# OFFICE OF THE ADJUDICATING OFFICER,
# GOVERNMENT OF GUJARAT,
# DEPARTMENT OF SCIENCE & TECHNOLOGY,
**Block No: 7, 5th Floor, Sardar Bhavan,**
**Sachivalaya, Gandhinagar.**

**SPECIAL CIVIL APPLICATION NO. 60**

**DATE OF DECISION: 04/05/2018.**

**IN THE MATTER OF:**

**Shri Vivek Johri,**
**31-32 Tulsi RowHouse,**
**Jodhpur Gam Road, Nr. Jain Derasar,**
**Satellite, Ahmedabad-380015,**
**Gujarat.....Petitioner**

**Vs**

**The Branch Manager,**
**M/s State Bank of India**
**Ashram Road Branch, Nr. Gujarat Vidhyapith Premises,**
**Ahmedabad-380009,**
**Gujarat.....Respondent**

**MR. DHNANJAY DWIVEDI**
**ADJUDICATING OFFICER UNDER**
**INFORMATION TECHNOLOGY ACT, 2000**

This matter has been filed by the petitioner under Section 43-A of the Information Technology Act, 2000. The complainant is a resident of Ahmedabad. The complainant was maintaining an account with the State Bank of India, Ashram Road Branch, Ahmedabad. The complainant was maintaining an account with No. ********935. At the time of making complaint, the complainant was using internet banking facility for the account for which the Cell Number of the complainant bearing No. *******092, was used for the purposes of receiving alerts from the bank.

2. The brief of the details as mentioned by the petitioner is as follows:

a) The petitioner has mentioned in the case that "an amount of Rs 405000/- was withdrawn between 2:05 AM to 5:15 AM in wee hrs of 08th October, 2016. The amount was being transferred as shown in bank statement "TO TRANSFE INB

SBIBUDDY". The first entry debiting Rs 10000/- in my (here is petitioner) account and the last entry is "TRANSFER-INB SBIBUDDY". The transactions right from 2:05 till 5:15 show complete carelessness of your (here is respondent bank) system who is monitoring internet banking all through 24hrs of the day."

b) The petitioner has also mentioned that "Immediately at 5:40 am 8th October, 2016 contacted SBI Helpline No 18004253800. Talked to the representative attending calls at Help Centre and he refused to give any help. I (here is petitioner) asked to lodge my (here is petitioner) complain and inform his (here is respondent bank) higher authority. He (here is respondent bank) refused to lodge a complaint as told that facility is not available to them hence no complain no can be given. The SBI was closed next three days because of as 08th being closed Saturday, 9th October being Sunday, 10th October being government declared holiday and 11th October being Dussera Holiday." The petitioner has mentioned in his application that "he has lodged FIR on 08th October 2016 morning at Crime Branch, Cyber Cell at Dafnala, Ahmedabad. Met AGM SBI Ashram Road Branch on 13th October 2016 and also handed over to him (here is respondent bank) detailed letter."

c) The petitioner has mentioned in his application that "Second consecutive theft repeated on 13/10/2016 of Rs 10000/- , despite SBI had frozen the account in response to letter issued by Policy Cyber Crime Cell, Dafnala, Ahmedabad on the basis of FIR lodged with them by me (here is petitioner) on 08th October 2016 morning around 11:30 AM. But again theft from the same savings account on 13.10.2016"

3. This matter has been filed by the petitioner under Section 43-A of the Information Technology Act, 2000 to this office for the aforesaid case.

4 The matter was heard on 20.04.2017, 30.06.2017, 21.07.2017, 11.08.2017 and 02.02.2018

5. In the hearing held on 20.04.2017, SBI was asked to provide details 41 Account of SBI buddy along with the account holder, KYC details, what is the balance in each of 41 buddy accounts and freeze from each buddy account Rs 10000/- when 10000 was moved and Rs 5000/- where 5000 was moved.

6. In the hearing held on 30.06.2017 and 21.07.2017, SBI was again asked to provide the details of 41 transactions details of SBI regarding transfer of money to which bank or which holding accounts, who is responsible person for that organization, what is the balance in 39 wallets, submit the transaction details of OTP and OTP for add beneficiary, what is the SBI policy for adding beneficiaries in same day, transactions in same hour / same day, details of Call centre record of conversation and ATR on 08th October, 2016 (@ 5:15 am) and log details of change login credentials from 05/10/2016 to 14/10/2016 of the petitioner account."

7. Based on the above para 7 and hearing held on 21.07.2017, SBI has submitted the information to undersigned wherein SBI has mentioned "SBI has provided the details of SBI Buddy transactions in the account are from 08.10.2016 to 13.10.2016 with the account of these transactions. The money is transferred to SBI Buddy Accounts of various beneficiaries. SBI INB Customer who has SBI Buddy application can add beneficiary event if he / she is not registered for SBI Buddy. The SBI Customer can add number of beneficiaries. The money is not transferred to any financial institution / organisation but it is in Electronic Form in the wallet of the beneficiary. SBI has also mentioned that "at time of transfer of fund to the beneficiary wallet though SBI Buddy no OTP is generated" in letter dated 09.08.2017 with the details of log.

8. The matter was heard on 11.08.2017 and SBI was again asked to provide the log details of SMS sent during the window when 41 transactions happened, Policy of SBI for buddy as well as online banking with no. of transitions, value of transactions, and rate of transactions (per hour, value per hour, per day), details of Call centre record of conversation and ATR from 07th October, 2016 to 14th October, 2016 and log details of change login credentials from 05/10/2016 to 14/10/2016 to this office.

9. In the hearing held on 02.02.2018, SBI has submitted the log of SMS details sent during the window when the transactions happened and Policy of SBI Buddy as well as online banking facility. SBI has mentioned in letter dated 02.2.2018 that "The no. of transactions and value of each transaction is decided by the user at the time of setting up the instructions by adding users using his / her profile password for transitions through online banking. The rate of transactions depends on the user option to schedule the payment instantly or pay latter at specified time."

10. Also SBI has submitted the details of Call Centre Records of Conversation and ATR from 07.10.2016 to 14.10.2016 and submitted the log details of change login credentials as asked, contained in the CD.

## ORDER

On perusal of the facts, it comes out that the petitioner maintained an account with the State Bank of India with a facility of internet banking. On 8th October, 2016, from 2:05 AM to 5:15 AM in a short span of less than 3 hours, through 41 transactions, an amount of Rs. 4.05 lakhs was transferred. Out of which 40 transactions of Rs. 10,000/- each were made into different mobile wallet accounts and a transaction of Rs. 5,000/- was made on an online site. It also appears that last of Rs. 10,000/- transaction was reversed on 10th October, 2016 whereupon another transaction of Rs. 10,000/- was made to mobile wallet account on 13th October. Thus, on a whole, petitioner has lost Rs, 4,05,000/- in transactions which were neither carried by him nor authorised by him.

2. Immediately after the occurrence of transactions, at 5:40 AM on 8th October, 2016, the petitioner called the official SBI helpline complaining about the unauthorised transactions and seeking a remedy. The SBI representative has submitted a recording of the audio conversation in relation to the alleged complaint. It appears that while the petitioner did mention about unauthorised transaction to mobile wallets, the counterpart at the call centre advised the petitioner to approach the Manager of the bank after opening of the bank during the day. The conversation also reveals that on the first call, the call centre executive could not appreciate the substance of the complaint and instead advised current petitioner for opening of a mobile banking account. This reflects not just the inadequacy of a

grievance redressal mechanism at the SBI level but also reflects lack of skill sets of the person(s) tasked with servicing customer grievances. The net result was precious five hours were lost before the bank Manager could initiate any action, which could otherwise have been important in processing stop transactions or hold transaction instructions.

3. Given that after the incident of 8th October was reported, one tranche of Rs. 10,000/- transaction was rejected and returned to the complainant's account on 10th October. The same amount was once again unauthorisedly transferred on 13th October to mobile wallet account speaks volumes on the inadequacy of grievance redressal mechanism at the bank to advise its customers for protecting their accounts (changing password would have been the most basic step).

4. Considering the fraudulent transfers, the SBI was asked to intimate its policy for online transfer of amounts to mobile wallets. The bank has provided a copy of the policy which mentions that any person can download the mobile wallet and can start transacting without any need for a separate KYC authentication from the bank. It appears that entire mobile wallet business runs on trust and the sanctity of KYC compliance by the mobile service providers. Unfortunately, that is not so, as it comes out all the mobile wallet owners who got transferred money in instant case are not traceable today.

5. It also comes out that whereas online banking transaction to any other bank account requires payee to be added and authenticated through an OTP and activated after a delay of minimum four hours, it is not necessary to do a separate transaction to add a mobile wallet or to authenticate it nor an OTP is required for it. This is a serious lacunae in the KYC as well as transaction authorisation policy of the bank. As it appears in the case of the complainant, he had only Rs. 4,05,000/- in his account which were completely siffoned off in tranches of Rs. 10,000/- each, and the fraudster had full access to the petitioner's account (except for the mobile phone which gets OTP). Had there been Rs. 50.00 lakhs in his account or any other amount in his account the fraudster would have succeeded in emptying entire amount. While inadequacy of reasonable security policy would not make the State Bank liable to compensate petitioner strictly from the perspective of Information Technology Act - sections 43 and 45, this one big lacunae still needs to be addressed as early as possible. Since the transaction related policies are advised by the Reserve Bank of India (RBI) and would be, subject to minor variation, be common to all the banks across the country; I deem it fit to recommend to the Governor, RBI, to evaluate the desirability of having mandatory two

factor authentication for transferring funds between mobile wallets or from online bank account to mobile wallets.

6. Each bank is supposed to have software based platform which would have the ability of detecting suspicious or fraudulent transaction. Few criterias for flagging such suspicious looking transaction would be transacting at odd hours, making multiple transaction in a very short period of time, size of a transaction which has previously never happened for the specific amount etc. It is desirable that the banks strengthen fraud prevention mechanism of their online banking platform. An option to supplement two factor authentication would be an additional confirmation either through mail or through a telephonic call in case of suspicious looking transaction(s). Through this order, I would request the RBI to examine possibility of devising a guideline for the same.

7. From the experience of Adjudicating Officer, it is worthwhile to mention that many citizens suffer this kind of fraudulent transactions due to their lack of awareness for data privacy. Many fall pray to tricks eventually sharing information relating to credit or debit cards or account login password or OTPs. Few account holders are alert and they try to reach out to the bank's public helpline to report such transaction. It is desired that a separate fraud prevention mechanism should be set up which should have access to the transaction infrastructure of the bank with sufficient responsibility and privileges. The persons manning such fraud prevention infrastructure could have the authorisation of stopping a transaction or deferring settlement of transaction and reversing the transaction in case there is a prima facie substance in the complaint of fraud. The sweet spot in terms of the transaction settlement time that retains the settlement efficiency yet gives a window for detecting and mitigating a fraud needs to be identified. It is recommended that the RBI would also examine the possibility of creating such a mechanism and would issue necessary advisories to all the banks.

8. Considering the present case, it appears that whosoever was the fraudster, he had obtained the user ID and password of the petitioner's account for which the bank cannot be blamed and therefore, the bank cannot be held responsible beyond the inadequacy of their policy for lack of second factor authentication. However, the response of the call centre to the complaint made at 5:40 in the morning, and lack of minimum expected advice to the petitioner to change his credentials (though it was also expected of the petitioner considering his education and professional experience) resulted in yet another transaction

on October 13 of Rs. 10,000/- which could, otherwise, have been prevented. In a sense, given the situation that the petitioner underwent on the night of October 8, it was expected of the bank to be more vigilant and to have been more supportive to the petitioner. It was also expected of the bank to have evaluated such unauthorised transaction from bank accounts to mobile wallets without second layer of security (OTP etc.). Under the circumstance, I feel that a token penalty of Rs. 20,000/- should be levied on the respondent Bank i.e. the SBI, Ashram Road Branch (Branch Code 2628) so as to sensitize the senior management to be more vigilant and supportive to the victims of unauthorised / fraudulent transactions.

9. The respondent Manager of the SBI shall pay Rs. 20,000/- to the petitioner within a period of 15 days. The Governor, RBI, may take appropriate action as recommended in the Order and may share an action taken report within a period of three months.

**(Dhananjay Dwivedi)**
**Adjudicating Officer under Information Technology Act, 2000 for the State of Gujarat.**