TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL

NEW DELHI

Dated 12th September 2024

Cyber Appeal No. 6 of 2014

Vodafone India Limited …Petitioner(s)

Vs.

Mr.Prashant Mahadeorao Buradkar And Ors …Respondent(s)

Cyber Appeal No. 7 of 2014

State Bank of India …Petitioner(s)

Vs.

Mr Prashant Mahadeorao Buradkar and Another …Respondent(s)

BEFORE:

HON'BLE MR. JUSTICE RAM KRISHNA GAUTAM, MEMBER

Cyber Appeal No. 6 of 2014

For Petitioner : Mr.Meet Malhotra, Sr. AdvAlongwith Mr Kaushik Moitra, Ms SubhalaxmiSen,

Ms Romi Kumari, Mr Ravi S S Chauhan,

Ms Pallak Singh For Vodafone Idea Ltd.

For Respondent : Mr.Diggaj Pathak, Ms Shweta Sharma,

Ms Vaibhavi Pathak, Mr Tanmay Dhari Sinha, Ms Shubhangi Tiwari, Mr Rakshit Singh, Ms Megha Sawani & Ms Alisha Ahuja For R-1

Mr Karn Kumar For R-2 For SBI

Cyber Appeal No. 7 of 2014

For Petitioner : Mr.Karn Kumar For SBI

For Respondent : Mr.Diggaj Pathak, Ms Shweta Sharma,
Ms Vaibhavi Pathak, Mr Tanmay Dhari Sinha,
Ms Shubhangi Tiwari, Mr Rakshit Singh, Ms Megha Sawani & Ms Alisha Ahuja For R-1
Mr Meet Malhotra, Sr. Adv alongwith
Mr Kaushik Moitra, Ms Subhalaxmi Sen
Ms Romi Kumari, Mr Ravi S SChauhan, Ms Pallak Singh For Vodafone Idea Ltd. For R-2

JUDGMENT

1. This **Cyber Appeal No. 6 of 2014**, under Section 57 (1) of the Information Technology Act, 2000, read with Rule 3 (1) of Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000, has been filed by Appellant, Vodafone Idea Limited, against Prashant Mahadeorao Buradkar, State Bank of India, General Manager, Local Head Office, Mumbai, as well as State Bank of India, Branch Manager, Mahal Nagpur Branch, near Khadi Gramodyog, Nagpur, before the Cyber Appellate Tribunal, New Delhi, against Order dated 18.02.2014, passed by Shri Rajesh Aggarwal, Adjudicating Officer(AO), Principal Secretary, Information Technology, Government of Maharashtra, in

Cyber Complaint No. 14 of 2013, with this contention that Respondent No. 1, complainant, was a subscriber of Appellant i.e., Vodafone India Limited (VIL), a public limited company, having its registered office at Vodafone India limited, Peninsula Corporate Park, Ganpatrao Kadam Marg, Lower Parel, Mumbai 400013. Appellant is a Cellular Network Service Provider and a licensee under Unified Access Service License, duly licensed by the Department of Telecommunications, Government of India, to provide mobile telephony services in the relevant service area. Being aggrieved by the impugned order passed by Adjudicating Officer, in Complaint No. 14 of 2013, i.e., order dated 18.02.2014, whereby Appellant had been directed to pay compensation to the tune of Rs. 6,00,000/- (Rupees Six Lakhs only), payable to Complainant/ Respondent No. 1, this appeal is with a prayer to set aside, the Impugned Order.

2. Respondent No. 1, an individual subscriber, since 2007, was with a Customer Agreement Form (CAF) entered by it with Appellant. At the time of registration, driving license, employment letter and salary slip, as document, for establishing identity and proof of residence, were filed. Those are **Annexures A-3** & **A-4** collectively. On 23.07.2011, one person, holding himself out as Mr Kaustubh Das, the authorized

representative of Complainant/ Respondent No. 1, having authorization letter from Mr Prashant Buradkar, visited the Vodafone store at Vashi and requested for replacement of the SIM card. Upon his request and on receipt of SIM replacement request in prescribed form, along with authorization letter, it was duly processed and a new SIM, bearing Number 12301460177, was provided to that person. On the same day i.e., 23.07.2011, the new SIM, bearing No. 12301460177, was got activated. True and correct copies of the SIM Replacement Form, with other submitted documents, were **Annexure A-5** colly. Respondent No. 1/ Complainant, admitted in his complaint that person who requested for replacement of SIM on the aforementioned date, was an imposter. Respondent No. 1 visited Vodafone store at Vashi on 26.07.2011, with a request for replacement of SIM and upon this request for replacement of SIM, in prescribed form, along with requisite documents of the subscriber (**Annexure A-6** colly), the request was duly processed and a new SIM was provided to person who visited the store and this was got activated on 26.07.2011. On 24.09.2011, Appellant received a request for furnishing information under Section 91 of Code of Criminal Procedure, 1973, from the Police Officer, Rabale Police Station, Navi

Mumbai, with respect to Complainant/Respondent No. 1. This request is **Annexure A-7**. On 11.10.2011, the Appellant submitted the information, as requested above, to the Inspector of Police, Rabale Police Station, Navi Mumbai, which is **Annexure A-8** to memo. Complainant/ Respondent No. 1, on 02.07.2013, lodged a complaint with Learned Adjudicating Officer, bearing Complaint No. 14 of 2013 under Section 43, 43A, 46 and 61 of the Information Technology Act, 2000, with this grievance that Appellant had failed in the performance of its obligation under the IT Act, causing an illegal siphoning of Rs. 10,50,000/- (Rupees Ten Lakhs Fifty Thousand only), from the bank account of Respondent No. 1, maintained with Respondent No.3, i.e., State Bank of India, Mahal Branch, Nagpur. This complaint was replied before Ld. Adjudicating Officer, and finally Impugned Order dated 18.02.2014, was passed, against which this appeal, with contention that impugned order had been arrived at finding, with observation which had never been alleged by the Respondent, and it had never been subject matter of adjudication, before Ld. Adjudicating Officer. Repeated breach of Section 43, 43A, 46 and 61 of the IT Act, by Appellant, was said in the complaint. Whereas, the allegation was with regard to siphoning of Rs. 10,50,000/- (Rupees Ten Lakhs Fifty

Thousand only) from the bank account of Respondent No. 1, maintained by Respondent No. 3. Whereas, Ld. Adjudicating Officer was with jurisdiction under Section 43A of IT Act, read with Section 46, restricted to the 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 the IT Act, 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 it owns, controls or operates.

3. The jurisdiction to adjudicate for any non compliance with subscriber verification by Appellant, falls within the jurisdiction of Department of Telecommunication, pursuant to the terms and conditions, of License Agreement, and that the Department of Telecom is the appropriate authority to decide and adjudicate upon the issues of failure in verification and imposing consequent penalties, if any. Ld. Adjudicating Officer did not have the jurisdiction in respect of above cause of action, which falls squarely within the domain of Department

of Telecom. Further, it is a settled position of law that in the cases, where there is a special legislation or regulation governing any activity, the deviations, if any, must be seen in the light of such special regulations. Hence, the impugned order is against the settled proposition of law.

4. The Appellant was not holding any sensitive personal information, the unauthorized access of which has caused any wrongful loss to Respondent No. 1 and second, not negligent in implementing and maintaining reasonable security practices and procedures, as prescribed by Section 43A of the IT Act read with Rule 8 of the Rules, in respect of any computer resource which it owns, controls or operates. Rather, Appellant acts as merely a conduit between two parties. In the instant case, the Appellant had only acted as a conduit between Respondent No. 1 and Respondent No. 3. He was with a limited role of facilitation of services to its customers. But Ld. Adjudicating Officer failed to consider the submission of Appellant on the ground of maintainability of above complaint. To bring a case in respect of Section 43A of the IT Act, the Complainant was must to show that there was a sensitive personal data or information being processed handled or dealt with by the Appellant. Whereas, it was

categorically denied in its reply before Adjudicating Officer. The Cellular Services, provided by Appellant, involves carriage of voice and data of its subscribers from one end to other, 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 Center i.e., simply a brain of network and this Mobile Switching Center 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 the 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 fiber. It is these BTSs, where upon antennas are installed which emit and receive wireless signals to and fro, between a person availing Cellular Mobile Telephony Services through his Subscribers Identify Module Card (SIM Card), which is inserted/ installed in the handset by subscriber.

5. The Appellant Company is a licensee of the Government of India, as a Unified Access Service Provider, in the State of Maharashtra & Goa, with effect from 06.11.2008 and it was with function to be governed

by the provisions of the Indian Telegraph Act, 1885, India Wireless Telegraphy Act, 1933, as well as Telecom Regulatory Authority of India Act, 1997. Under the said License, the Appellant Licensee is authorized to provide the Voice, Non Voice and Video Conference facilities. Access Service Provider can also provide Internet Telephony, Internet Services and Broadband Services. If required, access service provider can use the network of NLD/ ILD service licensees. The role of Appellant Company i.e., Telecommunications Service Provider, was restricted to providing access to its network, to the subscribers of such Telecom Service Provider for the purpose of transmitting messages in real time and other than in relation to a transitionary period. Such messages are not saved or stored on any computer resource owned or operated by the Appellant. Rather, Appellant does not have any access to the content of the messages (voice or text), being transmitted over its network and it neither stores, nor possesses, nor handles, nor deals with the content of the messages being transmitted over its network. The provision of Section 43A of IT Act, only attracted in relation to a body corporate possessing, dealing or handled in sensitive personal data or information. Therefore, Appellant does not have any access to the sensitive personal data or information, in the

course of its function to provide the Services, under the License granted to it, by the Department of Telecommunications. It cannot be said to be possessing, dealing or handling any information, whatsoever, to bring it within the area of Section 43A of Information Technology Act. Ld. Adjudicatory Officer had failed to recognize that the Respondent No.1/Complainant had not made any specific averment in their complaint, as regard to any breach of the Appellant's duty to implement and maintain reasonable security practices and procedures. Hence, there was no violation of Section 43A of the IT Act.

6. Reasonable security practices and procedures, as contemplated by the Information Technology Act, 2000, are in relation to the computer resource, which in the case of Appellant is its network and do not include the subscribers verification process at the time of issuance or re-issuance of SIM cards. Whereas, as per Rule 8, Body Corporate shall be deemed to have implemented and maintained reasonable security practices and procedures, if it had implemented and maintained the ISO 27001 standards for network security and Appellant had always complied with the Network Security Conditions. Hence, it was never negligent in implementing and maintaining the reasonable security

practices and procedures. There was no linkage, nor any proof between fraudulent transactions and negligence being alleged against the Appellant, in implementing the Network Security Conditions for Section 43 of IT Act, a specific averment that any of the acts under Section 43 (a) to (j) have been undertaken, without the permission of the owner or any other person in charge, of a computer, computer system or computer network, is to be levelled. Whereas, in the present case, Appellant, being a Service Network provider, is the owner/ person in charge and a complaint under Section 43 (g) cannot be made against the owner of the computer, computer system or computer network. There was no allegation in complaint with any specific averment in respect of any act given under Section 43 (a) to (j), being said to have occurred in respect of Service Network. Under Section 43 A of the IT Act, 2000, the Respondent No.1 establish, firstly, the Body Corporate, which is possessing, handling or dealing in sensitive personal data or information in its capacity, as owner, controller or operator of the computer resource, has breached in its duty to implement and maintain the reasonable security practices and procedures. Secondly, such breach of duty, has resulted in wrongful gain or loss, pursuant to the unauthorized access/ use of the sensitive

personal data or information and finally, such wrongful gain or loss, is attributable to the breach of the duty to implement and maintain the reasonable security practice and procedure, in respect of the computer resource in which the Body Corporate possesses, handles or deals with sensitive personal data or information. But it was never averred with regard to Appellant and its service network or conditions of its license, given in License Agreement for Unified License.

7. The present dispute pertains to fraudulent online money transactions. But Ld. AO has appreciated erroneously and had given a complete go by to the settled principles of attribution of liability. The impugned judgment was based on assumption and apportionment of liability between Appellant and Respondent no. 2, herein. Whereas, criminal trial for the same offence, in question, is still pending on the basis of charge-sheet bearing R.C.C. No. 564/ 2012, pending before Learned Trial Court. Respondent have specifically admitted in the pleading that the only inconvenience caused to Respondent No. 1, was the alleged non-receipt of intimation of the transfers, from the alleged bank account, maintained with Respondent No. 3 and impugned order has been passed on it. Whereas, one time password was to be given by complainant itself. At the outset, it is submitted that the

complainant have failed to first and foremost establish and prove that the entire wrongful loss caused to him was on account of the unauthorized access to the one time password. Appellant doesn't deal handle or possess the sensitive personal data or information, the unauthorized access of which has resulted in the alleged wrongful loss to the Respondent, was of no concern with appellant. Even if, Appellant inadvertently issued/replaced SIM Card to an alleged imposter, such replacement doesn't in any manner amount to assistance, which requires an overt intentional act, on part of any person alleged to be assisting. Mere access to a SIM Card, which continues to be a property of the Appellant, facilitates an access to a computer, which is owned by the Complainant, or which the Complainant is in-charge of, was to be proved by Complainant. But it was not proved so. Appellant is an 'intermediary', as defined in Section 2(1)(w), of the IT Act, and he, in its capacity, as a 'Telecom Service Provider', falls squarely, within the aforesaid definition. He is under exemption category as per Section 79 of Chapter XII. Appellant had observed due diligence in the matter, while discharging its duties and it had acted in good faith. An inconvenience caused to the Complainant/ Respondent No. 1 on account of deactivation of telecom

services to the SIM Card inserted in the handheld device of Respondent No.1, resulted his inability to receive intimation at the time of alleged unauthorized transfer of funds from the bank account, maintained with Respondent No. 3 and Appellant is not responsible for it. But Ld. AO has failed to appreciate it.

8. Verification of subscriber, at the time of replacement of SIM, is a reasonable security practice or procedure, and the Appellant is actually proved to have been negligent in such verification, even then Ld. AO has failed to identify the nature of the sensitive personal data or information possessed, handled or dealt by the Appellant, which had resulted in the loss or the negligence on the part of Appellant, resulting wrongful loss suffered by Respondent No.1. The damages awarded was not corresponding to actual loss and cause of negligence alleged against Appellant. The apportionment on the basis of contributory negligence was also not in consonance with the settled proposition of law. It was the Complainant/ Respondent No. 1, aware of User ID, Password, Transaction Password, Security Grid given to it and without this, siphoning may not be possible. Hence, it was the negligence of Respondent No.1, which resulted such fraud. Hence, this appeal, within the jurisdiction of this Tribunal, under the period of

Limitation, with a prayer for setting aside the impugned order, dated 18.02.2014 of Ld. Adjudicating Officer, passed in Complaint No. 14 of 2013.

9. The Complaint No. 14 of 2013 was filed before the Adjudicating Officer, Mumbai at Mumbai by Mr Prashant Mahadeorao Buradkar against State Bank of India, Head Office, Branch Office and Vodafone India Limited, under Section 43, 43A, 46 and 61 of Information and Technology Act, 2000, with a claim of damages, amounting to Rs. 10,50,000 /- (Rupees Ten Lakhs Fifty Thousand Only), with interest of 9.5%, from the date of incident, till date of adjudication, as well as pendentelite and future interest, till actual date of realization, with this contention that Complainant was having his Savings Joint Account in State Bank of India, Branch Office i.e., Respondent No. 2, in the name of him and his brother Mr Pravin Buradkar, as Saving Account No. 10483092588. Respondent No. 1, is a Nationalized Bank, offering banking services, having its Local Head office and Branch Office, Respondent No. 2 at Mahal, Nagpur. This Respondent No. 1 and 2 uses computer resource, under his control, and operate operation for its banking services. Respondent No. 3 is a prominent Cellular Company,

for the purpose of its business, using computer resource under its ownership, control and operation.

10. Complainant had its cell phone No. 9819026356 from Respondent No. 3. Online banking facility was got activated with Respondent Nos. 2 and 3 by Complainant. It was being availed by Complainant, as per manual instructions, given in usual guide with a secured online transaction, with a frequent change of password with all security measures. Complainant's brother Mr Pravin Buradkar had never used internet banking. Registered mobile no. 9819026356 of Respondent No. 3 was given by Complainant to his bank service provider i.e., Respondent No. 2, to get update on online activities and transactions from his account. On 23.07.2021, complainant's SIM with above mobile number, which was controlled by Respondent No. 3, was suddenly got deactivated. Complainant immediately called upon the call center of Respondent No. 3, at around 07.00 P.M., on the same day. Enquiry was made with regard to said deactivation of above mobile number, and it was explained by customer care representative that due to some technical error in the SIM card, it must have been deactivated. Hence, it be got replaced from nearest Respondent No. 3 gallery. As it was Saturday and Sunday, the next day complainant was

unable to go the Respondent No. 3 gallery. On 26.07.2011, Complainant went to Respondent No. 3, Vashi gallery to change the SIM Card and issuance of new SIM Card, which was got done. Subsequently, this card was got activated and on 30.07.2011, it was transpired that fund were missing. It was instantly intimated to Respondent No. 2, through phone and email, about illegal online transfer. Complainant was transpired that from 24.07.2011 till 26.07.2011, total 27 transactions of Rs. 10,50,000/- (Rupees Ten Lakhs Fifty Thousand only), have taken place in his account. It was by some unknown person, having unauthorized access to the Respondent Nos. 1 and 2 computer system, resulting penetration and siphoning from Complainant's Saving Account No. 10483092588. On 23.07.2011, some unknown person, got deactivated the complainant mobile and issued a duplicate SIM Card, issued by Respondent No. 3 at its Vashi Gallery, without due verification with no information to Complainant. When he called to Respondent No. 3, Call center on 23.07.2011, for enquiring about deactivation of his mobile number and on 26.07.2011, when a new SIM card was reissued to the Complainant, it was a gross negligence of Respondent No. 3, resulting loss of Rs. 10,50,000/- (Rupees Ten Lakhs Fifty Thousand Only) to complainant. A

criminal complaint, as case file no. 496 of 2011, was also got registered at concerned Police Station, Rabale, Navi Mumbai on 30.07.2011, for offence punishable under Section 420 read with 34 of IPC, read with Section 66 of IT Act.

11. Investigation also revealed about the shortcomings of system of Respondents, letting such fraudulent acts. Hence, this complaint with above prayer, was got filed before Adjudicating Officer. Wherein, notices were issued, replies were filed and after hearing both side, impugned order was passed by Ld. Adjudicating Officer, with a direction to State Bank of India to pay damages, to the tune of Rs. 6,00,000/- (Rupees Six Lakhs only), by way of compensation to the complainant, and in case of failure, compound interest, @12% to be compounded monthly, was also payable. Respondent No. 3, Vodafone was directed to make payment of damages in the tune of Rs. 6,00,000/- (Rupees Six Lakhs only) within a month, and failing which, the compound interest, @ 12% to be compounded monthly, was also chargeable.

12. This order of Adjudicating Authority is under appeal in **Cyber Appeal 7 of 2014,** filed by State Bank of India, through GM, having Local Head Office at Syenrgy, Bandra Kurla Complex, Mumbai, Respondent No. 1

in Complaint and State Bank of India, through Branch Manager, Mahal Branch, Mahal Nagpur, Respondent No.2, in Complaint, against Prashant Mahadeorao Buradkar, Complainant, present Respondent No. 1 and Vodafone Essar Limited, Respondent No. 2 that is Appellant of Appeal No. 6 of 2014, and opposite party No. 3 of main Complaint.

13. The facts are one and common, written Supra with a bit elaboration, for and on behalf of Bank, that the Complainant was having its Saving Bank Account, in his name and his brother in SBI Mahal Branch, with online banking facilities and it was being operated nicely. But with activation of new SIM Card by Vodafone Essar Company on 26.07.2011, Complainant found that since 24.07.2011 to 26.07.2011, there was illegal transactions in his account, thereby siphoning of Rs. 10,50,000/- (Rupees Ten Lakhs Fifty Thousand Only) by some unscrupulous and unknown persons, who had deactivated cell phone of Complainant, and had obtained duplicate SIM Card, issued by Vodafone Essar, in that period. A complaint was instantly got lodged at Police Station, Rabale, Navi Mumbai, then after this complaint for damages, was also filed before adjudicating authority. The allegation against bank was lack of due diligence in implementing and maintaining reasonable security measures/practices/procedures

according to Internet Banking in India Guidelines laid by RBI DBOD COMP BC NO. 130/07.03.2 June 2001, resulting loss to complainant. The Adjudicating Officer held that Bank Appellant have not followed the KYC norms, in opening and maintaining bank accounts, that's why liable to compensate Respondent No. 1 for his loss.

14. A reply was filed with contention that Internet Banking channel is protected by advanced security feature, both physical and logical. Appellants have considered various risks inherent in transacting over a public network, such as the Internet and have deployed appropriate security measures to protect customers. Firewalls allow only valid web traffic to reach the Appellant's server. Proven 128-bit Secure Socket Layer (SSL) encryption technology is deployed to ensure that the information exchanged between the user's computer and www.onlinesbi.com over the Internet is secure, and cannot be intruded upon. VeriSign certifies that information exchanged during a valid session is protected during its transmission over the internet. Further, the Appellants have additionally installed mechanism, such as Intrusion Detection System, which gives further protection to the transactions on the internet site. The procedure for activating Internet banking is as stated that Account Holder has to make a requisition for

Internet banking. He gets Internet Banking Kit, which contains First user ID and a password, with a unique registration code, to be entered in the system, at the time of activation of Internet banking facility. And once, the process of activation is completed, the Account Holder is to start using the Internet banking facility with the User ID and password provided in the Kit after lapse of 24 hours only. This First User ID and password is automatically generated by the system and no employee of the bank has the access or avenue to get acquainted with such User name and password.

15. The First ID and password provided by Appellant at the time of activation of Internet banking facility is to be used for the first time operation only, and after the entry with the First User ID and password the system immediately prompts for a new ID and password. Thus, the First User ID and password would be used only once in order to create customers own ID and password. And after its generation by Account Holder, the First password and User ID given in the Kit becomes lapse. A profile password is to be set by user. It is unique with each account holder and it can never be duplicated, copied or used without knowledge or permission of the Account Holder. High Security password is also generated and sent for each

transaction on internet facility. It is generated automatically and message to registered mobile number provided by Account Holder at the time of application for Internet banking. Thus, the mobile number and the SIM Card containing all information is an important component of the entire system, and it is imperative that the Account Holder is very careful as to what information he feeds into the SIM Card, which can be misused as his, in this instance. It is, therefore, clear from the above factual position, that it is the responsibility of individual Account Holder, to maintain the secrecy of his User ID and password. And in case of failure, its own negligence and carelessness with its own responsibility and cost.

16. In the present case, the unauthorized transactions, in 27 numbers, in between 24.07.2011 and 26.07.2011, siphoning amount of Rs. 10,50,000/- (Rupees Ten Lakhs Fifty Thousand Only), withdrawn by third party, was owing to negligence of Complainant, and Vodafone Essar Company. But without appreciating the facts and evidences, erroneously bank was directed to make payment of Rs. 6,00,000/- (Rupees Six Lakhs only). Even the practices of Banks abroad, has been written in the impugned judgment, which is of no concern, which is matter and issue before the Adjudicating Officer. The finding of

Adjudicating Officer, was not based on the evidences on record. Hence, this Appeal with above prayer.

17. The reply of this Appeal, as well as of Cyber Appeal No. 6 of 2014, were filed by Complainant, reiterating the contention of complaint.

18. Heard Learned Counsels of both sides and gone through the materials places on record.

19. While hearing in Appeal No. 6 of 2014, Vodafone India Limited Vs. Mr. Prashant Mahadeorao Buradkar and other, Order dated 22.02.2024 was passed as below:

> "1. Case taken up. Learned Counsel for both side are present.
>
> 2. Learned Senior Advocate, Mr. Meet Malhotra assisted by Mr Kaushik Moitra and Ms Romi Kumari, mentioned that in a bunch of cases, already decided by Court No. 1 of this Tribunal, first appeal has been decided against present appellant, and against that judgement of Court of first appeal, second appeal is pending, before Hon'ble Bombay High Court, wherein, a date in month of March 2024, is scheduled for hearing, and the legal questions involved, in present appeal, were also there in those first appeals, decided by this Tribunal, except one question that the laws, which were framed, and against whom deviation is being said, were of year 2016. Agreement entered in between, were never infringed and the alleged negligence, resulting this cause of action, were of period previous to those enactments.

3. Hence, on this narrow point, argument is to be advanced. Rest points are sub-judice and Cyber Appeal has been decided against the present appellant. A date be given for placing arguments on this point only. For rest, the judgement of erstwhile Cyber Appeals are there.

4. Learned Counsel for Respondent is with no objection, for accommodating Learned Senior Counsel.

5. Hence, list the matter on 05.04.2024 “for further arguments” in this Cyber Appeal.”

20. Meaning thereby, the points raised in memo of Appeals, narrated as above, were raised in other Appeals of the same bunch. It were heard and decided, against which, Appeal has been filed before Bombay High Court, as a Second Appeal wherein, a date for hearing is there and the legal question involved in this Appeal, was restricted to only one question that the laws, which were framed and against whom deviation is being said, were of year 2016. Agreement entered, in between, was never infringed and the alleged negligence, resulting this cause of action were of period, previous to those enactment. Hence, that legislation/ Rules of year 2016, are not applicable to this fact. Wherein replaced SIM Card was got issued prior to above rule of

2016 i.e., when there was not any Regulation and direction, to be observed, for replacement of SIM Card, by service provider.

21. The Appeal was to be heard on that narrow point only. But while being argued, it was further elaborated by both of the Appellants and as well as Respondents, in both of above Appeals. A written submission in form of brief note, was filed by Learned Senior Advocate, Mr. Meet Malhotra assisted by Mr Kaushik Moitra, Advocate, Ms Subhalaxmi Sen, Advocate, Ms Romi Kumari, Advocate, Mr Ravi S S Chauhan, Advocate and Ms Pallak Singh, Advocate, as follows:

I. That the Appellant has challenged the Impugned Order dated 02.07.2013, principally on the ground that the order is based on general finding of negligence against the Appellant, in issuance of duplicate SIM Card to the Respondent No.1 (July, 2011). Its with general negligence led to the Respondent No. 1, suffering loss on account of some imposter accessing the bank account of the Respondent No. 1, and fraudulently withdrawing certain sums of money, therefrom. The imposter had a prior knowledge of the bank account and password details of the Respondent

No. 1, and was able to illegally transfer money out of the said account. This had no direct reference to the duplicate SIM issued by the Appellant.

II. The pointed defence of the Appellant is that the present proceedings are not emanating from a general action for compensation on account of negligence in tort or damages for breach of contract. The action against the Appellant emanates from a right apparently conferred on Respondent No. 1 under Section 43A of Information Technology Act, 2000 ("IT Act, 2000") dealing with Compensation for failure to protect data.

III. It is the case of the Appellant that Section 43A of IT Act, 2000 must be read in totality, including the explanation thereto, (see Sundaram Pillai Vs. Pattabiraman, (1985) 1 SCC 591 Para No. 53). The main Section 43 A is couched in such words and terms as may lead to a conclusion that general negligence on behalf of an entity, such as Appellant shall render that entity to "pay damages by way of compensation" to a person affected by negligence of such entity.

IV. However, explanation to the Section, more particularly (ii) and (iii), are particularly significant and in the submissions of the

Appellant, if read in totality and holistically, with the main Section, will narrow down the scope of what constitutes actionable negligence attributable to an entity, such as the Appellant.

V. Since the Respondent No. 1 has chosen to avail a remedy especially provided by Section 43 A of the IT Act, 2000, the substantive definition of what constitutes negligence thereunder, must also strictly bind all stakeholders. Once having taken recourse to Section 43 A of the Act, the Respondent No. 1 cannot then rely on general principles of damages for breach of contract or tort. Viewed from this perspective "reasonable security practices and procedure" in explanation (ii) must necessarily mean: (a) such as specified in the agreement between the parties, or (b) specified in any law, or (c) in absence of any agreement or law, as prescribed by the Central Government.

VI. It is the case of the Appellant that issue of duplicate SIM card stands on a different footing than issue of a SIM card, in the first instance. That, at the time when the alleged infraction took place in July, 2011, there was no: (a) agreement between

parties as to norms covering issuance of duplicate SIM card (b) no law specifying practices and procedures required to be observed by the Appellant and (c) no security practices or procedure prescribed by the Central Government in consultation with professional bodies etc.

VII. Without prejudice to aforesaid, it is further the case of the Appellant that SIM card does not constitute "sensitive personal data or information" and is merely a card or merely a piece of hardware, which is inserted in a handheld mobile phone, connected with the mobile phone to network of the Telecom Service Provider ("TSP"); but that in itself, on a standalone basis, on as is where is basis, the SIM is a card or piece of hardware as given in various instances.

VIII. It is the case of the Appellant that on previous occasion the Hon'ble Tribunal noticed that Section 43 A, may not be attracted to a TSP, such as Appellant (ICICI Bank v. Saurabh Ravi Shankar Jain, 2019 SCC Online TDSAT 3480, Para No. 10). Subsequently, the Bench (Chairperson alone) decided a matter i.e., Vodafone Idea Limited v. Sandeep Singhal, Cyber Appeal No. 5 of 2018, against the TSP. In that judgment and order

dated 20.12.2019, reference is made to Section 43 A, but not to the explanation to Section 43 A, which is the crux of the legal submission on behalf of the Appellant in the present round of litigation. And the judgment of Sandeep Singhal, is under Appeal before in Bombay High Court in First Appeal (ST) 1339 of 2020 and operation of judgment is stayed on certain conditions. This does not operate as precedence so far as Appellant's case is concerned.

22. The circular dated 16.08.2016 was the guidelines with regard to issuance of replace SIM Card. Prior to 16.08.2016, there were DOT guidelines dated 10.05.2005 and 22.11.2006, for the issuance of a fresh SIM Card on boarding of a customer. And in view of guidelines of DOT dated 09.08.2012, no penalty shall be imposed on the licensee, in case of failure to take due care of process of activation verification applicable at that time.

23. In reply, the arguments of Complainant is that negligence of the Applicant Vodafone is fully covered under Section 43A of the IT Act 2000, because it was held to be negligent and failed to employ/enable reasonable security practices and procedure mandated by law, for issue of duplicate SIM Card. The guidelines/directions, which were

applicable for issuance of fresh SIM Card would apply with equal force to issue a duplicate SIM Card also, in case of no direction with that regard, till direction dated 16.08.2016.

24. Kamini Solanki, the witness of Appellant had admitted the procedure being observed with regard to issuance of duplicate SIM Card and it was not observed in the present case. The SIM card was not only a SIM card, and it was not a hardware. Rather, it was with identification module and the information furnished by Complainant for getting above cell number being given in Bank services, online transactions, it was with all information of banking transactions contained in computer maintained by banking company and any lapse on part of reasonable practice with regard to this software and hardware, was an act, within the domain of Section 43A of the IT Act.

25. Information Technology, reasonable security practices and procedures and sensitive personal data or Information Rules 2011 was with Rule 3, Rule 4, Rule 5.5, and Rule 8, specified law to be obeyed. But it was not obeyed so. Appellant controls and operate SIM Card carrying the customer's personal data and information which, in mobile technology driven world, facilitates personal, business and financial transaction processes. 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 the 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 with the system database of the Appellant cell Company. Appellant collect these sensitive and personal information from the customer, before any services, post-paid or pre-paid, are provided. Appellant is the custodian of such sensitive and personal information which includes photo identification, signatures, alternate phone number etc., of customer. It was negligent in issuing replaced SIM Card to the fraudsters, by allowing to access the sensitive personal data Information provided by Complainant at the time of obtaining its mobile number. Bank too was negligent in observing the guidelines relating to online banking. It never communicated through alternate

phone number or email. Unnatural transaction in between 24.07.2011 to 26.07.2011, with such a huge siphoning of money was there in the account of Complainant, but no heed was there. Hence, both of these Appeals were prayed to be dismissed.

26. Heard Learned Counsels of both side and gone through the materials places on record.

27. Learned Senior Counsel for Vodafone, i.e., Appellant of Appeal No. 6/2014 had narrowed down the dispute, written as above, that the issue of duplicate SIM card stands on a different footing than issue of SIM card, in the first instance, that at the time when the alleged infraction took place in July 2011, there was no agreement between the parties, as to norms covering issuance of duplicate SIM card, nor there was any law specifying practices and procedures, required to be observed by the Appellant, no security practices or procedure prescribed by Central Government in consultation by professional bodies was deviated. This plea was taken by Cellular Service Provider, in Cyber Appeal Nos. 1 and 4 of 2014, wherein, a judgement dated 14.02.2020, was with specific mention of the plea taken, for and on behalf of Vodafone, that it is the only a service provider under the licence, granted by the Department of Telecom, Government of India,

it does not possess, handle or deal with any sensitive personal data or information, and hence, Section 43A of the Information Technology Act, 200 (IT Act), will not apply to Telecom Service Provider, like Vodafone. Further, defence of Vodafone was that it had Customer Agreement Forms (CAF) and subscriber verification is not included in scope of the reasonable security practices and procedure under Section 43A. The identity and nature of sensitive personal data or information, possessed or handed by Vodafone, has not been established. In any case, since there was no intentional Act for assisting the fraudster, therefore, no contravention of Section 43 (g) of the IT Act, can be attributed and this plea taken before Adjudicating Officer, was taken in above appeal too, before Appellate Tribunal, and it was not accepted, even by Adjudicating Officer, as well as by this Tribunal. Rather, Adjudicating Officer in that particular case had held that there was direct nexus between blocking of SIM card of the complainant, issuance and use of duplicate SIM card by the fraudsters, and the unauthorised financial transactions, on the account of complainant. The importance of mobile numbers 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 revenues from such valid use of mobile phones. The significance of SIM or a duplicate SIM can best be understood by such service provider. In that particular case, documents of ICICI Bank show that not only bank transaction alerts but even OTP was sent to the registered mobile number, but in fact it went to the duplicate SIM card, which was issued purely on account of negligence boarding on connivance and laxity, in maintaining reasonable security measure and by ignoring the standard procedures, for verification of documents for replacement of SIM card with the original documents and the data available in the CAF of original SIM owner. But, if such duplicate SIM was not issued to the fraudster, 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. This prevented the complainant from getting alerts in respect of unauthorised transactions from his bank account. The security measure of Vodafone was hopelessly inadequate, because it had come on record that online filenet system was down for days. Even for a cursory comparison of check, the labelling the fraudulent nature of request of duplicate SIM as to why the Vodafone did not check

whether original number was in use or not remains a mystery. Not only this issue, rather other technical points were also raised by Vodafone, before Appellate Authority, as was previously raised before Adjudicating Officer alleging the same fact, which has been alleged in present Appeal. The facts and issues of this Cyber Appeal No. 1 of 2014, and present Appeal No. 6/2014 are one and similar. This Tribunal in aforesaid judgment dated 20.12.2019, in Cyber Appeal No. 3/2018, Bank of India vs Sh. Sandeep & Anr. read with Cyber Appeal No. 5/2018, Vodafone Idea Ltd. Vs Shri Sandeep Singhal and Anr, had reiterated with the finding that Vodafone was liable under Section 43(g) and 43A of IT Act, whereas the Bank was found deficient in security measures liable under Section 43A of IT Act, and both of these Appeals were dismissed.

28. Hence, the very argument raised by Learned Counsel, in present Appeal, written as above, for and on behalf of Appellant Vodafone are with same facts and of common issues, requiring no further reiteration. Rather, to get those previously settled proposition of law, applied in present appeal. The argument of Learned Counsel that the judgment of this Tribunal in ICICI Bank Limited vs. Mr Sourabh Ravishankar Jain in Cyber Appeal No. 5/2013 on September 24, 2019,

reported at 2019 SCC Online TDSAT 3480 at “Para No. 9 & 10” was with following mention :

> “In view of the nature of the pleadings and lack of proof we are not persuaded to accept that the Appellant Bank had established good and healthy security measures and those were operational and were used for avoiding fraud in the case of the complainant. Sections 43 and 43A of the Act create such responsibility on the Bank because it stores sensitive data of its account holders in its computer system. In our considered view Appellant Bank has failed to show that at the relevant time it had put in place adequate security measures. Thus the other plea urged on behalf of appellant is with a view to hold Respondent No. 02 liable for a further amount of money for a contributory negligence. Before coming to this issue it will be useful to note that since the amount awarded against Respondent No. 02 was only 25,000/- , it chose to pay that amount to the complainant instead of filing any Appeal. This stand was taken when Respondent No. 02 appeared in this appeal and that explains why no cross appeal has also filed once the amount was accepted and paid. In view of such factual situation, a categorical stand has been taken on behalf of Respondent No. 02 that the legal issue as to whether a Telecom Service Provider like the Respondent No. 02 can be made liable under the IT Act, for the lapse of issuing duplicate SIM, should be left open to be decided in appropriate case, when the

telecom Company has preferred appeal or cross appeal. We accept the aforesaid submission and leave those issues of law open for determination in an appropriate case."

But in the subsequent case of Vodafone Idea Limited vs Mr Sandeep Singhal & Anr, supra, which was decided by Single Bench of Hon'ble Chairperson, and it is under Appeal listed in Bombay High Court. Hence, it does not operate as a precedent, so far Appellant's case is concerned.

29. This argument of Learned Senior Counsel is not tenable because the question was raised in case of State Bank of India Vs. Shri Chander Kalani and Anr, in Cyber Appeal No. 13 of 2015 with M.A No. 282 of 2017, decided on 31st July 2018, reported at 2018 SCC Online TDSAT 738, wherein Section 46 with regard to execution of Adjudicating Authority and Section 43A of IT Act, was raised, heard and decided with the finding that Bank through its computer resource was clearly possessing, dealing and handling sensitive personal data and information of complainants in its computer resource. The reasonable security practices and procedures required to be implemented and

maintained, had to be designed to protect such information from various acts, such as unauthorised access and use.

30. The judgment of this Tribunal, delivered in Bank of India vs Sandeep Singhal, in Cyber Appeal No. 3 of 2018 as well as Vodafone Idea Ltd. vs. Sandeep Singhal and Anr in Cyber Appeal No. 5 of 2018, was with specific discussion and finding that too, after hearing both side in Para 26 as follows :

> "When a Telecom Service Provider is able to show that it is handling only the information, data or communication link for any third party then subject to provisions in sub Sections (2) and (3), it can lawfully claim exemption from liability, but such exemption clearly can not apply when the Telecom Service Provider is dealing with matters which are not related to third parties but its own customers with whom it already has a service contract and whose personal data and information has been collected through CAF or KYC process and as per requirement stored in the data base of such service provider. The protection of interest of its subscribers who are not in any way third parties, cannot be covered by exemption granted by Section 79 of IT Act. Hence, there is no requirement of further analysing the submissions advanced by Learned Counsel for the complainant that even if Section 79(1) was to apply to subscribers and consumers of Vodafone by treating them as third parties, in view of requirement of under sub-Section 2 (b)

(ii) and (c), the intermediary is required to observe due diligence and observe or follow other guidelines prescribed by the Central Government such as the Information Technology (Intermediaries Guidelines) Rules 2011, (hereinafter referred to as the Guidelines Rules of 2011). Under Rule 3 of Guidelines of 2011, the intermediary is required to follow due diligence while discharging a number of duties enumerated in that rule. One of the duties is to strictly follow the provisions of the Act and any other Law of the timing in force. The intermediary is required to also take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures, as prescribed in The information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.

27. Once the computer resource of the intermediary contains informations relating to SIM No and other details of a subscriber, these informations have to be kept secured and not allowed to be tampered or changed in a casual manner. Such information is required to be secured almost in identical terms as required by Section 43A of the Act. "

31.In paras 43 and 44, it has been specifically held :

"The telecom service provider, as discussed earlier, has the details of all persons who are already its customers / subscribers. Such details include personal details which such subscriber is permitted to utilize the Telecom Services. The Scope and variety of Telecom services depend upon technology

that is expanding every day. It is lawful and permissible for the subscriber to depend upon communications through the mobile number allotted to him with his Banker and with other persons without threat or apprehension of unlawful invasion of his privacy. In such a situation transferring the aforesaid facilities by changing the SIM number already available in the personal data or information of the customer/ subscriber can have serious adverse impact upon the subscriber. If such an eventuality happens because the Telecom Service Provider is found to be negligent in implementing and maintaining reasonable security practice and procedures as mandated by Guidelines Rules of 2011 and thereby it has caused wrongful loss to the subscriber, section 43 A can also get attracted against the Telecom Service Provider. The plea that the lapses in verifying the bonafides and authenticity of the person applying for a duplicate SIM amount only to violation of CAF procedure or KYC procedure cannot have any diluting effect upon the rigours of section 43 A. Once the essential Ingredients of negligence are attracted and established. The minor penalties for CAF violations or for KYC lapses cannot be treated to be an effective shield against claims arising under sections 43 and 43A.

44. On the basis of above discussion, it can be safely concluded that if the facts and materials are found sufficient, in a case of present nature involving un-authorised / fraudulent transfer of money from a bank with the help of a duplicate SIM issued in an

apparent negligent manner, the Telecom Service the Provider which has issued the duplicate SIM and made it operational by including the same in its computer network, can be held liable to pay damages by way of compensation under section 43A read with Section 43 (g) of the Act. The Telecom Service Provider, in his turn, in an appropriate case may sue its errant employee/agent for appropriate relief of recovery etc. but that will not be a shield against a claim by an aggrieved subscriber."

32. The very argument with regard to application of guidelines of dated 1.8.2016, as has been argued by Learned Senior Counsel that provision for observing security practices and procedures in the matter of issue of duplicate SIM, has been included in the guidelines of Department of Telecommunications (DOT). (Only through guidelines dated 1.8.2016); The earlier guidelines of 2012, provide guidelines for issuance of SIM to a new subscriber and also of for change of SIM for pre-paid to post-paid and vice versa, but not specifically for issue of duplicate SIM. This issue was also heard and decided by this Tribunal, in above judgment that guidelines which were with regard to issuance of SIM card or change of its nature were fully applicable with regard to issuance of duplicate SIM card, and it was guidelines given in year 2012 as well as 2016 that in the interest of National Security Purpose, the close monitoring and verification, with regard to issuance of SIM card or its

activation or deactivation was required. Hence, the argument that it was not required, is not tenable. Rather, the argument of Learned Counsel of Respondent are being found to have merit that even as per 2012 Guidelines, the Telecom Service Provider has to adopt all the basic security measures, before deactivating SIM card of its subscriber and issuing a fresh SIM card to an applicant claiming to be an existing subscriber. Hence, in present case, the photograph, signature etc of the present complainant and of the imposter, who claimed for issuance of SIM card was with quite difference, legible apparently, and there was no precaution taken by having a contact on alternate phone number for verifying the veracity of applicant and the request made by it. Hence, the argument raised by Learned Senior Counsel for Appellant, is of no avail. Hence, Cyber Appeal No. 6 of 2014, merits its dismissal with cost.

33. So far as appeal of Bank is concerned, the issues raised by Bank had been decided in many appeals, including in those two appeals discussed supra and bank was held liable for making payment to fraudster. In present case too, there was unusual transaction of withdrawal, without any confirmation to complainant, and Learned Adjudicating Officer in its judgment has elaborately discussed with

those circumstances and had awarded compensation, in apportionment, in the tune of Rs. 6 lakhs, to be borne by Bank. The principle and law held by this Tribunal, in those previously decided Cyber Appeals are with same facts and alike argument, as has been raised by Learned Counsel for Bank, in present appeal. Hence, the appeal of Bank also merits to be dismissed by this Tribunal.

34. Accordingly, both of these appeals are being dismissed with costs.

……..
(Justice Ram Krishna Gautam)
Member

12.9.2024
/NC/