BEFORE THE ADJUDICATING OFFICER

SH. RAJESH AGGARWAL,
PRINCIPAL SECRETARY, INFORMATION TECHNOLOGY,
GOVERNMENT OF MAHARASHTRA

Complaint No. 30 of 2013 dated 26th September 2013

IN THE MATTER OF

1. Sh. Sanjay Govind Dhande
2. Dr. (Smt.) Medha Sanjay Dhande
3. M/s Sango Consultants Pvt. Ltd.

…….. **Complainants**

Versus

1. Branch Manager, ICICI BANK, Audh Branch, Pune
2. Vodafone Store, Wakdewadi, Shivajinagar, Pune
3. Vodafone India Ltd., Corporate Office

…….. **Respondents**

Advocates:

1. For complainants - Adv. Prashant Mali & Adv. Vaishakh Raut
2. For Respondent No. 1 - Adv. Partha Banerjee, Adv. Sharon Pinto, Adv. Saee Jondhale, Adv. Khushboo Sinha, Adv. Ayushi Agarwal, Adv. Kehkasha Sehgal, Adv. Ranju Yadav & Adv. Samreen
3. For Respondent No. 2 and 3 - Adv. Yogesh Nayak & Adv. Sameer Sibal

This is proceedings of a complaint filed by the complainant for Adjudication under section 46 of the Information Technology Act, 2000. In keeping with the basic principles of natural justice and reasonable opportunity, detailed hearings were held in which both parties i.e. the Complainant and the Respondents were presented with equal and adequate opportunities to present and defend their case. Following the completion of hearing and response of all concerned parties, conclusion has been arrived at and the judgment is being delivered herein.

ORDER

1. **Brief Facts of the Case as per Complainants are as follows:**

I. Complainant 1 and 2 are the Directors of M/S Sango Consultants Pvt. Ltd, Pune which is listed as Complainant No. 3. Complainants hold a Current account bearing No 007305008xxx with ICICI Bank, Aundh Branch, Pune (Respondent No. 1).

II. Complainants state that, between dates 6th to 10th September 2013, many fraudulent fund transfers amounting to about Rupees 19 lacs were done by an Unknown persons from their account.

III. Complainant 2 states that the current account is linked with the mobile number (8552902xxx) which was issued by Respondent No. 2.

IV. Complainant 2 states that, Respondent No. 2 and 3 (Vodafone) have not taken adequate safeguards to protect Complainant's data with them. Respondent No. 2 issued a duplicate SIM Card of Complainant's Mobile Number to Fraudsters without cross-checking the documents submitted by the fraudsters with the Original identity documents which were submitted by the Complainant. Due to this act of Respondent No. 2, fraudsters have managed to commit grave illegal act and has caused great financial loss to the Complainants.

V. Chronological Events:

a. On 6th September 2013, the Complainants mobile phone stopped functioning in proper manner.

b. On 7th September 2013, Complainants through their family driver contacted Vodafone Shop located in Sanghvi, Pune. The concerned Representative of Respondent No. 2 checked the phone and informed that the Phone instrument is working properly, but, the SIM card needs to be replaced.

c. Complainant states that as September 8th and 9th were holidays, the Complainant contacted Vodafone office (Respondent No. 2) on 10th September 2013. Complainant submitted an application for new SIM Card with all the verification proofs such as copy of PAN Card and photograph etc. and a new SIM card was issued by Respondent No. 2 Complainant states that however, the calls were getting diverted to some other number. Hence the Complainant again contacted Respondent No. 2 office and they corrected the database and the phone number started functioning properly from evening hours of 10th September 2013.

d. Complainant states that during the period when their mobile was non-functional, the fraudulent transactions took place, and amount to the tune of Rupees 19,01,073.16 was fraudulently siphoned off.

e. Complainant states that it is admitted position by Respondent No. 2 that the fake SIM card was indeed issued by Vodafone on 6th September 2013 at their franchisee office in Nagpur. This information was revealed to Complainant when he went to submit a complaint to Vodafone on 16th September 2013.

f. Complainant initiated a police complaint and FIR was registered with Chaturshringi Police Station, Pune bearing CR No. 315/2013 on 14th September 2013, and later the case was transferred to Cyber Crime Cell, Pune for the further investigation.

VI. Complainants have submitted Copy of the Bank account statement, Copy of the FIR registered at Chaturshringi Police Station, Pune, Copy of the correspondence with Dy. Branch Manager, ICICI bank, Aundh Branch, Pune dated 11th September 2013, Copy of the correspondence with Dy. Branch Manager, ICICI bank, Aundh Branch, Pune dated 16th September 2013, and Copy of the correspondence with MD & CEO, ICICI bank, Mumbai, dated 21st September 2013.

2. In their written arguments and oral arguments, Respondent 1, i.e., ICICI Bank has made following points:

I. They have submitted Copy of List of Transactions, Copy of Customer Relationship form, Copy of Terms and Conditions of Corporate Internet Banking, and Copy of Terms and Conditions Governing Mobile Banking Facility.

II. Complainant was a frequent user and well versed with the internet banking facility of ICICI Bank.

III. Complainant has filed police complaint and FIR bearing no. 315/2013 with Chaturshringi Police Station, and the same is under investigation and the culprit is yet to be ascertained. Hence, unless the detailed inquiry & final report is submitted by the investigating agency, the Complainant should not be given any interim relief.

IV. Respondent No. 1 has no role to play in the complaint under reply and hence the complaint should be dismissed against the Respondent No. 1. Most of the allegations are made against Respondent No. 2 and 3.

V. Unless the information from the registered mobile is received with regards to any dispute/transaction, the Bank can't restrict any of the transaction initiated by the account holder, as SMS for every transaction is sent to the customer mobile no. registered with ICICI Bank Ltd.

VI. The allegations that the rapid pace with which these fraudulent transactions have taken place indicate the lax attitude of Respondent No. 1 and they should have verified and cross checked the transactions with the Complainant before completing the said transactions is completely false, baseless and is against the Terms and Conditions agreed and accepted by the complainant before availing the Corporate Internet Banking facility of ICICI Bank.

VII. Customer is responsible for maintaining the security of his internet banking ID, password and transaction password.

VIII. A Payee is not registered unless an URN (Unique Registration Number) generated by the bank is filled in by customer for confirming the payee. The URN is sent to the customer on his registered mobile number. Further, for making any payments as fund transfer for the customer is required to fill in the details of the grid which is affixed to the backside of the debit card.

IX. ICICI Bank has not only extended all support to the investigation but has also taken serious action to get part of the amount recovered from the fraudster's/disputed beneficiaries' ICICI Bank account after coming to know about the fraudulent transactions and was able to recover a sum of Rupees 3,26,604.17. ICICI Bank had also immediately frozen the Complainant's account so that further fraudulent transfer could be prevented. The account was however unfrozen and regularized on the basis of the order of the Adjudicating Officer dated 8th October 2013. Further the monies recovered from the accused persons were immediately credited to the Complainant's account by the ICICI Bank.

3. Papers submitted by Vodafone – Corporate Office (Respondent No. 3):

They have submitted Copy of Customer Agreement Form dated 30th August 2012, Copy of the PAN Card and Electricity Bill of the Complainant, Copy of the SIM replacement request form along with the documents of the subscriber submitted by imposter, Copy of the SIM replacement request in the prescribed form along with the requisite documents of the subscriber submitted by Original Subscriber, Copy of the Letter dated 14th September 2013 by the Complainant No. 2 to officer in charge, Vodafone, Copy of the submission by Respondent No. 3 dated 18th September to the Police Inspector, Cyber Cell, Nagpur, Notice under section 91 of The Code of Criminal Procedure 1973 (CrPC) from Cyber Crime Cell, Pune, and Copy of the submission by Respondent No. 3 dated 26th September 2013 to the Cyber Crime Cell, Pune.

4. The event chronology according to Vodafone is as follows:

I. Respondent No. 3 submits that a certain person holding himself out as Complainant No. 2 visited their Nagpur Franchisee office of Respondent No. 3 on 6th September 2013 and requested for replacement of SIM. Upon receipt of SIM replacement request in the prescribed form along with the requisite documents of subscriber, the request was duly processed and new SIM was issued to the person who visited the store and then same was activated on the same day. The Complainant has alleged in his Complaint that the person requesting the replacement of SIM on the aforementioned date is an imposter.

II. The Respondent No.3 submits that the Complainant No.2 visited the Vodafone Store at Wakedawadi, Shivaji Nagar, Pune 411003 which store is a company store of Respondent No. 3, on 10th September 2013 and requested for replacement of the SIM. Upon receipt of the SIM replacement request in the prescribed form along with the requisite documents of the subscriber, the request was duly processed and new SIM was provided to the person who visited the store. The SIM was activated at 16:43:46 IST on 10th September 2013. The Complainant has admitted in his Complaint that he requested for the replacement of the SIM on the aforementioned date.

III. A letter dated 14th September 2013 by the Complainant No. 2 was addressed to the Officer in charge of the Respondent was received by Respondent No. 3 alleging that the wrongful SIM hacking had led to illegal financial withdrawals using online banking and purchase facilities resulting in a huge loss from the bank account of Complainant No. 3 having the mobile number 8552902xxx of the Complainant No. 2 as the recorded contact number.

IV. On 18th September 2013, pursuant to internal investigation the Respondent No. 3 submitted to the Police Inspector, Cyber Cell Nagpur that on 6th September 2013, that a person had approached

their store in Nagpur and had sought replacement of SIM for the mobile number 8552902xxx claiming to be the lawful owner of the same and that it was later on understood (on the basis of complaint by genuine customer) that the person was an imposter. The Respondent No. 3 also requested the Police Inspector to take appropriate action against the imposter and showed the willingness to co-operate with the Inspector in relation to the same.

V. On 19th September 2013 the Respondent No. 3 received a request for furnishing information under Section 91 of the Code of Criminal Procedure 1973 (Notice to produce documents) from the Cyber Crime Cell, Pune with respect to the Complainant No. 2. Respondent No. 3 submitted the information on 26th September 2013 to the Cyber Crime Cell, Pune.

5. Vodafone has argued mainly that:

I. The Respondent No. 3 does not "possess, handle or deal" with "sensitive personal data or information".

II. It is the submission of Respondent No. 3 that to bring a case in respect of Section 43A, the Complainant must show that there is "sensitive personal data or information" being "possessed, handled or dealt" with by Respondent No. 3. The Respondent No. 3 categorically states that it does not possess handle or deal with any "sensitive personal data or information" and therefore Section 43A does not even apply to Respondent No. 3 and in light of the same, the instant complaint must be dismissed.

III. In Services dated 6th November 2011 granted by the Department of Telecom to Respondent No. 3, under the scope of the 'services' the Respondent No. 3 is entitled to provide "collection, carriage, transmission and delivery of voice and/or non-voice messages over the Licensee's network in the designated Service Area".

IV. The Respondent No. 3 does not have any access to the content of the messages (voice or text) being transmitted over its network and it neither stores or possesses nor handles or deals with the content of the messages (voice or text) being transmitted over its network. It is submitted that the provisions of Section 43A are only attracted in relation to a 'body corporate' 'possessing, dealing or handling' in 'sensitive personal data or information'.

V. The instant case does not involve any "sensitive personal data or information" of the Complainant No. 2 and therefore is not maintainable under Section 43A.

VI. It is further submitted that Respondent No. 3 has entered into a customer agreement form with the Complainant No. 2 in its individual capacity and not in his capacity as a representative of the Complainant No. 2 and Complainant No. 3. The Respondent No. 3 hence does not owe any duty or responsibility to Complainant No. 2 and Complainant No. 3. In the instant case it is the allegation of the Complainants that a wrongful loss has occurred to Complainant No. 2 and Complainant No. 3 on account of negligence on part of Respondent No. 3 in implementing and maintaining the "reasonable security practices and procedures" in respect of the computer resource in which the Respondent No. 3 possesses handles or deals with the 'sensitive personal data or information' of Complainant No. 2 and Complainant No. 3. It is submitted that Respondent No.3 has no obligation or duty whatsoever owed to the Complainant No. 2 and Complainant No. 3 and therefore the question of the Respondent No. 3 being negligent does not arise in the first place.

VII. The scope of "reasonable security practices and procedures" under Section 43A of the Information Technology Act, 2000 does not include subscriber verification.

VIII. It is submitted that the law specified in this regard is the Condition 46.1A of the License Agreement for provision of Unified Access Services dated 6th November 2011 granted by the Department of Telecom to

Respondent No. 3 as notified by the Department of Telecommunications vide its letter dated 31st May 2011 ("Network Security Conditions"). In light of the foregoing it is submitted that the reasonable security practices and procedures as contemplated by the IT Act, 2000 are in relation to the computer resource (which in the case of the Respondent No. 3 is its network) and do not include the subscriber verification process at the time of issuance or re-issuance of SIM cards.

IX. It is submitted that the Complainant No. 1 has himself averred in his pleadings that the only inconvenience caused to the Complainant No. 2 on account of deactivation of the telecom services to the SIM card inserted in the handheld device of the Complainant No. 2 was that he was unable to receive intimation at the time of alleged unauthorized transfer of funds from the bank accounts of Complainant No. 2 and Complainant No. 3. It is submitted that it is not the Complainants' case that such non intimation resulted in unauthorized access to the Complainant No. 3's bank account. Complainant No. 2 has failed to attribute any cause of action on part of Respondent No. 3 which directly attributes any alleged negligence in 'implementing and maintaining reasonable security practice' in respect of any 'sensitive personal data or information' of the Complainant No. 2, on part of Respondent No. 3 to the unauthorized access to the bank account of the Complainant No. 3 and the consequent transfers.

X. Assuming but not accepting, merely for the sake of argument, that (i) the verification of subscriber at the time of replacement of SIM is a 'reasonable security practice or procedure' and (ii) the Respondent No. 3 is actually proved to have been negligent in such verification, even then the Respondent No. 3 has failed to (a) identify the nature of the 'sensitive personal data or information' 'possessed, handled or dealt' by Respondent No. 3 which has resulted in the loss; and (b) attribute the alleged negligence on part of Respondent No. 3 to the 'wrongful loss' suffered by the Complainant No. 2. It is submitted that, if at all, Respondent No. 3 has been equally defrauded and the alleged imposter has cheated the Respondent No. 3 in the same manner as he has defrauded and cheated the Complainant.

XI. Assuming but not accepting that Respondent No. 3 inadvertently issued a replacement SIM to an alleged imposter, such replacement does not in any manner amount to an assistance which requires an overt intentional act on part of any person alleged to be assisting. Further it is not correct to state that mere access to the SIM card (which continues to be a property of Respondent No. 3) facilitates an access to a computer, computer system, computer network or computer resource which is owned by the Complainant No. 2 or which the Complainant No. 2 is in-charge of. In light of the same the Complainant has failed to prove any contravention of Section 43 (g) on part of the Respondent No. 3.

6. The police has made detailed investigations into the case and submitted the following report:

I. Complainants hold a Current account with ICICCI Bank, Aundh Branch in the name of their firm Sango Consultants Pvt. Ltd.

II. The account has Internet banking facility. Between the dates 6th to 9th September 2013, some unknown person has illegally transferred Rupees 19,01,073.16 from Complainants bank account. FIR has been registered at Chaturshringi Police Station bearing CR No: 315/2013 under section 419, 420, 467, 468, 471 of Indian Penal Code and under section 66, 66C, 66D of Information Technology Act.

III. Police Investigation:

a. Police has arrested Vinayak Mahadev Tirlotkar on 6th October 2013 and he was in police custody from 7th to 17th October 2013. The amount from complainant's account was transferred to 11 accounts of ICICI Bank, and some other accounts. Police has received accounts documents along with KYC documents from ICICI Bank for only 8 accounts.

b. Police has already requested to the concerned Mobile Company for getting the details of Mobile numbers registered with the said 11 ICICI

Bank accounts.

c. Police has not received information about the SBI Bank account which is in the name of Mr. Lalit Mahata.

d. Rupees 52,130 and Rupees 47,985 were transferred illegally to Account no. 41501513078 with ICICI Bank which was hold by one Vinayak Mahadev Tirlotkar. He has withdrawn total Rupees 1,00,115 from this account by using ATM card.

e. During the course of investigation Police found out that, between 6th to 9th September 2013, 10 transactions were made from Complainants account to "itzcashcard" using internet via IP address 67.208.112.94, and this IP address belongs to ISP Crucial Paradigm, Turkey. Police had requested the information about the concerned IP address from the above mentioned ISP and received reply on 18th October 2013 from ross@crusialp.com. The email reads as under:

"To whom this concerns, after some basic investigation the IP Address you have listed is associated with a product known as a Virtual Private Server or VPS. Basically it is a VM or Virtual Machine that is used by a customer. The product information is available on our website. The customer has full root access to the VM and may use it as they see fit, within the conditions of our terms of service (http://www.crucialp.com/site/aup/php). We suspect though unconfirmed that this virtual service is being used as a proxy or VPN based services".

The Customer's details are as follows:

First Name: Ali
Last Name: Ghasemi
Company Name:
Email Address: mehrabani.raoof@gmail.com
Address 1: hurriyet.mah.12.sok no:1
Address 2:
City: Tehran
State/Region: Tehran
Postcode: 93138
Country: TR-Turkey

Phone Number: 5513344057

The IP details from when they last logged into our billing system is as follows:

IP Address: 46.183.217.149

Host: ip-217-149-dataclub.biz

IV. Lacunas from ICICI Bank's side, as per Police:

a. On 6th September 2013 and 7th September 2013, within a short span of time, there were 22 illegal transactions and amount Rupees 19,01,073 got transferred from Complainants' account. Considering the history and pattern of transaction done by Sh. Dhande (Complainant) in past, ICICI Bank could have identified such suspicious activity.

b. The transactions were done from IP's which belonged to foreign countries. Bank should have verified the same, whether the complainant has done those transactions.

c. ICICI Bank has not given the CCTV footage of ATM & in person Cheque / Cash withdrawal at Branch.

d. Bank has not verified whether the transaction OTP was sent to the genuine customer.

e. It is observed that Bank has not followed the RBI Guidelines many times. They have not complied with KYC norms and AML related guidelines.

f. Police have recorded the statement of the Bank Manager and sales team in charge Ms. Asmita Pangarkar. Police have also visited the address of the Accused Vinayak Tilotkar, which was provided during KYC. It was observed that the address given by the Accused is bogus.

g. Police have sought the information regarding the bank accounts opened by Ms. Asmita Pangarkar during last 1 year and whether those accounts have been used in any criminal activity, but the bank has not provided

the information till date.

h. According to the Police, a fake bank account was opened at Bangalore ICICI Bank in the name of Ashish Aggarwal and without authorization Rupees 1 Lakh was transferred from Complainants account to this fake account. The concerned person who had opened the fake account was caught in Mumbai and the name of that person is Pankaj Jain and not Ashish Aggarwal. ICICI bank has failed to observe proper due diligence and KYC norms while opening the account.

i. According to the Police, an account was opened at Kandivali, Mumbai in the name Ravi Kumar Singh, but no one is residing on the address provided by the same person while opening the account. Police requested the Bank on numerous occasions to show them the address of the concerned person but there was no response from the bank. ICICI Bank and its officials are not assisting the Police in the investigation.

V. Lacunas from Vodafone's side, as per Police:

a. Accused successfully deactivated the Mobile No. 85529XXXXX, by contacting Vodafone on 6th September 2013 and collected a replaced/duplicate SIM from the concerned Vodafone store. This mobile was linked to complainant's account.

b. There is no date written on the SIM replacement form.

c. Replaced SIM was given to a third person even after finding out that the person is not the SIM owner (Smt. Megha Dhande).

d. Vodafone did not follow Basic Due diligence on numerous occasions while issuing replaced SIM card (Calling on alternate number 98224XXXXX, given on the SIM replacement form for verification, passport copy given for the SIM replacement is of a male person while the SIM is registered on a female customer, address on the passport and address on the original SIM registration form is different, no receipt available collected towards etc).

e. Xerox copy of the Passport bearing Passport No. 406XXXX was given for SIM replacement; there is a doubt that the same Passport copy has been submitted before at various other telecom service provider outlets for committing various crimes.

f. At the time of SIM replacement Vodafone failed to carry out mandatory verification through File Net System because the system was down at the time.

g. The photo given for the SIM replacement form is a scanned color photo on a normal paper, which might be a fake photo.

h. Vodafone has not submitted the original documents submitted along with SIM replacement form. Vodafone has provided only photocopy by email.

i. As per information provided by store executive of Khamla, Nagpur there is only scanned copy of photo instead of original photo. Also this photo belongs to Ex-Union Minister Sh. Dayanidhi Maran.

j. Vodafone ignored the email sent by the Police regarding non-functional CCTV cameras and took no efforts to change the same. CCTV footage obtained by the Police is of the CCTV camera outside the building and for the date 5th September 2013, which is irrelevant as the SIM replacement was done on 6th September 2013.

7. My analysis of the documents before me, and the arguments made by various parties before me, is as follows:

I. Both ICICI and Vodafone, two big names in Banking and Telecom sector respectively, have badly let their customers down, and are totally non-repentant about their laxity, bordering on connivance, which has resulted in this crime.

II. Before passing any order in this case, I think it is important to realize that Net banking and mobile banking are increasingly being promoted

by the Banks, and used by their customers, to do financial transactions. While the customers are expected to use their discretion to secure their net banking /mobile banking IDs and passwords, the onus of securing customer's data is on the banks. Similar is the case with telecommunication companies that bask in huge revenues due to use of mobile services by their customers.

III. The Government has realized the critical importance of security of the data reposed with banks and telecommunication companies and has enacted laws and issued various guidelines to ensure basic minimum security of consumers' data and money. Section 43 and 43A of the Information Technology Act, 2000 (IT Act) are steps in the same direction. Likewise, the KYC norms issued by the RBI and the guidelines for issuance of SIM cards issued by TRAI/DOT are also measures that go a long way in protecting the interest of the innocent citizens.

IV. First, let me deal with the laxity shown by ICICI Bank, which has resulted in this crime.

a. ICICI has been treating KYC norms with total impunity. Account of Vinayak Tilotakar turned out bogus. Address of Ravi Kumar Singh was bogus. One Pankaj Jain opened account in false name Ashish Aggarwal in Bangalore. And so on. Police says that their bank manager Ms. Asmita Pangarkar may have been lax in opening many other bogus accounts. Still, the bank is neither cooperating with the police, nor doing any internal investigation.

b. ICICI Bank has not given to the police the CCTV footage of ATM & in person Cheque / Cash withdrawal at Branch.

c. The use of foreign IP addresses and fast withdrawals, totally at variance with the normal transaction activities of the complainants, also did not raise any alerts within the bank's system. This shows that real-time fraud analytics are not in place.

d. Despite this being a case of huge financial loss to the customer, the bank has done no meaningful internal investigations. Their Fraud Investigation Unit (FIU), mandated by RBI guidelines, seems non-existent.

e. I have carefully gone through the *"Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/ Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002"* dated 2nd July 2012, and find that ICICI Bank has violated para 2.8 of the circular regarding Money Mule Accounts by not taking sufficient precautions in this regard.

f. I have also carefully gone through the *"Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds"* issued by RBI on 29/04/2011. It has detailed instructions to Banks on Fraud Risk Management; need of strong KYC norms to prevent cybercrimes; Transaction monitoring; Dedicated email ID and phone number for reporting suspected frauds; Mystery shopping and reviews; reporting of frauds as indicated in the RBI circular, dated July 1, 2010; Filing of police complaints (Banks should readily share data and documents requested by the police even in cases where the bank in question is not the victim of the fraud but has been a receiver of fraudulent monies into its accounts); customer awareness etc. It is very clear that ICICI falls short on many of these counts, which has contributed to its customer getting cheated of his hard earned money. Chaprt 6 on Cyber Frauds in the RBI notification dated 29/04/2011 clearly mentions that *"… the response of most of the banks to frauds in these areas needs further improvement, thereby avoiding putting the entire onus on the customer …".*

g. I have also gone through the Internet websites indicating protection offered by various banks abroad to their customers who use electronic channels to conduct transactions. Most of the banks in USA and in other developed nations INSURE their customers against online/ATM frauds

etc., beyond a liability of 50 dollars. Section 909 of the "Electronic Fund Transfer Act" of USA dealing with Consumer Liability is really loaded in favour of the consumer. It is expected that in India also, the banks will not only educate the customers about precautions to be taken while using Net Banking, or credit/debit/ATM cards, but will also insure the customers against possible frauds. It is quite sad to see the Global Banks operating in India proclaiming very loudly that they are following best international practices, but not giving its Indian customers same level of protection what they offer abroad.

h. Criminals mainly used accounts of ICICI opened on fake papers to defraud the complainant. It is my view that if the KYC norms were strictly followed by the Bank or if the CCTVs had been working, it could have helped the enforcement agencies to trace the fraudsters and the Complainant's money could have been recovered.

i. I also have on record an emotional letter written by complainant Sh. Sanjay Dhande to MD & CEO of ICICI Bank Smt. Chanda Kochar. He says that he has served as Director IIT, Kanpur for 11 years, has received Padmashree Award for his services to the Nation, and is presently a member of National Security Advisory Board. That Smt. Kochar or her office has not even bothered to reply to this letter shows how shabbily they treat their customers, and how their grievance redressal mechanism has totally broken down.

V. ***Now, let me deal with the issue of laxity, almost bordering on connivance, on part of Vodafone, which has resulted in this crime.***

a. There is an undeniable direct nexus between blocking of SIM card of the Complainant, issuance and use of the duplicate SIM card by the fraudster and unauthorized financial transactions from the account of the Complainant. In fact, the Bank transactions happened after the duplicate SIM card was procured and activated by the fraudster.

b. As I understand, it is common practice to register one's mobile number with banks. Banks use this number for any communication regarding the associated bank account with the customer. The mobile number is used by the banks to identify their customer. It could also be used, along with certain other details, in case one wanted to change ones password or create a One Time Password (OTP) for doing a transaction. In this particular case*, ICICI documents show that not only bank transaction alerts, but even OTP was sent to the duplicate SIM card.*

c. It is not farfetched to state that the duplicate SIM card was used by the fraudster to access the password/id of the Complainant. According to me, access by the fraudster to the Complainant's SIM card has played a major role in accomplishing the unauthorized financial transaction. Further, blocking of the SIM card of the Complainant by Vodafone also disabled the Complainant from getting alerts from his ICICI Bank account.

d. Based on the facts and documents placed before me, it is clear that Vodafone did not check the authenticity of the claim or reason for issuance of a duplicate SIM card. They did not check the picture on the fake license with their database; nor was the sign matched; the online File Net system was down for days. The person took the blank form, and came back in ten minutes, with forged details, a photo of male person on scanned normal paper rather than a proper photo; there is no payment receipt for duplicate card fees; the store manager was not in shop but came next day and backdated his signature on the form – the list of omissions is endless. , They didn't even bother to check if the number was in use and active or not. A mere phone call on the Complainant's mobile number, which is the minimum due diligence one would expect, could have averted the difficulties and agony suffered by the Complainant.

e. Clearly, Vodafone has been negligent in giving duplicate SIM to fake person by not following the procedure laid down by the Government and its own company policy document submitted to me.

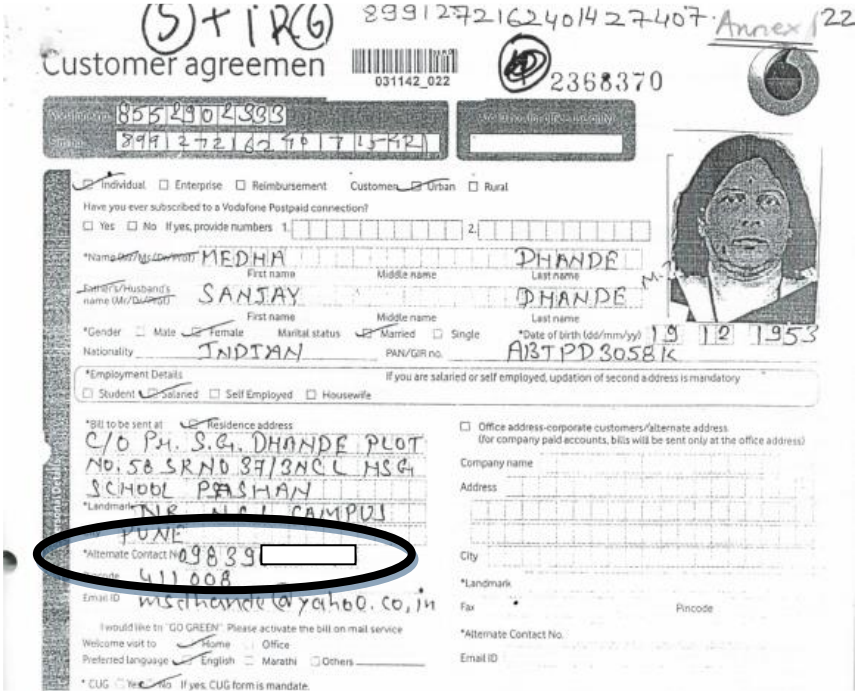
f. The apathy of the telecom companies towards observance of norms/regulations/guidelines related to proper and effective subscriber verification has been brought to the fore in the Hon' Supreme Court in Avishek Goenka Vs. Union of India & Anr. case the decision of which was delivered on April 27, 2012. The Supreme Court in that case took note of the fact the SIM cards are provided without any proper verification, which causes serious security threat as well as encourages malpractices in the telecom sector. It appears that the concerns raised in that case have not been given any heed to by Vodafone.

g. When a citizen applies for obtaining a SIM card, he provides a battery of information which is personal and sensitive in nature. He reposes his faith and trust in the company that his details and data would not be shared with third parties. It is not hard to realize that such information, if falling in wrong hands, can be misused. A SIM card is a veritable key to person's sensitive financial and personal information. Realizing this, there are clear guidelines issued by the DOT regarding the issuance of SIM cards. The IT Act also intends to ensure that electronic personal and sensitive data is kept secured and reasonable measures are used to maintain its confidentiality and integrity. It is extremely crucial that Telecom companies actively follow strict security procedures while issuing SIM cards, especially in wake of the fact that mobiles are being increasingly used to undertake financial transactions. In many a case brought before me, financial frauds have been committed by fraudsters using the registered mobile numbers of the banks' account holders.

h. By not implementing security procedures, Vodafone is jeopardizing the sensitive and personal data of all its customers and in a way abetting in commission of frauds related financial transaction.

i. This is starkly brought out by the following papers from Police investigation:

Original Agreement Form submitted by Smt. Medha Dhande



(5)+IR(6) 8991272162401427407 Annex 122

Customer agreemen 031142_022 2368370

8552902383

8991272162401427407

Individual ☐ Enterprise ☐ Reimbursement Customer ☑ Urban ☐ Rural

Have you ever subscribed to a Vodafone Postpaid connection?

☐ Yes ☐ No If yes, provide numbers 1. 2.

*Name MEDHA (First name) (Middle name) DHANDE (Last name)

Father's/Husband's name (Mr/Dr/Prof) SANJAY (First name) (Middle name) DHANDE (Last name)

*Gender ☐ Male ☑ Female Marital status ☑ Married ☐ Single *Date of birth (dd/mm/yy) 19 12 1953

Nationality INDIAN PAN/GIR no. ABTPD3058K

*Employment Details If you are salaried or self employed, updation of second address is mandatory

☐ Student ☑ Salaried ☐ Self Employed ☐ Housewife

*Bill to be sent at ☑ Residence address

C/O PH. S.G. DHANDE PLOT NO. 58 SR NO 87/3 NCL HSG SCHOOL PASHAN

*Landmark NCL CAMPUS

PUNE

*Alternate Contact No 09839

411008

Email ID msdhande@yahoo.co.in

I would like to 'GO GREEN' Please activate the bill on mail service

Welcome visit to ☑ Home ☐ Office

Preferred language ☑ English ☐ Marathi ☐ Others

* CUG ☐ Yes ☑ No If yes, CUG form is mandate.

☐ Office address-corporate customers/alternate address (for company paid accounts, bills will be sent only at the office address)

Company name

Address

City

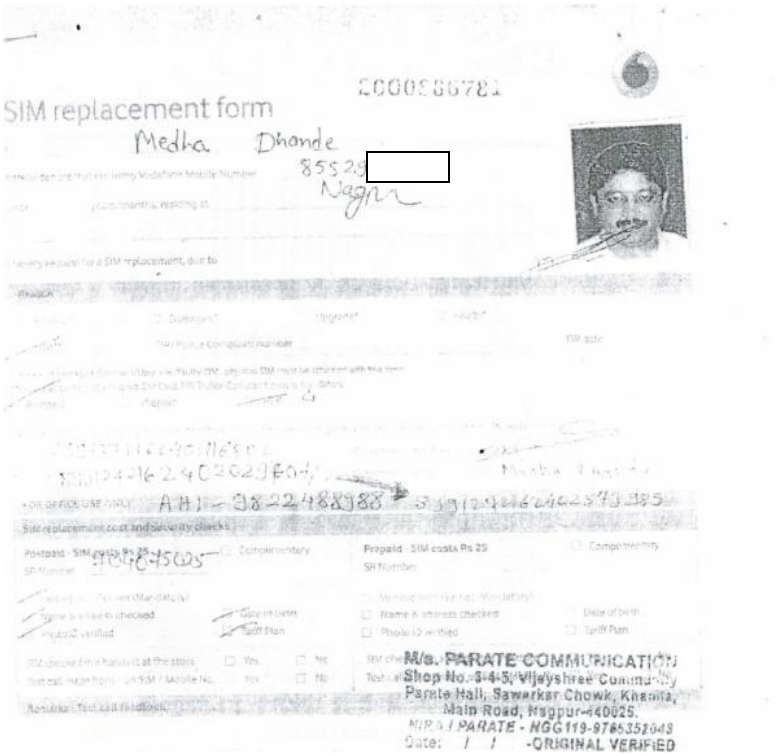
*Landmark

Fax Pincode

*Alternate Contact No.

Email ID

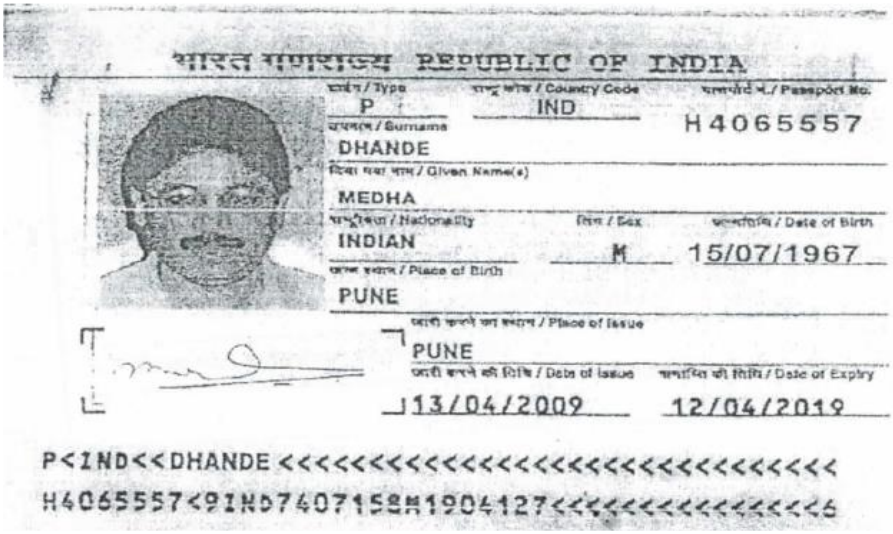
Duplicate SIM Replacement form & forged passport documents submitted by the Fraudster:


SIM replacement form

Medha Dhande

Nagpur

M/s. PARATE COMMUNICATION
Shop No. 3-4-5, Vijayshree Community
Parate Hall, Sawarkar Chowk, Khamla,
Main Road, Nagpur-440025.
MIRA / PARATE - NGG119-9765352643
Date: / / -ORIGINAL VERIFIED


भारत गणराज्य REPUBLIC OF INDIA

P

IND

H4065557

DHANDE

MEDHA

INDIAN

M

15/07/1967

PUNE

PUNE

13/04/2009

12/04/2019

P<IND<<DHANDE<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

H4065557<9IND7407158M1904127<<<<<<<<<<<<<<<6

j. In arguments before me, Vodafone has further tied itself in knots. They claim that they are not dealing with, handling or storing the Contents of

Voice or Text messages, and hence they are not dealing with Personal Sensitive data. Then they contradict themselves by stating that:
In Services dated 6th November 2011 granted by the Department of Telecom to Respondent No. 3, under the scope of the 'services' the Respondent No. 3 is entitled to provide "collection, carriage, transmission and delivery of voice and/or non-voice messages over the Licensee's network in the designated Service Area".

k. They also state that they do not have any access to the content of the messages (voice or text) being transmitted over its network and it neither stores or possesses nor handles or deals with the content of the messages (voice or text) being transmitted over its network. This is amusing, given that they store SMSes and MMSes, albeit in transit, and provide interception facilities to Police and others. In fact, even the Metadata, i.e. caller and called number logs, locations, duration and time of call etc. are highly sensitive personal data. Who called suicide helpline, or AIDS helpline, who is calling whom frequently at night, which two phones were in close vicinity for how long, all this is undoubtedly highly sensitive, personal data. The content of voice call or SMS or MMS is obviously still more sensitive. Hence, a Telecommunication company saying that they do not "handle" sensitive, personal data, is an argument which has no merit at all.

l. They also state that this is a "high profile case" and they have suspended two employees of the franchise. They also admit that clearly a duplicate SIM card was issued by their Nagpur franchise to an imposter, and their own rules and procedures were violated by the franchisee.

8. In light of the foregoing discussions, in my considered view:

(a) During Police investigations or ICICI Bank's internal investigations, if any, it is not the case that the complainant deliberately or negligent divulged all his details to the criminals. Hence the liability of the loss cannot be passed on to him. Also, the complaint is not a novice in electronic transactions. In fact, the complainant **Sh. Sanjay Dhande has served as Director, Indian**

Institute of Technology for 11 years, has been awarded Padmashree for his services to the Nation, and is presently a Member of the National Security Advisory Board.

(b) As Rupees 3.26 lakhs have been reversed out of initial fraud of Rupees 19 lakhs, I assess total fair compensation to complainants at about Rupees 18 lakhs, to cover their loss and legal fees etc. Vodafone must share bigger blame because duplicate SIM card played most critical role in this crime.

(c) ICICI Bank has defaulted on multiple counts as enumerated earlier in my Analysis of this case. Their omissions fall within the ambit of Section 43A of the IT Act. Accordingly, I order Respondent 1, i.e. ICICI Bank to pay damages to the tune of **Rupees 6,00,000** by way of compensation to the Complainant, within a month of this order, failing which compound interest of 12 percent compounded monthly will also be chargeable.

(d) Vodafone i.e. Respondent 3, by not following the reasonable security practices and procedure and the established guidelines before issuing a duplicate SIM card, has led to the access of sensitive personal data and information of the Complainant to an unauthorized person and thereby caused wrongful loss to the Complainant. According to me, this falls within the ambit of Section 43A of the IT Act. Accordingly, I order Respondent 3, i.e. Vodafone to pay damages to the tune of **Rupees 12,00,000** by way of compensation to the Complainant, within a month of this order, failing which compound interest of 12 percent compounded monthly will also be chargeable.

(e) I must also make a few suggestions to Department of Electronics and Information Technology (DeiTY), Govt. of India regarding the Cyber Crimes. The IT Act was passed in 2000. The Police, lawyers, Adjudicating officers, etc. are still not very familiar with nuances of cyber crimes. Workshops of various stakeholders, including Adjudicating Officers should be held, to sensitise and train them. The post of Chairman, Cyber Appellate Tribunal is vacant for more than three years. Perhaps the focus needs to shift from

policing the cyber citizens to policing the cyber criminals? Perhaps a telephonic Helpline to help the victims of cybercrimes may be useful. Hence, a copy of this order be also sent to Secretary, DeiTY, Govt. of India, for debate within his Ministry on these issues.

(f) The Department of Telecommunications, Govt. of India, also needs a hard look at the lack of Regulatory compliances by the telecom companies. The omissions on part of Vodafone go beyond simple laxity, and almost border on connivance with the cyber criminals. Hence copies of this order should also be sent to Secretary, DoT, Govt. Of India and Chairman TRAI.

(g) Both the departments, DeiTY and DoT, should note that forged papers with photograph of ex-Union Minister of both these departments, Sh. Dayanidhi Maran have been used to commit this crime.

(h) The role of ICICI in this crime is clearly established. What is sad is the lack of response by their MD to victims of cybercrimes, indicating total apathy and breakdown of grievance redressal mechanisms. I wonder what use are various Guidelines issued from time to time by RBI, on KYC, Money Laundering, Mule accounts, Fraud Investigation Units, use of real time Analytics etc., if banks are flouting them with impunity, and there is no supervisory mechanism or Third Party Audit mechanism by RBI. A copy of this order be sent to Secretary Banking, Govt. of India, for further necessary action in this regard.

Signature Not Verified

Digitally signed by Aggarwal Rajesh Madanlal
Date: 2014.01.16 17:04:31 IST
Reason:

Rajesh Aggarwal
Pr. Secretary (Information Technology)
Government of Maharashtra,
Mantralaya, Mumbai- 32