(13)

TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL
NEW DELHI

Dated 21st February, 2019

Cyber Appeal No. 4 of 2015

SBI Cards and Payments Pvt. Ltd. ... Appellant

Versus

Dr. Vijay Gopal Kulkarni and Ors. ...Respondents

BEFORE :

HON'BLE MR. JUSTICE SHIVA KIRTI SINGH, CHAIRPERSON

HON'BLE MR. A.K. BHARGAVA, MEMBER

Appellant : Ms. Rashmi, Authorised Representative
Mr. Pawan Kumar, Authorised Representative

Respondent : Mr. Prashant Mali, Advocate

ORDER

A K Bhargava, Member – The appellant Company SBI Cards & Payments Services Pvt. Ltd. (referred to as Bank or SBI hereafter) is engaged in the business of providing credit cards to its customers. The respondent/complainant applied and received a credit card from the

appellant in the year 2008 and renewed it on 21-1-2013. It is against this credit card that the disputed online transactions happened between 0150 Hrs to 0220 Hrs on 1-7-2013. During this short period, about six fraudulent transactions amounting to Rs. 1,39,094.34 took place. The respondent got to know about these transactions when he received SMS alerts on his registered mobile. Subsequently the respondent disabled the credit card and lodged complaint with SBI. The respondent also made a complaint with local police station on 3-7-2013 and lodged a complaint with the Cyber cell as well on 13-8-2013.

2. In the meanwhile, respondent also filed a complaint on 28-2-2014 for adjudication under Section 46 of the Information Act, 2000. Learned adjudicator passed an order on 10-1-2015. Operative part of this order is as follows:

"(i) Bank has not given any meaningful, detailed report about the internal investigation into crime by their FIU (Fraud Investigation Unit). They have not been able to explain through use of logs how the customer credential got leaked out. Further they do not seek to have any monitoring system to alert about suspicious transactions.

(ii) I hold the respondent in violation of section 43 A of the IT Act, and order them to a compensation of Rupees 1,30,000/- (Rupees One Lakh Thirty Thousand) 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."

Being aggrieved by this order, Appellant has filed this appeal on 10-2-2015, praying for setting aside the impugned order.

3. Learned council for the appellant has submitted that the alleged online transaction was done in a secured e-commerce environment which requires certain information pertaining to the credit card like transaction password, card CCV, card expiry date and VBV password known to cardholder only. This ensures that no third party can transact unless and until the information in personal and exclusive possession of the customer is shared at the payment gateway process while making the electronic transaction. In view of this, appellant claims to bear no liability for the transaction. On the other hand respondent claims that the online transactions happened in Russia at sprypay.ru-PETOZAVOSK and that he was not abroad at the time of these transactions. Learned Adjudicator has recorded that the police has made investigation into the case and submitted the following report:

"I. As per the letter received from the Respondent No. 1, fraudulent transactions have occurred in Russia.

II. The fraudulent transactions were made from computer system having IP address 180.215.88.235. Cyber Police Station, Bandar Karla Complex, Mumbai were requested to provide further details about the owner of this IP address. But no report is received from them."

A casual google search of the IP address reveals that this IP address belongs to someplace in India (this may not be accurate and only investigation may point it out correctly). In any case, as argued by the learned counsel of the appellant, physical presence is not necessary for online transactions and identity of the beneficiaries and their relationship with the appellant, when disputed, can be known and acted upon only by the investigation agency. Apparently, the

investigation in this case is incomplete and inconclusive, depriving appellant of the relief, if any. In such cases, investigating agencies are well advised to conclude cyber-crime cases promptly and in a time-bound manner. However, a complainant is entitled for compensation from appellant under section 46, if any violation of IT Act 2000 on part the appellant can be shown. The respondent has alleged violation of Section 43A on part of the appellant in his complaint and that complaint has been considered by the learned Adjudicator.

3. Appellant company SBI has been held responsible for violation of the Section 43A of IT Act by the learned adjudicator. Section 43A in The Information Technology Act, 2000 is as follows:

"43A Compensation for failure to protect data - Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation: -For the purposes of this section -

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised 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 the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) 'sensitive personal data or information' means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

4. There is no dispute that the appellant company is a "body corporate" within the above definition and that the credit card related information like card number, ccv, expiry date and VBV password are 'sensitive personal data or information'. However, we do not find any material in the impugned order to show that the appellant company was *"negligent in implementing and maintaining reasonable security practices"*. Respondent has alleged that OTP system was not followed by the appellant leading to negligence in implementing and maintaining security practices. Learned counsel for Appellant submits that OTP at the time was not mandatory and that in addition to other information, use of VBV password known to the customer only, was an accepted security practice. Appellant's case is that it has complied with the RBI guidelines since the transaction was secured by transaction password and also by Verified by Visa (VBV) password which ensures additional level of security. System of VBV password has been used extensively and it has not been shown that such system was compromised. In view of this, negligence in implementing and maintaining security practice is not established merely by alluding to the

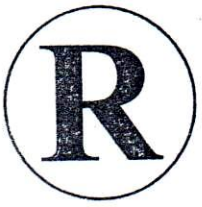
fact that OTP system was not offered by this Bank while some other Banks were doing so at that time.

5. Learned adjudicator has found deficiency in terms of Bank not giving any meaningful and detailed report about the internal investigation into crime by their FIU (Fraud Investigation Unit). What would be a 'meaningful' report is not elaborated. However, we note that the Bank has identified and given details of the alleged transactions with the report that all pre-requisite of a secured transaction were met with and that they were carried out in a secured environment. There is nothing on record to show that this information was not meaningful or what further information would be required for a meaningful report. Learned Adjudicator also holds that the Bank has not been able to explain through use of logs how the customer credentials got leaked out. This pre-supposes that the customer credentials got leaked out by the Bank. This has not been shown by any argument or fact or circumstances, except for a mere statement by the complainant that his credentials were leaked out by the Bank. On the other hand, learned counsel for the Appellant has pointed out that the complainant could have shared the password knowingly or unknowingly through phishing mail etc. It has also been held that the Bank does not seem to have any monitoring system to alert about suspicious transactions. Learned counsel for the appellant submits that the Bank has sent the SMS alerts (post transaction) to the complainant as required. Beyond this, Bank has to only ensure that the transaction happens in a secure environment and on the basis of card number, expiry date, cvv and VBV. In view of these

submissions, we are not persuaded to concur with the learned Adjudicator to hold the Appellant in violation of Section 43A of the IT Act.

6. Learned Adjudicator has mentioned about providing insurance coverage to the customers for electronic transactions as part of the best practices in banking and also as a consumer friendly measure. We can only observe and hope that the sector regulator and the participating banks will take note of such suggestions.

7. In facts of the case, the order under appeal is set aside and the appeal is allowed. No costs to either party.



.....

(S. K. Singh, J)
Chairperson

.....

(A.K. Bhargava)
Member