GAHC010007392013

THE GAUHATI HIGH COURT
(HIGH COURT OF ASSAM, NAGALAND, MIZORAM AND ARUNACHAL PRADESH)

Case No. : WP(C)/3085/2013

SMTI. JYOTI BEZBARUA GOSWAMI and 2 ORS.

2: SMTI. ANANYA GOSWAMI

3: SHRI TONMOY GOSWAMI

VERSUS

THE STATE OF ASSAM AND 6 ORS
REP. BY THE COMMISSIONER AND SECY. TO THE GOVT. OF ASSAM, HOME DEPTT., DISPUR, GHY- 6.

2:THE ADDL. DIRECTOR GENERAL OF POLICE CID
ULUBARI
GUWAHATI.

3:THE RESERVE BANK OF INDIA
REP. BY ITS REGIONAL DIRECTOR
PAN BAZAAR
STATION ROAD

GHY- 1.

4:THE STATE BANK OF INDIA
REP. BY ITS CHAIRMAN
STATE BANK BHAVAN
COPORATE CENTRE
MADAME CAMA MARG
MUMBAI
MAHARASTRA- 400021.

5:THE STATE BANK OF INDIA
PANJABARI BRANCH
REP. BY ITS BRANCH MANAGER
OPPOSITE GUWAHATI PSYCHIATRIC HOSPITAL
BAGHORBORI
BRANCH CODE 13292
GHY- 37.

6:THE BHARAT SANCHAR NIGAM LTD. BSNL
ASSAM CIRCLE
REP. BY THE CHIEF GENERAM MANAGER
TELECOM
ASSAM TELECOM CIRCLE
B.S.N.L.
ADMINISTRATIVE BUILDING
TELEPHONE EXCHANGE COMPLEX
PANBAZAR
GHY- 1.

7:THE OFFICER IN CHARGE
CHACHAL POLICE STATION
VIP ROAD
SIX MILES
GUWAHATI

Advocate for the Petitioner : MR.S BANIK

Advocate for the Respondent : GA, ASSAM

BEFORE

HON'BLE MR. JUSTICE KALYAN RAI SURANA

For the petitioner : Mr. S. Banik, Advocate.
For State respondent Nos.1, 2 and 7 : Mr. N. Goswami, Govt. Advocate.
For respondent No.3 : Mr. P. Hazarika, Advocate.
For respondent Nos.4 and 5 : Mr. S.S. Sharma, Senior counsel.

Mr. B.J. Mukherjee, Advocate.

Date of hearing : 20.06.2023.
Date of judgment : 18.09.2023.

JUDGMENT AND ORDER

(*CAV*)

Heard Mr. S. Banik, learned counsel for the petitioner and Mr. N. Goswami, learned Govt. Advocate for respondent no. 1, 2 and 7, Mr. P. Hazarika, learned counsel for respondent no. 3, and Mr. S.S. Sharma, learned senior counsel, assisted by Mr. B.J. Mukherjee, learned counsel for the respondent nos. 4 and 5. None appears on call for the respondent no. 6.

Case of the petitioner and submissions of his learned counsel:

2) The petitioner is the holder of account no. 11288865192, which is maintained in Panjabari Branch of the State Bank of India. The petitioner claims that an ATM –cum- Debit Card was issued to him on 29.03.2004, without e-commerce facility. It is projected that although subsequently e-commerce facility was provided to the petitioner by providing a 16 (sixteen) digit ATM –cum- Debit Card of the petitioner, but without informing him and without providing the CVV number, which is a security code to the said card. Accordingly, it is projected that without CVV, e-commerce or on-line transaction cannot be done through the said ATM –cum- Debit Card. It is also projected that the petitioner did not create '3D' password, which is mandatory for making on-line transaction through SBI secured gateway. It is also projected that the petitioner never made any On-line purchases by using his 16 (sixteen) digit ATM –cum- Debit Card. It is the case of the petitioner that between the period from 08.05.2012 and 17.05.2012, a sum of Rs.4,44,699.17 was swindled out of his account through illegal on-line transactions, however, without any sms alert

being received in his registered mobile number. On 17.05.2012, the petitioner lodged a complaint in State Bank of India, Panjabari Branch (respondent no.5), following by lodging of a *ejahar* before the Addl. Director General of Police (CID), Assam, which was registered as CID PS Case No. 53/2012 under section 420 IPC read with sections 66 and 66(d) of the Information Technology Act, 2000. Thereafter, the petitioner moved the Banking Ombudsman by filing a complaint, which was registered as Guwa.BKG. OMB/494/2012-13. The petitioner projects that his complaint was rejected by the Banking Ombudsman by order dated 02.04.2013 under Clause 13(c) of the Banking Ombudsman Scheme, 2006 as the determination would require consideration of documents and oral evidence.

3) Therefore, by filing this writ petition under Article 226 of the Constitution of India, the petitioner has prayed for an enquiry into the matter as to why sms alerts for on-line transaction to the extent of Rs.4,44,699.17 did not reach the petitioner's registered mobile no. 9435017059 and for directing the refund of the sum of Rs.4,44,699.17 along with applicable interest.

4) The petitioner had filed an additional affidavit on 28.06.2013, wherein a letter dated 02.06.2013 by the petitioner to Branch Manager, SBI, Panjabari Branch is annexed, thereby projecting that on 02.06.2013, he had received one sms from LM-SBICRD informing that transaction of Rs.233.01 on card ending with XX9944 was made at Mirage Hotel #1366912396 on 02.06.2013 had been declined and the petitioner was directed to call at 18601801290/ 39020202 for details. The petitioner projects that he had called 18601801290 and asked the customer care to block the card and issue a fresh card with different number and electronic data and that he had received electronic confirmation of the card being blocked. The petitioner had requested that as the failed transaction can be tracked, the bank should lodge and FIR.

5) The learned counsel for the petitioner had referred to the affidavit-in-reply filed by the petitioner against the affidavit-in- opposition filed by the respondent nos. 4 and 5 and it was submitted that the 16 digit ATM-cum-debit card was never activated or used and that the fraudulent transactions were made by use of 19 digit ATM-cum-Debit card, which admittedly did not support internet transactions. It was submitted that the sms alerts which was received by the petitioner between 08.05.2012 to 17.05.2012 were only in respect of ATM transactions and not for any internet transactions, which was not supported by the said 19 digit card. It was further submitted that while the 19 digit replacement card to the petitioner was issued on 19.01.2010, the unsolicited 16 digit card was issued to the petitioner on 29.07.2010.

Stand of the respondent no. 2 and submissions of the learned Government counsel:

6) On behalf of the respondent no. 2 i.e. the Additional Director General of Police (CID), an affidavit-in-opposition was filed by the Senior Superintendent of Police (CID), Assam, *inter alia*, stating that unknown criminals had committed the offence on-line through computer devices and that the investigation revealed that the crime of the case had originated from Thane District of Maharashtra and that the Investigating Officer had visited Maharashtra in connection with the case but the name and address of the suspect was found to be fake. It was stated that the Investigating Officer found 12 IP addresses out of which two address was found related to one Sarala Subhash Vanjari of Central Police Station area of Ulhas Nagar, Thane, Maharashtra, but the address of the suspect was found fake and that effort were being made to trace out the remaining 10 IP addresses. The learned Government advocate had further referred to the additional affidavit filed by the Superintendent of Police (CID), Assam and it was submitted that status report

of investigation dated 25.01.2019 was annexed thereto. As per the said report, till 16.06.2013, no report relating to IP addresses was received by the Investigating Officer and on submitting a fresh requisition for the same, the Nodal Officer, CID, Assam had informed that the internet service provider keeps log details for 6 (six) months and that IP details of more than 6 (six) months could not be provided. It was submitted that as per the said status report, the Investigating Officer had issued a requisition to the Branch Manager, SBI, Panjabari Branch to provide information on 6 (six) queries. However, as per the reply received from Panjabari Branch of SBI, it was disclosed that the bank account of the petitioner bearing no. xxxxxxxx192 (previous 8 digits are masked with letter 'x' in this order) was a joint account with his wife, which was active and that in respect of the said account mobile phone no. xxxxxxx059 (previous 7 digits is masked with letter 'x' in this order) was registered. It was also informed that card is required for POS purchase and if transaction is done on-line, then ATM card details was required for transactions.

7) The learned Govt. counsel had referred to the said status report and had submitted that the earlier Investigating Officer had neither seized the petitioner's mobile nor collected the CDR of the SIM for the period between 08.05.2012 and 17.05.2012 and therefore, there is no scope to verify the truthfulness of the version of the petitioner to establish whether he had received SMS alert or not and there is less scope for tracing out the accused of the case in near future.

Stand of the respondent no. 3 and submissions of their learned counsel:

8) The learned counsel for the respondent no. 3 had referred to the affidavit-in-opposition filed by the said respondent and it was submitted that highly disputed questions of facts was raised in this writ petition, which could

have been effectually and efficaciously agitated by approaching the Banking Ombudsman or by filing a civil suit. It was submitted that as per the RBI circulars dated 18.02.2009, 23.04.2010 and 29.03.2011, it was mandated that the banks should put in place a system of providing for additional authentication and/or validation based for all on-line transactions except IVR transactions.

Stand of the respondent nos. 4 and 5 and submissions of their learned senior counsel:

9) On behalf of respondent nos. 4 and 5, i.e. SBI, affidavit-in-opposition was filed by the Branch Manager, SBI, Panjabari Branch, wherein it was admitted, *inter alia*, that the card issued to the petitioner did not have e-commerce facility and that internet banking could not be done by the said card of 19 (nineteen) digits. It was further stated that the said card was lost and the petitioner had made a request for a replacement card, which was provided. It was also stated that since 2006, the bank's customers were provided with 16 (sixteen) digit ATM-cum- Debit cards with instructions to create his own 3D password and to keep it as a secret. It was projected that the petitioner must have given his card and a 3D password to someone, who carried out internet transaction. It was disputed that the petitioner did not receive sms alert for 35 internet transaction between 08.05.2012 and 17.05.2012 and it was stated that non-receipt of sms is only possible if the messages are diverted to another number. It was stated that without card and secret code, transactions could not have been made. It was admitted that the card was blocked on 17.05.2012. It was also stated that the 16 digit card was a new card and not a replacement card. It was also stated that the transactions could have been carried out only by logging of 3D password generated by the card holder.

10) In the additional affidavit-in-opposition filed by the respondent

nos. 4 and 5 on 09.05.2019, reference is made to the printout of the statement of accounts of the of the petitioner bearing no. xxxxxxxx192 and it has been stated that during the period from 08.05.2012 to 17.05.2012, the following transactions were made. On 08.05.2012, there were two entry of ATM withdrawals of Rs.1,200/- and Rs.500/-. On the same date there was one debit entry of Rs.916/- on clearing of cheque issued by the petitioner. On 16.05.2012, there were two entries, one was a WDL TFR of Rs.4,250/- and the other was ATM WDL of Rs.5,000/-. However, the rest of 40 entries during the period from 08.05.2012 to 17.05.2012 were towards on-line transactions using 19 digit card provided to the petitioner. The last entry was on 21.05.2012 for Rs.29,015 transferred from FR xxxxxxxxxx321 (first ten digits have been masked with letter 'x' in this order). It was emphatically stated in the said affidavit that it was not disputed that 16 digit card was not used/ operated by the petitioner and that all the on-line transactions were done through 19 digit ATM card. However, it has been stated that in 19 digit card, one need not wait for generation of OTP for each transaction from the bank and then to place orders by feeding card details, PIN number, etc. and thus, the bank or its officers were not responsible for cyber crime.

11) The learned senior counsel for the respondent nos. 4 and 5 had submitted that 19 digit cards could be used for making e-commerce and/or on-line purchases by feeding card details and PIN known to the petitioner, which he might have disclosed to others. It was submitted that when the petitioner had previously swiped his card, the merchant or merchant's staff could have known the card number and the PIN, and might have cloned the card and used it for on-line transactions, which was clearly a cyber crime and the bank or its staff were not responsible for commission of such crime.

12) Thus, from the pleadings of the petitioner and respondent nos. 4

and 5, it appears as follows:-

a. On 29.03.2004, a 19 (nineteen) digit ATM –cum- Debit Card bearing no. 6220180537700008551 was issued to the petitioner, which could not be used for on-line and/or e-commerce purchases. The said card is projected to be misplaced/ lost.

b. Therefore, a replacement 19 digit ATM-cum-debit card bearing no. 6220180537700030332 was issued to the petitioner. The petitioner claims that he had never made any request for on-line/e-commerce facility in his said card and had no knowledge of card being activated for on-line/e-commerce facility. Petitioner alleges that fraudulently, a sum of Rs.4,44,699.17 was swindled out of his account during the period between 08.05.2012 and 17.05.2012. Thereafter, the card was blocked on 17.05.2012. The date of issuance of the said ATM card is not pleaded either by the petitioner or by the respondent nos. 4 and 5.

c. As per the RTI reply dated 02.03.2013 provided by the AGM (Premises & Estates) & CPIO, State Bank of India to the petitioner, e-commerce facilities to debit card was introduced in December, 2006.

d. The petitioner was provided by a 16 (sixteen) digit ATM-cum- debit card. In their additional affidavit-in-opposition, the respondent nos. 4 and 5 have admitted that the said 16 (sixteen) digit ATM-cum-debit card was not used and by lapse of time, it had expired on 16.04.2014.

13) Thus, it appears that during the currency of a 19 (nineteen) digit ATM-cum- Debit card, the petitioner was provided with 16 (sixteen) digit card.

14) As per the stand taken by the respondent nos. 4 and 5 in para 5 of their additional affidavit-in-opposition, to carry out on-line transactions

through the said ATM card, one was not required to wait for generation of OTP for each transaction from the bank and then to place order by feeding card details and PIN number and that the system of generating OTP was introduced in and around March, 2015.

15) Nonetheless, as per the petitioner's RTI application dated 10.10.2012, which is annexed to the additional affidavit-in- opposition filed by the respondent nos. 4 and 5, the admitted position of the petitioner is that the 19 (nineteen) digit ATM-cum-debit ward was a 'shopping' card and that as per the SBI's RTI reply dated 30.10.2012, the said card had e-commerce facilities and that the elaboration was given in the manual supplied by the card vendor along with the kit.

16) As per the stand of the CID, Assam, during their investigation carried out in CID PS Case No. 53/2012, registered under section 420 IPC read with sections 66 and 66(d) of the Information Technology Act, 2000, they could trace out that crime of the case had originated from Thane District of Maharashtra and that the Investigating Officer had visited Maharashtra in connection with the case but the name and address of the suspect was found to be fake and that out of 12 IP addresses, the Investigating Officer found that two address related to one Sarala Subhash Vanjari of Central Police Station area of Ulhas Nagar, Thane, Maharashtra, but the address of the suspect was found fake. The CID could not trace out the remaining 10 IP addresses. The Nodal Officer, CID, Assam had informed the Investigating Officer that the internet service provider keeps log details for 6 (six) months and that IP details of more than 6 (six) months could not be provided. The CID neither seized the petitioner's mobile nor collected the CDR of the SIM for the period between 08.05.2012 and 17.05.2012. Therefore, there is no scope to verify the truthfulness of the version of the petitioner to establish whether he had received

SMS alert or not and there is less scope for tracing out the accused of the case in near future. The respondent nos. 4 and 5 have not produced any record to show that sms alert against alleged fraudulent transactions were generated and sent from their computer system.

17) The petitioner had reported to the call centre number of the State Bank of India about unauthorized withdrawal and therefore, on 17.05.2012, the petitioner's 19 (nineteen) digit ATM card was blocked. But the respondent nos. 4 and 5 did not preserve their record of having sent sms alert to the petitioner regarding e-commerce/ internet use of his ATM card.

18) The respondent nos. 4 and 5 had not disclosed when the 19 digit ATM card no. 6220180537700030332 was issued to the petitioner, the date when it was activated for e-commerce and/or internet transaction. The respondent nos. 4 and 5 have also not pleaded that since the issuance of ATM-cum- debit card, the petitioner had been using it for e-commerce and/or internet transaction even before the disputed transactions done between 08.05.2012 and 17.05.2012.

19) Therefore, in this case, 35 (thirty-five) transactions take place between the short period from 08.05.2012 to 17.05.2012. Out of these transactions, the State CID had been able to locate 12 IP addresses in Thane District, out of which 2 (two) IP addresses are fake. Therefore, the preponderance of probability is that the petitioner is a victim of cyber-crime. The respondent nos. 4 and 5 have not been able to show that any sms alerts were issued to the petitioner for all these transactions disputed by the petitioner.

20) In light of the discussion made above, the Court is of the considered opinion that transactions that had taken place from the account of

the petitioner vide 19 digit ATM Card No. 6220180537700030332 between 08.05.2012 and 17.05.2012 to the extent of Rs.4,44,699.17 were unauthorized and fraudulent in nature because as per the investigation carried out by the State CID, they could find that 12 of the IP addresses through which transactions were made were located in Thane district in the State of Maharashtra. Therefore, the petitioner is not found to have any liability in respect of the said transactions to the extent of Rs.4,44,699.17. These transactions are reflected in the statement of bank account of the petitioner, which is annexed to the affidavit filed by the respondent nos. 4 and 5. Therefore, the respondent nos.4 and 5 are required to reverse the said amount in the savings bank account of the petitioner. However, with liberty to recover the said from the persons to whose account said money or part thereof were siphoned off. Consequently, the respondent nos.4 and 5 are directed to deposit a sum of Rs.4,44,699.17 in the bank account of the petitioner within an outer limit of 60 (sixty) days from the date of service of a certified copy of this order to the State Bank of India, Panjabari Branch (respondent no.5).

21) It is also provided that in the event the money is not deposited in the bank account of the petitioner within the time allowed, the said amount shall carry interest @6% p.a. from the date of the order till realization.

22) Parties are left to bear their own cost.

JUDGE

Comparing Assistant