**BEFORE THE ADJUDICATING OFFICER**

**SH. S.V.R. SRINIVAS**

**PRINCIPAL SECRETARY, INFORMATION TECHNOLOGY**

**GOVERNMENT OF MAHARASHTRA**

**Complaint No. 39/2016 dated 9th August, 2016**

**IN THE MATTER OF**

| | |
|---|---|
| Mr. Rajkumar Shreelal Singhee | ..... Complainant |
| **Versus** | |
| Gajanan Doye/Shreemant Services, Gondia | ..... Respondent No. 1 |
| IDEA Cellular Limited (AT&T), Nagpur | ..... Respondent No. 2 |
| A T and T Services Ltd. (IDEA Cellular), Pune | ..... Respondent No. 3 |
| United Bank of India (Shankarnagar Branch), Nagpur | ..... Respondent No. 4 |
| Punjab National Bank (C A Road Branch), Nagpur | ..... Respondent No. 5 |
| Saraswat Bank (Gandhibag Branch), Nagpur | ..... Respondent No. 6 |
| State Bank of India, West Bengal | ..... Respondent No. 7 |
| Satyajeet Biswas (SBI Account), West Bengal | ..... Respondent No. 8 |
| UCO Bank, West Bengal | ..... Respondent No. 9 |
| Sandipan Ghosh (UCO Bank Account), West Bengal | ..... Respondent No. 10 |
| ICICI Bank, West Bengal | ..... Respondent No. 11 |
| Sujata Dresses Prop. Pintukumar Kandu (ICICI Account), West Bengal | ..... Respondent No. 12 |
| IndusInd Bank, West Bengal | ..... Respondent No. 13 |
| Milan Ray (ICICI Account), West Bengal | ..... Respondent No. 14 |
| Priti Vishwas Ghosh (IndusInd Account), West Bengal | ..... Respondent No. 15 |

Advocates:

| | | |
|---|---|---|
| 1. | For Complainant | : Adv. Shri Mahendra Bhaskar Limaye |
| 2. | For Respondent No. 1, 2 & 3 | : Bharucha & Partners, Advocates & Solicitors: |
| 3. | For Respondent No. 5 | : M/s. INTRALEGAL, Advocates & Consultants |
| 4. | For Respondent No. 6 | : M Mulla Associates, Advocates & Solicitors |
| 5. | For Respondent No. 9 | : SKR & Associates |
| 6. | For Respondent No. 11 | : SNG & Partners, Advocates & Solicitors |
| 7. | For Respondent No. 13 | : Adarsh Jayaswal |

GOVERNMENT OF MAHARASHTRA * ADJUDICATING OFFICER (I.T.) * सत्यमेव जयते MUMBAI

**ORDER**

The order pertains to loss on account of duplicate Sim Card given to a person who allegedly was not the real owner of the Mobile Sim Card. The complainant Mr. Rajkumar Shreelal Singhee r/o Flat No. 303, Swami Apartment, Plot No. 47, Ramdaspeth, Nagpur-12 avers that the monetary damage suffered by him on account of this in 2016 has not been compensated by the Respondents No. 1, 2, 3, 4, 5, 6, 7, 9, 11 & 13. It is alleged that the loss is caused by the action of these respondents.

The complainant is the proprietor of Suryodaya Metal Craft Pvt. Ltd., Sanket Steel Industries and Swastik Refrigeration located at Nagpur. The complainant has accounts with United Bank of India (A/c No. 1258210031851), Punjab National Bank (A/c No. 0353002100965426) and Saraswat Bank (A/c No. 067500100000271) for above said business units. The complainant's mobile number 9822227982 is registered with these banks. The complainant is using this mobile number since last 10 years, as stated by the complainant.

On July 2, 2016 evening, the complainant noticed that his mobile had no connectivity. The complainant, on visiting the office of Respondent No. 2, was informed by the service provider that new duplicate Sim Card was issued on the number of complainant on July 2, 2016 by one of the dealers (Respondent No. 1). The complainant protested the said unauthorised activation of his Sim Card without his consent. On July 4, 2016, the Respondent No. 2 issued a new Sim Card to the complainant on the same mobile number and informed the complainant that mobile will be activated after complete verification is done.

On July 5, 2016 morning, complainant received two messages from United Bank regarding debit of Rs.5,00,000 each. On visiting the office of Respondent No. 4, the complainant observed that a total of Rs.17,00,000 was transferred from his United Bank of India's account on July 4 & 5 through NEFT and RTGS mechanism. On verifying with his other accounts also, the complainant observed that his Punjab National Bank and Saraswat Bank accounts were also showing fraudulent transfer of Rs.3,70,000 and Rs.6,00,000 respectively. It is claimed by the complainant that all these NEFT/RTGS and mobile mechanism transfers were not authorised by the complainant.

GOVERNMENT OF MAHARASHTRA ★ ADJUDICATING OFFICER (I.T.) ★ सत्यमेव जयते MUMBAI

A police complaint was lodged in this respect on July 6, 2016 at Tahsil Police Station, Nagpur vide FIR No. 135/16. The matter was investigated by the police who came to the conclusion on the basis of the documents including complainant's plea and the responses given by the Respondents investigated by the police.

The immediate reason for the occurrence of unauthorised transaction in the bank account of the complainant appears to be a duplicate Sim Card issued by Respondent No. 1 (Respondent No. 1 is a franchise of Respondent No. 2) without properly verifying the KYC of the person requesting for a duplicate Sim Card. It was also alleged by the complainant that there is lack of reasonable security practices and procedures by the banks, i.e. Respondent Nos. 4, 5 & 6 as the complainant used to carry out RTGS/NEFT transactions by issuing cheque and never through online fund transfer option, except in matters of government tenders and the same deviation was not caught by the Respondent Banks. It was alleged by the complainant that Respondent Nos. 7, 9, 11 & 13 being the beneficiary banks, did not follow the KYC norms while opening accounts. Therefore, it is claimed that the financial loss suffered by the complainant be compensated by these respondents.

In response, the Respondent No. 2, on behalf of Respondent Nos. 1, 2 & 3 (IDEA vide reply dated July 26, 2017) stated that they have implemented all security practices and layers mandated by the DOT and TRAI Guidelines and that the complainant and Respondent Banks has been negligent in keeping his account details safe and confidential. Respondent No. 2 stated that the request for issue of duplicate Sim Card was made by the fraudster citing loss of Sim Card as the reason and documents given for the same, i.e. Pan Card copy with name of Rajkumar Singhee and the request form signed by the said fraudster, were properly verified. Since complainant had not provided his registered email address to the Respondent, notification of Sim Card change was sent on the alternate mobile number of the complainant. Respondent No. 2 also stated in their written response dated August 14, 2018 that the bank transfer cannot be completed without a Customer ID or Login ID, and the same cannot be recovered or changed using mobile number.

In response, the Respondent No. 4 (United Bank of India, vide reply dated August 13, 2018) stated that the details of the transactions were delivered to the complainant via SMS alert and all beneficiaries were added on July 2, 2016, the information of which was also sent to the complainant.

GOVERNMENT OF MAHARASHTRA
सत्यमेव जयते
MUMBAI
ADJUDICATING OFFICER (I.T.)

No deviation in the system with respect to security and OTP based transaction and no lapse in Bank's internet banking were observed by the Bank. Respondent No. 4 stated that the complainant must have compromised with the login and transaction passwords and that the complainant should have visited the Bank immediately on noticing the registered mobile number had no connectivity, in order to avoid illegal transactions.

In response, the Respondent No. 5 (Punjab National Bank, vide reply dated August 9, 2018) stated that the fraud was practiced by creating duplicate Sim Card facilitated by Respondent Nos. 1, 2 & 3. Respondent No. 5 stated that SMS intimation was served for the transaction in question on the registered mobile number of the complainant. Meaningful investigation through Fraud Investigation Unit was carried out by Respondent No. 5, as stated by them. Respondent No. 5 stated that they have necessary checks and balances to ensure that no fraud takes place and have all KYC norms in place.

In response, the Respondent No. 6 (Saraswat Bank, vide reply dated August 6, 2018) stated that they have undertaken measures to mitigate the risks of unauthorised use of the customer's online banking and mobile banking facilities and have inbuilt codes in their software systems to avoid suspicious transactions. Respondent No. 6 stated that the person who accessed the online banking of the complainant was already aware of the login and passwords and the bank only generated the OTP when it was requested from the registered mobile number. Respondent No. 6 stated that the IP address from which the fraudulent transaction took place is the same IP address from where number of other transactions have been carried out by the complainant. They also said that they have taken all necessary actions in relation to complainant's online banking account as directed by him.

In response, Respondent No. 9 (UCO Bank vide reply dated August 13, 2018) stated that on July 4, 2016, Rs.5,00,000 were credited to the beneficiary's account in question through RTGS and on the same day the amount was withdrawn using six transactions. Post this, no transaction was carried on by the beneficiary in the account in question and hence, the said account has been placed under "Dormant Status" by Respondent No. 9 as stated by them.

GOVERNMENT OF MAHARASHTRA
सत्यमेव जयते
MUMBAI
ADJUDICATING OFFICER (I.T.)

In response, Respondent Nos. 11 & 13 (ICICI Bank and IndusInd Bank, respectively vide respective reply dated August 8, 2018) stated that all KYC norms were followed at the time of opening the accounts of the beneficiary. They had marked the account with debit freeze immediately on intimation of fraudulent transactions, as stated by Respondent Nos. 11 & 13.

Hearings were conducted for this matter on June 22, 2017, July 26, 2018 and final hearing on August 9, 2018. All the parties were given equal chances to be heard and submit their averments and written statements. All the parties were present in these hearings, other than Respondent No. 7, State Bank of India. No written statement has been submitted by Respondent No. 7 and no representative was present for any hearing.

On the basis of averments and the written statements submitted by the complainant as well as the respondents, it is clear that the loss was caused to the complainant due to the duplicate Sim Card issued to the alleged fraudster without following the KYC norms. The Respondent No. 1 should have thoroughly checked all the relevant documents before issuing a duplicate Sim Card, as per telecom guidelines. The complete name as well as the signature of Mr. Rajkumar Shreelal Singhee on the Pan Card should have been properly tallied. This does not seem to have been done by the IDEA franchise. Because of this issuance of duplicate Sim Card, the money transfer was facilitated and as a consequence, a loss of Rs.26,70,000 was caused to the complainant. As far as the responsibility of Respondent Banks and other beneficiary banks is concerned, they seem to have followed all the norms and security measures.

In the final analysis, the responsibility of Respondent No. 1, 2 & 3 is quiet serious and cannot be condoned. The undersigned, therefore, directs that the complainant be compensated Rs.26,70,000 as the loss was caused due to the issuance of duplicate Sim Card by Respondent No. 1, 2 & 3 without proper due diligence. Respondent No. 1, 2 & 3 are directed to pay the said amount to the complainant within one month of the receipt of this order.

The case is disposed as of above. No order as to costs.

GOVERNMENT OF MAHARASHTRA ★ ADJUDICATING OFFICER (I.T.) ★ सत्यमेव जयते MUMBAI

14/8/18

(S.V.R. Srinivas, IAS)
Principal Secretary (Information Technology)
Government of Maharashtra,
Mantralaya, Mumbai 400 032