy Nine

Lakhs Twenty Six Thousand Only) vide 08 transactions, to various accounts held with different Respondents, including the Appellant Bank. The SMS alert facility, provided by Bank of Maharashtra to its subscriber to receive it on registered mobile number for each online transaction, made in that account, was with registered mobile number, of subscriber Complainant and this mobile number was of Vodafone Essar Limited, obtained by that subscriber. There was contention of above Telecom Service Provider that some unknown person, representing himself as Authorized Representative of the Complainant, got SIM Card replaced on 17th July 2013 and activated the same and by using that SIM card, fraudulent transfer of amount of Rs. 79,26,000.00 (Rupees Seventy Nine Lakhs Twenty Six Thousand Only) was got managed. It was the connivance, between Telecom Service provider, in issuing duplicate SIM Card and the Bank concerned, which resulted this fraud.

23. The gross negligence of Vodafone, resulting the blocking of mobile alert of Complainant and 8 fraudulent transactions in siphoning such a huge amount from the Bank account of Complainant, maintained in Bank of Maharashtra, Pune, was established before Ld. Adjudicating

Officer. The failure to take reasonable security and practices by Bank of Maharashtra, Pune, where the account of Complainant was existing, was also established, because no such unusual transaction in a day in the tune of 8 (Eight) transactions, siphoning such a huge amount was communicated, either through telephone, or mobile number to Complainant. But this Appellant bank has been fastened with above adjudged liability.

24. Hence, this appeal is with above prayer for setting aside the impugned order.

25. The same Impugned Order, passed under same Complaint, on same date, by the same Adjudicating Officer, has been assailed by State Bank of India against M/s Suhas Enterprises & Ors in this **Cyber Appeal No. 22 of 2015,** under Section 57 of IT Act, 2000, with a prayer for setting aside Impugned Order, whereby, State Bank of India, present Appellant has been directed to pay Rs. 2,00,000/- (Rupees Two Lakhs Only), as compensation to Complainant within One month of the order, and in case of failure, to pay compound interest @ 12% to be compounded monthly.

26. In brief, the Memo contends that Ld. Adjudicating Officer failed to appreciate facts and law placed before it, and has acted beyond its jurisdiction. He was with no jurisdiction to adjudicate against Appellant, under Section 46 of IT Act. No specific default, on the part of Appellant Bank, was there in the Complaint, nor in the evidence. Rather, Adjudicating Officer let off the Complainant, even after noticing the facts that the Complainant compromised its Internet Banking credentials with its Accountant and didn't use with due diligence, the Maker Checker Facility provided to it by its banker, Bank of Maharashtra. Even it let off Bank of Maharashtra, which was the originating bank and was fully responsible for all the amount suffered by Complainant. A saving account, in the name of Sumit Bablu Singh was got opened with the State Bank of India, Khadra Branch, Brahm Nagar, Sitapur Road, Lucknow on 08.03.2013. This was got opened on producing PAN Card No. EOXPS5580C with Reliance Post-paid bill for Mobile No. 9580621766, as his proof of identity and proof of address, with a duly filled account opening form and photograph pasted over in on 07.03.2013. This Applicant was got introduced by Manju Lata, who was account holder in this bank branch having her Account No. 30769286753, active since 20.05.2009. Hence, this Saving Bank

Account, in the name of Sumit Bablu Singh, was got opened by Appellant Bank, after duly following the norms and procedures including KYC Norms. This account was got credited with amount of Rs.7,95,000/- (Rupees Seven Lakhs Ninety Five Thousand Only) through RTGS No. MAHBH13198100191 dated 17.07.2013 by M/s Suhas Enterprises from its account with the Bank of Maharashtra and this RTGS transaction was only through the Internet Banking facility provided to Complainant customer, having its Unique Customer ID number and Password. For this transfer of any amount online, needed customer to add payee, followed by entering confirmation code, received on the registered Mobile Number and/or registered email ID, as the case may be. Also, as an additional security, before final transfer, the customer also needs to enter certain special digits given at the back of the Bank Debit Card, indentified by unique alphabet.

27.Hence, in the present case, the said internet banking option, and all the security provisions were to be provided by the Respondent No. 2 - Bank of Maharashtra, which was to be used by respondent no. 1, with utmost caution and privacy of its customer ID and password. Sumit Bablu Singh withdrew Rs. 1000/- and Rs. 2000/- from his account,

through ATM at 13.59 P.M and 14.23 P.M on 17.07.2013, then after sought to withdraw the remaining amount Rs. 7,92,000/- (Rupees Seven Lakhs Ninety Two Thousand Only) from his account on the pretext of urgent payment to be made for a land deal, and in utmost precaution Officials of SBI Khadra Branch had initially declined to accept the withdrawal request for Rs. 7,92,000/- (Rupees Seven Lakhs Ninety Two Thousand Only), because of being huge amount. But as the account was with amount credited through RTGS, appellant Bank could not legally refuse the withdrawal of the above amount. Hence, only Rs. 3,00,000/- (Rupees Three Lakhs Only), as part payment, were allowed to be withdrawn and remaining Rs. 4,92,000/- (Rupees Four Lakhs Ninety Two Thousand Only), was saved by bank. Hence, this Appellant Bank deserved appreciation for saving that amount. Rather, it was fastened with liability.

28.The SMS with regard to keeping above amount on hold was subsequently received and was acted upon. But by that time, Rs. 3,03,000/- (Rupees Three Lakhs Three Thousand Only) was withdrawn. All these facts were placed before Adjudicating Officer, but without going those and keeping in mind the no fault of Appellant Bank,

Impugned Order has been passed. Hence, this Appeal with above prayer, for setting aside Impugned Order, is there.

29. As all these **Cyber Appeals i.e., Cyber Appeal Nos. 14, 16, 18 and 22**

of 2015 are against one and common Impugned Order, “in one and common set of facts, in one and common complaint case, against one and common order of adjudication, by one and common Adjudicating Officer, in various Appeals, having one and common parties, in their Memo as well as in initial complaint”. Hence, all these appeals were heard together and a common judgment is being passed, with a direction to keep copies of this Judgment in all these Appeals separately.

30. A common reply to all these Appeals, have been filed by M/s Suhas Enterprises, the Complainant, in all these appeals, with this contention that all above mentioned Appeals have been filed against the Impugned Judgment and order dated 12.01.2015, whereby, Adjudicating Officer, partly allowed the Complaint filed by Complainant, under Section 45, 45A, 46, 61, 72 read with 85 of Information Technology Act, 2000 and directed Vodafone Cellular

Limited to pay damages in the tune of Rs. 10,00,000/- (Rupees Ten Lakhs Only), Dhanlaxmi Bank to pay Rs. 18,00,000/- (Rupees Eighteen Lakhs Only), State Bank of India to pay Rs. 2,00,000/- (Rupees Two Lakhs Only), State Bank of Patiala and Punjab National Bank is to pay Rs. 7,50,000/- (Rupees Seven Lakhs Fifty Thousand Only) to Complainant, in one month of the Judgment, otherwise to pay compound interest @ 12% compoundable per month in addition to above directed amount.

31. Learned Adjudicating Officer, Principal Secretary, Information Technology, Government of Maharashtra, Mumbai had rightly held that all the Respondents had committed violation of various statutory guidelines and instructions issued by Reserve Bank India, in respect of steps to be taken and measures to be adopted by the Bank, and to ensure safe and secure online banking facilities. Service providers were negligent in issuance of duplicate SIM to the fraudsters, without checking the authenticity of the claim or reason for issuance of duplicate SIM. Appellants were responsible for the loss occasioned to the complainant due to their failure to implement security layer, regarding the Bank Account of Complainant and failure to adhere strict and mandatory statutory guidelines and Code issued in this

regard, by Reserve Bank of India, under Banking Regulation Act, 1949 read with Prevention of Money Laundering Act, 2002.

32. Complainant is a registered Partnership Firm, and for its business purpose was having cash credit account with Bank of Maharashtra, Pune, which had provided a login ID and default password to activate online banking facility. All those directions were adhered and after due diligence in this connection, default password was got changed. Online banking facility was being availed by complainant. Precautions were being availed. On 17.07.2013, in the Office, Complainant received a call from the Security Operation Center (SOC) of Bank of Maharashtra, informing about unnatural transaction of high value from his Bank Account. After going through, this was reported instantly with the Bank of Maharashtra, with a request for taking all necessary steps to stop such fraudulent unauthorized transactions from his above account. A request to freeze the amounts, that were unauthorizedly transferred to unknown banks, was also made. It was found that all services, like incoming calls, outgoing calls and messaging service of authorized mobile number of Complainant, were suddenly barred by Vodafone Cellular Limited, Telecom Service

Provider. Despite adhering to all these instructions, issued by Bank of Maharashtra and other undertaking, all necessary due diligence in connection with the activation and operation of online banking facility, with no fault of Complainant, these unauthorized transactions were committed, for which a Criminal Complaint was instantly got lodged on 17.07.2013, at Police Station at Pune.

33. A complaint, under Section 43, 43A, 46, 61, 72A, read with Section 85 of IT Act, was got lodged before Ld. Adjudicating Officer, Principal Secretary, Information Technology, Mumbai as Case No. 26 of 2013, against the Telecom Service provider as well as Bank of Maharashtra, Pune, inter alia, claiming damages by way of compensation on amount of **Rs.56,95,000/-**, with a cost of this proceeding in the tune of Rs. 11,30,000/-. It was established by Complainant, before Adjudicating Officer, that there is a failure on part of Telecom Service Provider, as well as Respondent Bank to follow and ensure compliance of Master Circular on KYC/Anti Money Laundering Standards/Combating Financing of Terrorism/ Obligation of Banks under Prevention of Money Laundering Act, 2002. With failure on behalf of Vodafone

Cellular Limited, to follow necessary safe-guards while issuing duplicate SIM Card and blocking initial SIM Card of the Complainant.

34.The Banks, from whom, those money were withdrawn, were subsequently, added as Respondent in above Complaint and all those answering respondents were given notice for filing their reply. They all appeared and filed their reply, denying the claims raised by Complainant. All the replies were nothing more than a bald statement that all rules and procedures were adhered and complied with. Adjudicating Officer, after considering the facts and circumstances placed on record, held the defiance of Master Circular Letter, as well as directions by Telecom Service Provider. Thereafter, Complaint was partly allowed, and Telecom Service Provider, Vodafone and Banks were directed to make compensation payment, as per above total amount in the tune of Rs. 45,00,000/- (Rupees Forty Five Lakhs Only).

35.Vodafone Cellular Limited had given Mobile Cell connection to Complainant and undisputedly, it was a registered mobile number for the cash credit account of Complainant, being maintained with Bank of Maharashtra, Pune. It is undisputed fact that M/s Vodafone Cellular Limited, had blocked the SIM issued to the Complainant and a

duplicate SIM for the same number, was got issued and it was without any security verification, whatsoever. A normal practice, before issuing a duplicate SIM Card, on the ground of its lost of previous one, a report at Police Station is a condition precedent, for entertaining subsequent application, for replace/reissue the same. There is nothing on record to show, any such requirement has been adhered with. Even the simple comparison of the signature on the copy of request form, for issuance of duplicate SIM and the signature on CAF form, would show that two signatures are at quite different. This basic exercise was not made, which was very well apparent on the face of it and a duplicate SIM was issued to fraudster. The original SIM Card was issued at Pune, while duplicate was issued at Nasik and registered address of business place of Complainant was of Pune, having no record of Nasik. It itself raised suspicion while issuing duplicate SIM card and owing to this issuing and the nexus between blocking of SIM Card, enabling Complainant not to have SMS alert, this unauthorized financial transaction from the complainants account, thereby siphoning huge amount could be successful.

36.State Bank of India, was to adhere with the guidelines given in Master Circular KYC Norms dated 02.07.2012, but it failed to obey. Sumit Bablu Singh, approached State Bank of India, got his account open and on the day money was transacted through RTGS in his account, two times money was withdrawn from ATM and subsequently, it was got withdrawn in a huge amount in one transaction. Though in previous, annual income status of Sumit Bablu Singh was Rs. 1,80,000/- (Rupees One Lakhs Eighty Thousand Only) and that in one single day, there was deposit of Rs. 7,95,000/- (Rupees Seven Lakhs Ninety Five Thousand Only) and withdrawal of this huge amount. It was never taken care of, whereas, for allowing to withdraw Rs. 3,00,000/- (Rupees Three Lakhs Only) in one stroke that too in cash, there was additional precaution to be taken, so far as cash withdrawn was being permitted.

37.State Bank of Patiala, while opening account of Mr Saurabh Pandey, failed to adhere KYC Norm. No credentials of said Saurabh Pandey was verified or cross checked. Nor the address of Saurabh Pandey was physically checked. Due diligence as per clause 2.4A RC was not carried out by this Bank.

38. Merely account opening form and the account statement is sufficient to show that various suspicious transactions have been carried out, both in the form of deposit as well as withdrawal from the said account. Monthly income of the said Saurabh Pandey was said to Rs. 20,000/- (Rupees Twenty Thousand Only) and in one single day there was deposit of Rs.9,50,000/- (Rupees Nine Lakhs Fifty Thousand Only). It itself raise suspicion and the withdrawal of that Rs. 9,50,000/- (Rupees Nine Lakhs Fifty Thousand Only) was also of full of suspicion. The authorities were never reported regarding such negligence.

39. Dhanlaxmi Bank too, failed to adhere with Master Circular regarding KYC norms. Even failed to obtain very basic information while opening the account of said Irfaan Ansari. No credentials were got verified or cross checked. Due diligence was also not adhered. Account opening form, states the monthly income of said Irfaan Ansari to be Rs. 40,000/- (Rupees Forty Thousand Only). Anticipated level of transaction was Rs. 5,00,000/- (Rupees Five Lakhs Only) yet, in one and single day there was deposit of Rs. 30,00,000/- (Rupees Thirty Lakhs Only). It itself raised suspicion and withdrawal of Rs. 20,00,000/- (Rupees Twenty Lakhs Only) of it, was with all suspicion and

connivance with no report to appropriate authorities of these unnatural transaction. Account Statement itself shows that pre 17.07.2013 transactions were always less than of Rs. 1,00,000/- (Rupees One Lakh Only) and suddenly on 17.07.2013, Rs. 30,00,000/- (Rupees Thirty Lakhs Only) were put in the account, and it were got withdrawn with huge amount.

40. There was blatant defiance of guidelines on Information Security, Electronic Banking Technology, Risk Management and Cyber Fraud, dated 29.04.2011. Banking Codes and Standard Board of India had issued Code of Bankers Commitment to the customers, which limits the extent of losses to a maximum of Rs. 10,000/- (Rupees Ten Thousand Only) for a customer. There had been security lapses by Bank of Maharashtra where Complainant was having its cash credit account operated. Bank of Maharashtra, Pune had blatantly violated various modifications, circulars, guidelines, instructions issued by Reserve Bank of India. The Adjudicating Officer has rightly appreciated the facts and evidences placed on record.

41. Section 43A of Information Technology Act, empowers the Adjudicating Authority to decide such cases, and pass appropriate orders in this regard, which was availed by Adjudicating Officer in Impugned Order, well in its jurisdiction. Hence, all these Appeals were prayed to be dismissed.

42. Having heard Learned Counsels of both side, and gone through record, it is apparent, that the facts of the Complaint filed before Adjudicating Officer, as Complaint No. 26 of 2013, is one and common, written as above. But, the same is being reiterated in brief, that Complainant, being a Registered Partnership Firm of Shri Suhas Mankame and Smt. Surekha Dekate, as its partner, was holding cash credit account with Bank of Maharashtra, Hi- Tech Agri Branch, Pune, wherein online banking service facility, with registered Mobile No. xxxxxx0825 of Complainant was provided by Vodafone Essar Limited and this was given as mobile number of Complainant in its above banking transaction account. On 17.07.2013, Complainant received a call from Security Operation Center of Bank of Maharashtra, Head Office at Pune and branch office Hi- Tech Agri Branch, Pune, informing above transactions of high value, through the Complainant's account. Branch

Manager of Bank of Maharashtra, Hi- Tech Agri Branch, Pune was instantly requested about this call and to take necessary steps and to stop such fraudulent transactions. Complainant, also submitted a letter to freeze the amount, where the money was transferred.

43. On 17.07.2013, all services like incoming call, outgoing call and text messages service of mobile number XXXXXX0825 were suddenly barred by Telecom Service Provider, Vodafone Essar Limited and upon complaint on the day, this was reported to be due to technical error in SIM Card. Hence, a request for new SIM Card on the same day was raised. It was found that Vodafone Essar Limited, without verifying details of unknown person, had issued new SIM Card and blocked the mobile phone of Complainant, unauthorizedly, enabling that third person to penetrate into Complainant's account and fraudulently transfer amount 79,26,000.00 (Rupees Seventy Nine Lakhs Twenty Six Thousand Only) vide 8 transactions to various accounts, held with different Respondents. A complaint was got lodged instantly on the same day of 17.07.2013 with Police Station Datta Wadi, Pune as well as Cyber Cell, Pune Branch.

44. This Complaint before Adjudicating Officer was also got filed on 6th September 2013, wherein, Interim Order was issued on 14.10.2013 and 29.10.2013, to release the frozen amount available with Respondent Nos. 4, 5 & 6. Rs. 79,26,000.00 (Rupees Seventy Nine Lakhs Twenty Six Thousand Only) was fraudulently transferred from Complainant's Account, was only with Rs. 31,26,000/- (Rupees Thirty One Lakhs Twenty six Thousand Only) recovered by freezing by Maharashtra Bank, Pune. Hence, compensation of an amount of Rs. 56,95,000/- (Rupees Fifty Six Lakhs Ninety Five Thousand Only) from all the Respondents with interest @ 13.5% Per annum from the date of Complaint, till actual realization plus Rs. 11,30,000/- (Rupees Eleven Lakhs Thirty Thousand Only), towards the cost of proceeding and fees of Rs. 1,41,600/- (Rupees One Lakh Forty One Thousand Six Hundred Only), which was paid through demand draft, was claimed. The notices were issued to all the opposite parties, and they had filed their reply with the same contention written in their memo of appeals, narrated at above.

45. Learned Adjudicating Officer, after hearing arguments of both side, came to conclusion that Respondent No. 1 and 2 i.e., Bank of Maharashtra Head Office and Bank of Maharashtra Hi tech Agri

Branch, Pune were quite proactive in this case. The fraud was brought to the notice of the Complainant by their Security Operation Center. They informed the complainant that large amount of fund is taken out from the Complainant's bank account. Respondent No. 4, Dhanlaxmi bank had been extremely lax with its procedures. Huge sum of Rs. 30,00,000/- came into fraudster's account and within 15 mins, it allowed Rs. 20,00,000/- to withdraw in cash, which speaks of not only negligent, but also complicity. All other Respondent Banks have also failed to adhere strong KYC norms to prevent cyber crimes and also violated circular regarding Money Mule Accounts by not taking sufficient precautions in this regard. Hence, an order was to pay by Respondent No. 4 (Dhanlaxmi Bank), Respondent No. 5 (State Bank of India), Respondent No. 6 (State Bank of Patiala) and Respondent No. 7 (Punjab National Bank), damages to the tune of Rs. 18,00,000/- (Rupees Eighteen Lakhs Only), Rs. 2,00,000/- (Rupees Two Lakhs Only), Rs. 7,50,000/- (Rupees Seven Lakhs Fifty Thousand Only), and Rs. 7,50,000/- (Rupees Seven Lakhs Fifty Thousand Only) respectively by way of compensation to the Complainant within a month of above order, failing which compound interest @ 12% compoundable per month was to be paid. Vodafone i.e. Respondent No. 3 was held to

have committed failure to take reasonable Security Practices and Procedure, with defiance of established guidelines, before issuing duplicate SIM Card and permitting to access sensitive personal data and information of the Complainant, to an authorized person, resulting this wrongful loss to the Complainant and held liable under Section 43A of the IT Act, with a direction to pay damage in the tune of Rs. 10,00,000/- (Rupees Ten Lakhs Only), by way of compensation to the Complainant, with interest of 12%, per month compoundable.

46. The very objection, raised before Adjudicating Officer and before this Appellate Tribunal, by Appellant Vodafone India Ltd., relates with this contention that it was not holding any sensitive personal information, the unauthorised access of which has caused any wrongful loss to the complainant. It had never been negligent in implementing and maintaining reasonable security practices and procedures, prescribed by Section 43A of IT Act, 2000, read with Rule 8 of Rules, in respect of any computer resource, which it owns, controls or operates. Rather, Appellant acts as merely a conduit between two parties and it had only acted as a conduit between complainant and its Bank, providing net banking. It was with a limited role of facilitation of services to its

subscriber and customers. But Ld. Adjudicating Officer failed to consider the submissions made before it and it was very well objected there at that complaint was not maintainable against any Telecom Service Provider. To bring a case under Section of 43A of the IT Act, a complainant must show that there was a sensitive personal data or information, being possessed, handled or dealt with by Telecom Service Provider. Whereas, it was categorically denied in its reply before Adjudicating Officer. The cellular service, provided by Appellant, involves carriage of voice and data of its subscribers, from one end to another, within or outside its network. For this purpose, the service provider is required to establish a cellular mobile network, which comprises of a Mobile Switching Centre that is, simply a brain of network and this Mobile Switching Centre is connected to Base Station Controllers, located across the service area, either through wireless signals, emitted through the cellular antennas, installed by various service providers, at both the ends, or through optical fibers, and this Base Station Controllers are connected to Base Trans-receiver Stations (BTS), located at different locations, either through wireless signals emitted through cellular antennas, installed at both the ends or through optical fibres. It is these BTSs, whereupon antennas are

installed, which emit and receive wireless signals, to and fro, between a person availing Cellular Mobile Telephony Services, through its Subscribers Identity Module Card (SIM card), which is inserted/installed in the handset by subscriber.

47. The same defence was there in the same words in previously decided Cyber Appeal No. 5 of 2018, Vodafone Idea Limited vs. Shri Sandeep Singhal and another, as well as decided by this Tribunal itself, in Cyber Appeal No. 6 of 2014 Vodafone India Ltd. vs. Mr. Prashant Mahadeorao Buradkar And Ors, each of the point of defence, taken in reply, before Adjudicating Officer in above complaint, filed by Mr. Prashant Mahadeorao Buradkar and others, before same Adjudicating Officer and raised before this Appellate Tribunal, were alike to the present appeal and these legal questions have been decided by the then Appellate Tribunal, as well as present Appellate Tribunal, by an elaborate and considered judgment.

48. Accordingly, all these issues raised, are settled by this Tribunal, holding the position that Telecom Service Provider i.e. Vodafone, in present Appeals, controls and operates SIM card carrying the customer's personal data and information, which, in mobile

technology driven world, facilitates personal business and financial transaction process.

49. The full form of SIM card suggests that it is Subscribers Information Module, thereby meaning that the entire information of the subscriber is controlled by the same. The entire business of the mobile operators critically depends on use of vast amount of data both, personal and business related, transacted over mobile platform, and constitutes the core of the profits of these operators. The customers are using mobile phones to facilitate their business and to share sensitive business data and information related to their business activities. The sensitive personal data and information, in the present case, is the SIM card along with the proof of identity, signature and alternate phone number of the customer that are fed in the system database of Telecom Company. Appellant, Telecom Company collected the sensitive and personal information from the complainant/subscriber/customer, before any services, post-paid or pre-paid, are provided. Telecom Company is the custodian of such sensitive and personal information, which includes photo identification, signature, alternate phone number, etc., of the customer and the above mobile number was got deactivated

suddenly. The SMS alert could not be received by complainant and this huge siphoning by unauthorised access to the bank account of complainant was there. It was fully proved that the Telecom Company was negligent in issuing the replaced SIM card to the fraudsters by allowing the access to the sensitive personal data and information, provided by complainant, at the time of obtaining its mobile number. It was held in those previously decided appeals, wherein, likewise present one, Adjudicating Officer had held that there was direct nexus between blocking of SIM card of the complainant and issuance of duplicate SIM card to the fraudsters, resulting unauthorised financial transaction from the account of complainant. This Appellate Tribunal had categorically held that the importance of mobile number for use in financial transactions and other sensitive transactions is growing by leaps and bounds and it is not a secret to Telecom Service Provider, like Vodafone. They earn huge revenue from such very use of mobile phones. The significance of SIM or a duplicate SIM can best be understood by such service provider.

50. In this particular case, bank established that not only bank transaction alerts, but even OTP were sent to registered mobile number, but in

fact, it went to the duplicate SIM card holder, 'fraudster' and this duplicate SIM card was managed to be issued, purely on account of negligence, boarding on connivance and laxity in maintaining reasonable security measures and practices, and by ignoring the standard procedures for verification of documents, for replacement of SIM card with the original documents and the data available in CAF of original SIM owner. But if such duplicate SIM was not issued to the fraudsters, the unauthorised financial transactions were not possible. The fraud could still be prevented had Vodafone not blocked the original SIM card of the complainant, without contacting original SIM owner.

51. This prevented the complainant from getting alerts in respect of unauthorised transactions from the bank account. The security measure of Vodafone was hopelessly inadequate. Hence, Vodafone was liable under Section 43(g) and 43A of IT Act and this law held by this Tribunal repeatedly stands good regarding the facts and circumstances of the present Cyber Appeal. The Adjudicating Officer had held liability of Vodafone India Ltd. on the basis of facts and law placed before it on record.

52. There is nothing erroneous, requiring any interference by this Appellate Tribunal. Accordingly, **Cyber Appeal No. 14 of 2015** merits its dismissal with costs.

53. The Adjudicating Officer has held that respondent nos. 1 and 2, i.e. Bank of Maharashtra, Head Office, Pune and its Branch Office Hi Tech Agri Branch, Pune was pro active in the case. And this fraud was brought to the notice of complainant by their Security Operation Centre. By informing complainant that large amount of funds was taken out from the complainant's bank account and this fraud came in the light on the basis of this vigilance of that bank, which instantly on the same day of occurrence, communicated the complainant and this action was taken into the motion. No appeal by Bank of Maharashtra is there. Hence, with regard to liability or negligence of this bank, no comment is required to be made by this Appellate Tribunal.

54. So far as respondent no. 4, i.e. Dhanlaxmi Bank, is concerned, it is very well apparent on the basis of pleadings, as well as evidence, and in the argument that in one stroke, Rs. 30 lakhs were transacted in account of Irfan Ansari and this was through RTGS at 12.16 pm on 17.7.2013.

Rs. 20 lakhs were withdrawn on the same day within 16 minutes. This unusual transaction was permitted by the officer of Dhanlaxmi Bank without adhering to KYC norm to prevent cyber crimes as well as circular regarding Money Mule A/c by not taking sufficient precaution in this regard. There was a communication received with regard to fraudulent RTGS by Dhanlaxmi Bank on the same day of transaction by 3.30 pm. But, in between, huge money was siphoned. This itself was unusual transaction, nor cared or interfered by bank. The judgment of Adjudicating Officer is in accordance with the law and facts, placed before it, and merits, no interference by this Appellant Tribunal.

55. The very argument of learned counsel for State Bank of Patiala was that an instant action was taken after having the freeze request, but the amount lying could only be freezed and subsequently, transferred. Learned Adjudicating Officer has held about the KYC norms and Anti Money Laundering Standards, Combating of financing of terrorism/Obligation of Banks under PMLA, 2002 with Master Circular issued to banks regarding above subject, on 2nd July 2012 and it was there that appellant banks were at failure with violation of para 2.8 of

the circular, regarding money mule account, by not taking sufficient precautions in this regard.

56. Withdrawal of huge amounts from the mule accounts in a short period after receipt of money through RTGS, and withdrawal in form of cash, without any suspicion or taking of action, as per guidelines, sensing fraud in net banking, is apparently there on record. The transactions recorded in statement of account of those account holders, through which money was siphoned, reveals that their annual income range and the mode of operation, previous to that fraudulent withdrawal, were entirely unusual than the fraudulent withdrawn. There was no consonance at all, which can be said to be of not any nature creating any suspicion, but no suspicion with regard to fraud or action regarding fraud suspected to be, given in above guideline, was taken by concerned bank authorities. Rather, cash withdrawal, much above the prescribed limit from those mule accounts was permitted. Hence, the argument raised by learned counsels for banks are of no support in their contention, rather the judgment of Adjudicating Authority, impugned in these Appeals, were in accordance with law and facts, placed before Adjudicating Officer.

57. Hence, all Appeals merit their dismissal with costs.

58. Accordingly, all these Cyber Appeals are being dismissed with cost.

59. Let a copy of this judgment and order be kept in all the files of Cyber Appeals separately.

25.9.2024
/NC/



.....
(Justice Ram Krishna Gautam)
Member