

**TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL
NEW DELHI**

Dated 3rd July, 2018

Cyber Appeal No. 13 of 2015
(M.A. No.282 of 2017)

State Bank of India

... Appellant

Versus

Shri Chander Kalani and Anr.

... Respondents

BEFORE:

**HON'BLE MR. JUSTICE SHIVA KIRTI SINGH, CHAIRPERSON
HON'BLE MR. A.K. BHARGAVA, MEMBER**

For Appellant : Mr. Ramji Srinivasan, Sr. Advocate
Mr. Rajiv Kapur, Advocate
Mr. Naveen Hegde, Advocate

For Respondent : Mr. Nikhil Singhvi, Advocate
Ms. Nikita Pandey, Advocate

ORDER

By Shiva Kirti Singh, Chairperson – Aggrieved by order dated 12.01.2015 made by the Adjudicating Officer, Government of Maharashtra (Principal Secretary, IT, Government of Maharashtra) in Complaint No.1 of 2014, the appellant, State Bank of India, has preferred this Appeal under Section 57 of the Information Technology Act, 2000 (IT Act). By the

impugned order, the learned Adjudicating Officer has dealt with and disposed of a complaint filed by the complainants, Shri Chander Kalani and his wife, Smt. Romi Kalani, in exercise of power under Section 46 of the IT Act. The order discloses the brief facts of the case as per complainants, the documents submitted by the parties including the Police Reports as well as the submissions advanced on behalf of the parties. After analysing the documents and the arguments in the light of facts available on record, the learned Adjudicating Officer has given his final conclusions in Para 6 of the order which is as under:

“6. In view of the above,

1. Complainant has been doing transactions with the banks only through emails, which is insecure way of doing things. Mechanisms like alternate email, SMS alerts etc. were not used. Complainant had not informed the bank about his defunct mobile number. Hence, both the Complainant and the Respondent Bank have to share the blame.

2. I hold the **Respondent No.1(State Bank of India)** in violation of Section 43A of the IT Act, and order them to a compensation of **Rupees 40,00,000 (Rupees Forty Lakhs)** to the Complainant to partly cover his loss, within a month of this order, failing which compound interest of 12 percent compounded monthly will also be chargeable.”

2. On behalf of the appellant Bank, Mr.Ramji Srinivasan, learned senior counsel has first highlighted some of the facts with a view to substantiate the stand of the appellant Bank that the complainant was not diligent. He highlighted that Mr.Kalani being a Non-Resident Indian (NRI) had used his

Email identity in the past for directing the Bank to create fixed deposits out of funds available in his savings bank account. Of course, he had confirmed the same through his talks from registered mobile number also, but at the time of relevant occurrence towards the end of October, 2013, his phone had got defunct and he did not supply any alternative phone/mobile number through which the Bank could recheck or confirm the instructions for transfer of funds from his account to some other accounts as per instructions in the Emails originating in his name from his Email ID. It was also highlighted by learned senior counsel that the complaint of hacking of Email ID of the complainant was made belatedly on 13.12.2013 and thereafter the Bank itself took steps to inform the Police as well as the two other banks where, in total, an amount of 60000 GBP had been transferred and this led to recovery from one of the accounts of 16710 GBP(approx.) which was made available to the complainant.

3. According to learned senior counsel, the loss of approximately 43300 GBP was not on account of any negligence on the part of the appellant Bank and therefore, the award of Rs.40 lakhs which is equivalent to almost the entire loss of 43300 GBP, to the complainant is not just and proper; moreover, when the learned Adjudicating Officer himself has held that both, the complainants and the Bank have to share the blame.

4. It has further been argued that how the respondent Bank is liable to share the blame has not been established by supply of reasons. It was urged that even

if this finding is found acceptable, the compensation should have been less and not Rs.40 lakhs so as to cover the entire alleged loss to the complainant. It was also submitted that the Adjudicating Officer should have exercised his wide powers to obtain reports from experts as to whether the Email ID of the complainants was actually hacked or not and if so, by whom.

5. Learned senior counsel for the appellant has also raised a plea that in the complaint petition the complainant has also referred to Section 43(a)(b) but those provisions of law are not attracted. According to him, Section 43A under which the claim for compensation has been allowed does not provide for compensation for any wrongful loss etc. to any person from a body corporate unless the facts lead to a conclusion that such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and that such negligence has caused the wrongful loss to the person who has sought damages by way of compensation.

6. So far as relevant and essential facts are concerned, the complaint dated 13.12.2013 filed by the respondents discloses the particulars of an NRI Account which the complainants had in the respondent Bank along with fixed deposits. The complainant stated that he had no bank account in London where the money had been sent. Photocopy of Passport was also enclosed to show that he has not travelled to London. He denied to have authorised termination of his fixed deposits through Emails. He requested for restoring back the entire

amount in his fixed deposits accounts. Besides such complaint to the Manager of the Bank, he filed a complaint bearing No.1 of 2014 before the Adjudicating Officer on 30.12.2013 giving all the details. In addition to two officials of the Bank, unknown persons were also shown as respondents. In Para 3, the complainant has highlighted the crux of his complaint by stating that the complainants had never sought facilities of any internet banking or phone banking nor had permitted in writing or orally for entertaining any transactions using Email and yet three fixed deposits of the complainants were fraudulently transferred to unknown beneficiaries upon fake Email requests. Complainants alleged negligence on the part of respondent Bank in transferring the funds, approximately amounting to Rs.63 lakhs and in sharing sensitive personal information (account details) with unknown person in course of replying to the fake Emails. The complainants claimed to be senior citizens and Non-Resident Indians(NRIs). They disclosed that while they are residents of Mumbai, they also have business dealings in Lagos, Nigeria and West Africa. They had 6 joint fixed deposits with the Bank having different maturity dates and amounts. On 13.12.2013, when Mr.Kalani visited the Bank for updating the passbook and to collect one original FDR, he was shocked to know that their FDs have been fraudulently broken and money transferred to some account without any authorisation from them. It was alleged in the petition of complaint that the Bank had transferred the amount arbitrarily and without any verification. It was also highlighted that when the complainants had never opted for banking

transactions through Email, phone or internet, respondent Bank should have been diligent to cross-check before acting upon the fake Emails. In the petition of complaint it was also highlighted that for transfer in foreign exchange, signature of the account holder on A-2 Form is required and admittedly no signature of the complainants was available on such form. Instead, the Bank acted on a scanned signature on A-2 Form, that also of only one of the joint account holders.

7. In reply to the defence raised on behalf of appellant Bank, learned counsel for the respondents/complainants submitted that the defence raised by the Bank in its pleadings has not been substantiated by any material. There was no correspondence or document raising any doubt in respect of grievances of the complainant. The Bank never doubted this in its complaint to the Police nor the investigation by Police found anything wrong with the case lodged by the complainant. It was submitted that use of Email by the complainant on one occasion was not for taking out fund from the Bank in favour of any other entity but only for creating fixed deposits with the Bank and that also was done after confirmation through registered mobile number. It was also submitted that there was no delay in lodging the complaint of hacking of Email ID and unauthorised transfer of funds from complainant's account. It was disclosed in the complaint to the Bank Manager that the entire fraudulent and illegal transaction came to knowledge of the complainant only when he visited the

Bank on 13.12.2013 for updating the passbook and for collecting one original FDR. Even thereafter, the Bank acted on the information and was able to recover a substantial amount of 16710 GBP and the same was given back to the complainant. Had there been any wrong intention on the part of the complainant, no such amount could have been traced or recovered on action initiated after his complaint.

8. Learned counsel for the respondent/complainant pointed out that the appellant has nowhere denied the case of the complainant on any essential and material facts. There is no denial to the averment in the petition of complaint that the Bank had transferred the amount; that the complainant had never opted for transaction through Email, phone or internet and further that the Bank should have been diligent to cross-check before acting upon the fraudulent Emails. It was also highlighted that while requirement of A-2 Form is signature of the account holder, the joint account from which money was transferred was in the name of husband and wife but the Bank accepted such Form only with scanned signature of only one of them. It was vehemently argued that scanned signature is no signature and when the complainants have not opted for net-banking, phone banking or Email banking, appellant had to seek original signature of the account holders before effecting the transfer. Admittedly, no digital signature of the complainants was used for the fraudulent transaction.

9. Learned counsel for the respondent took us through each of the Emails dated 28.10.2013, 06.11.2013, 12.11.2013 and 25.11.2013 to point out how certain information in respect of FD accounts and their numbers were supplied by the Bank itself and it facilitated the fraud. It has been argued that supply of such information from the computer system of the Bank was unauthorised and clearly a negligent act. Learned counsel referred to Para 26 in the Memo of Appeal to point out that the appellant has acknowledged that the Adjudicating Officer examined the police investigation reports dated 10.03.2014 and 26.08.2014 and that these reports confirmed that the Email ID used by the fraudsters was hacked. Learned counsel pointed out that Section 43(a) and (b) has been mentioned in the claim petition because unknown persons who were beneficiaries of the fraud have also been made parties as unknown. They could also be liable to pay damages by way of compensation to the claimant and hoping that the Police may locate them, the aforesaid provisions were mentioned. He clarified that the liability of the Bank is under Section 43A and that is the finding of the Adjudicating Officer also who has allowed the claim under said provision only.

10. Before adverting to the scope and ambit of Section 43A in the light of submissions advanced on behalf of the appellant, it would be appropriate to conclude the issues of fact by reverting to rejoinder submissions on behalf of the appellant. In reply, learned senior counsel for the appellant submitted that

the claimant has not filed any proof of hacking of his Email ID which was necessary because in pleadings the Bank had not admitted hacking. According to him, the jurisdictional facts for applicability of Section 43A have not been proved by the claimant. He also submitted that the Adjudicating Officer ought to have asked the parties to lead evidence and allowed the other parties to cross-examine such evidence before giving findings on disputed facts. In other words, the submission is that the power to adjudicate under Section 46 of the IT Act has not been exercised fairly and in an appropriate manner and that since the Adjudicating Officer has some powers of a civil court and is deemed to be a civil court for certain purposes, it ought to have followed the detailed procedure of holding a fair trial in respect of issues arising from rival cases.

11. In view of last submission it is necessary to notice that under Section 46, the jurisdiction of the Adjudicating Officer is limited to claim not exceeding Rs.5 crore. The rules of natural justice are clearly applicable because subsection (2) of Section 46 requires the Adjudicating Officer to provide a reasonable opportunity to the person alleged to have caused injury or damage, for making representation in the matter and by holding inquiry through this process, if the Adjudicating Officer is satisfied that such person has committed the contravention, he may impose penalty or award such compensation as may be appropriate and in accordance with the provisions of the IT Act. Considering the specific provision of giving reasonable opportunity to make representation

and on such inquiry, a finding or satisfaction can be recorded, there is no difficulty in holding that the procedure does not warrant an elaborate trial as is required to be held by a civil court in a suit. No doubt some powers of civil court have been vested in the Adjudicating Officer but these are only to enable the officer to summon or discover relevant materials, whenever necessary for coming to a proper finding in such inquiry. From the powers, it cannot be concluded that the inquiry should be replaced by an elaborate trial like that of a suit in civil court. Such interpretation would defeat the very purpose of providing a summary procedure of inquiry for adjudicating claims upto Rs.5 crore by the Tribunal under the IT Act.

12. Keeping in view the aforesaid discussion, the procedure adopted by the learned Adjudicating Officer cannot be held to be against the procedure provided by the IT Act.

13. So far as pleadings and requirement of proof of hacking is concerned, it has already been noted that admittedly police report supported the case of the claimant that his Email ID was hacked and no material was produced by the appellant to create any doubt on this issue. The submissions advanced on behalf of the respondent/complainant deserve acceptance. The appellant failed to bring on record any material to rebut the case of the complainant that they had never authorised the Bank to transfer their money to other bank or entities through internet or Emails. Although a submission was advanced that the Bank,

as a policy, had extended the facility of banking through Emails to NRI account holders but nothing has been brought on record to support this plea.

14. The Emails disclose that the Bank itself leaked-out certain vital information relating to details and numbers of the Fixed Deposits of the complainants that were becoming due for maturity. The transfer of funds on instructions through Emails and on a scanned signature on A-2 Form leave no manner of doubt that the Bank was negligent in sharing financial information of the complainants which is covered by Rule 3 which defines sensitive personal data or information under “The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (hereinafter referred to as the ‘Rules’). Hence it can safely be held that the Bank, a body corporate, while processing, dealing and handling sensitive personal data or information in its computer resource, owned, controlled and operated by it, was negligent in not verifying from the available records that the complainants had never authorised transfer of money or instructions through Email and the act of the Bank in divulging informations relating to complainants’ fixed deposits was also a negligent act without implementing “reasonable security practices and procedures”. Such negligent acts did cause wrongful loss to the complainant. We find no good reasons or materials to reverse the satisfaction arrived at the inquiry as recorded by the learned Adjudicating Officer in the impugned order. In the light of such finding on

facts, we shall now revert to the legal issue in respect of ambit, scope and applicability of Section 43A of the Act in the present case.

15. As already noted, the submission on behalf of the appellant is that negligence has to be proved not in respect of any banking transaction leading to wrong transfer of funds but only in implementing and maintaining reasonable security practices and procedures and compensation can be allowed only when negligence of such nature relating to security practices and procedures has caused wrongful loss to the claimants.

16. On a careful reading of Section 43A, it is absolutely clear that negligence in implementing and maintaining reasonable security practices and procedures alone creates a liability to pay damages or compensation under Section 43A, if such negligence has caused wrongful loss or wrongful gain to the person affected. Negligence by a banker in not properly comparing specimen signature with a signature on a cheque may also lead to wrongful loss or wrongful gain but such negligence will not be amenable to the scope of Section 43A. For this Section to apply, firstly, the body corporate should be possessing, dealing or handling sensitive personal data or information in a computer resource under its ownership, control or operation. Secondly, it should be found negligent in implementing and maintaining reasonable security practices and procedures and thirdly, by such negligence it caused wrongful loss or wrongful gain to any person.

17. The Explanation appended to Section 43A seeks to define: (i) body corporate, (ii) reasonable security practices and procedures and (iii) sensitive personal data or information. A careful reading of the Explanation reveals that “body corporate” has been given a wide and inclusive definition so as not to be confined only to a company incorporated under the Company Law. “Reasonable Security Practices and Procedures” are all such practices and procedures which are designed to protect particular kind of information not only from unauthorised access, damage but also from its use, modification, disclosure or impairment as may be specified in an agreement between the parties or in any law in force and in absence of both, such reasonable security practices and procedures, as may be prescribed by the Central Government in the prescribed manner. Clearly, the definition is again very widely worded and includes unauthorised use, disclosure etc. “Sensitive Personal Data or Information” has been assigned a meaning as may be prescribed by the Central Government in consultation with competent bodies or associations.

18. There is no dispute that much before the cause of action arose in the present case, the Central Government had, on 11.04.2011 published the Rules in the Gazette of India in exercise of powers conferred under provisions of the IT Act including Section 43A thereof. Since the Rules came into force from 13.04.2011, the definition of sensitive data or personal information came to include, as per Rule 3, financial information such as Bank Account or Credit

Card or Debit Card or other payment instrument details. It also includes any details relating to this clause provided to the Bank for providing service or for processing, whether such information is stored or processed under lawful contract or otherwise. For the case at hand, clauses (ii), (vii) and (viii) of Rule 3 are relevant. The Bank through its computer resource was clearly possessing, dealing and handling sensitive personal data and information of the complainants in its computer resource.

19. 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 uses. In the present case nothing has been brought on record by the Bank to show that it had implemented and maintained reasonable security practices to protect such information from unauthorised use. Rather the Bank itself used Email received on its computer resource unauthorisedly (without authority from the complainants for such use) for transfer of complainants' money to another bank account. Had there been reasonable security practices and procedures in operation, the concerned personnel could have found out that transfer through Email had not been authorised by the complainants. In fact, no safety or security measure appears to be in place because the transfer was made even without confirmation through registered mobile. The fact that complainant's registered mobile number was not functioning should have worked in his favour

because by way of reasonable security practices, the Bank if it had the practice of confirmation through mobile phone of the account holder, ought to have rejected the request for transfer of funds through Email on the valid ground that there was no confirmation available through registered mobile of the account holder. Use of scanned signature on A-2 Form received through Email was another unauthorised and illegal use of a so called signature which cannot have any sanctity either under the general law or under the IT Act.

20. Rule 4 requires a body corporate to have in place a policy for privacy and disclosure of information. In the present case in spite of serious allegations of unauthorised use of data and information relating to the complainants, the Bank has failed to bring on record any material to show that it had in place a policy as required by Rule 4. Rule 8 contains provisions for the purpose of finding out as to when a body corporate shall be considered to have complied with reasonable security practices and procedures. The appellant Bank did not bring on record any material to show that it had complied with the provisions for “reasonable security practices and procedures” in terms of Rule 8.


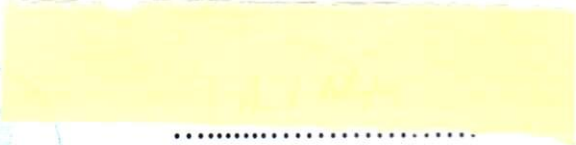
21. In view of aforesaid discussion, it is found that the Bank was negligent in implementing and maintaining reasonable security practices and procedures at the relevant time at least and thereby it caused wrongful loss to the complainants and hence it is liable to pay damages by way of compensation, as held by the learned Adjudicating Officer. All the ingredients for attracting and

applying Section 43A of the Act are made out. Hence, on this account, no interference is required with the impugned order.

22. The last submission on behalf of appellant is that compensation awarded by the learned Adjudicating Officer is excessive because there is a finding in Para 6 of the order that both, the complainant and the respondent Bank have to share the blame. On that account, as per submission, the compensation awarded should have been lesser and not Rs.40 lakhs which is almost equal to the total loss suffered by the complainants. This submission also does not merit acceptance. The complainants have claimed damages of Rs.1 crore. Para 11 of the claim petition shows that the first claim is for Rs.63 lakhs with interest @ 18% per annum from the date of fraudulent transfer and the second claim is also for compensation for Rs.37 lakhs under various heads such as Legal Fees and Expenses, Contraventions, Negligence and Failure to protect Complainants' data. In the light of such large claims the learned Adjudicating Officer has not committed any mistake in awarding a compensation of only the actual loss of approximately of Rs.40 lakhs suffered by the complainants. Hence, this plea also is not found acceptable.

23. In the result, we find no merit in the Appeal. It is dismissed accordingly. The amount of compensation awarded to the respondents should be made available to them, if not already made available, within one month from today failing which it shall become payable with interest @ 8% per annum with

annual rest, from the date of the order of Adjudicating Officer till the date of realisation. The respondents are also held entitled to Rs.25,000/- as consolidated cost of the Appeal. This shall also be payable along with the compensation awarded.


.....
(S. K. Singh, J)
Chairperson
.....
(A.K. Bhargava)
Member

sks

