BEFORE THE ADJUDICATING OFFICER

SH. VIJAY KUMAR GAUTAM

PRINCIPAL SECRETARY, INFORMATION TECHNOLOGY,

GOVERNMENT OF MAHARASHTRA

Complaint No. 40 of 2015 dated 13th July, 2015

IN THE MATTER OF

Mr. Nirmalkumar Shankarrao Athawale .....Complainant

Versus

1. My Idea Authorized Franchisee Idea Cellular
2. Idea Cellular .....Respondents

Advocates:

1. For Complainant - Adv. Mahendra Bhaskar Limaye , Adv. Rajesh Tekale
2. For Respondent 1 & 2 - Adv. Bharucha & Partners
3. For Respondent 2 - Adv. Jehangir Jejeebhoy, Adv. Tushar Mittal, Adv. A. Kumar

JUDGEMENT

1. Brief Facts of the Case:

1.1 This proceeding emanates from the complaint filed by the complainant under Section 43 (a), (f), (g), (h) and 43 A for adjudication under Section 46 of the Information Technology Act, 2000. Following the basic principles of natural justice, reasonable and equitable opportunity of being heard was provided to both parties 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.

1.2 From the complaint and documents enclosed with the complaint, written statement submitted by the Respondent, the admitted facts are that –

(a) The Complainant owns Close User Group for his organization since last ten years with account no. 100016443348 and has 9 CUG Connections.

(b) The complainant is using mobile number 9373120789 and rests of the numbers are provided to other employees / Persons for organizational activity.

(c) The complainant's mobile services were stopped by the respondents on 01.06.2015 on an application, with supporting documents, received by the respondents.

(d) On scrutiny of the application and documents leading to closure of the services to the original SIM by the service provider, it was found that the said application and the documents were forged and that the respondents, without asking for the production of the damaged SIM card, suspended the services of the original SIM card relying only on documents submitted to them.

(e) No CCTV footage of the Centre of the service provider respondent could be made available for the twin reasons of no regular electricity supply and no battery backup available.

(f) The complainant has submitted written complaint to police station Wadi as well as to respondent no 2 on 02.06.2015 and has filed FIR to Police Station Wadi on 03.07.2015.

1.3 Relying on the contents of the complaint, copies of the documents submitted by the fraudster on 01.06.2015 to the respondent (request letter on letter head of M/S Preetee Builders, PAN card, request form), copies of the documents submitted by the complainant (request letter on letter head of M/S Preetee Builders, PAN card, request form), copies of complaint to Police Inspector, Police Station Wadi on 02.06.2015, communication dated

12.06.2015 by respondent No.1 regarding unavailability of video footage for date 01.06.2015 and First Information Report to Police Station Wadi on 03.07.2015, the contention of the complainant are:

(a) That the service provider (respondents) have failed in maintaining reasonable security practices by not properly verifying the documents submitted by the fraudster for issuance of the duplicate SIM card and making it, further, convenient for the fraudster by not asking for the production of the damaged SIM card which was put as reasons for the issuance of the duplicate SIM card by the said fraudster.

(b) That the complainant apprehends some foul play on part of the service provider as it has failed to even produce CCTV footage on grounds of neither availability of regular power supply nor any power back up.

(c) That the respondents have acted to correct the mistake because of the swift action taken by the alert complainant.

(d) That this gross negligence on the part of the respondents has facilitated unauthorized access of information and service to fraudster who intended to block the SIM card preventing the complainant from closing some financial deals on that date.

(e) That in view of above, the respondents have definitely been guilty of contravention of Section 43 (a), (f), (g), (h) and 43A leading to potential financial loss and mental harassment to the complainant and, therefore, the token claim of damages of Rs. 15,000/- (Rs. Fifteen Thousand Only) by way of compensation be awarded in his favour.

1.4 In the reply submitted through written statement and during the oral argument before me, the respondent contends that –

(a) There is no financial loss to the complainant and the proceedings are not covered under Section 43A of the Information Technology Act, 2003.

(b) The TRAI Guidelines provide immediate provisioning of the duplicate SIM to the customer. On verification and having come to know that the SIM is issued to the fraudster on behalf of the customer, the services were immediately stopped and no financial losses have been suffered nor there is any misuse of the New SIM as such the complaint is not tenable.

(c) This Hon'ble Forum does not have jurisdiction to try, entertain and dispose of the present complaint and only a criminal court of competent jurisdiction can entertain such a complaint.

(d) The Respondent merely acts as an 'intermediary' as defined under Section 2 (w) of the Act, and is, in any event, exempt from liability under section 79 of the Act.

(e) In the event that there has been any denial of service, the provisions of Consumer Protection Act would apply. It is a settled position in law that telecom services are 'services' for the purpose of Consumer Protection Act , 1986 and do not fall within the scope or ambit of the Act for the purposes of the present complaint.

(f) The Respondent has implemented all security practices /layers mandated by the DOT and TRAI Guidelines.

(g) The Complaint on his own admission appears to have doled confidential information to his employees thereafter attempted to cover up its tracks of having freely doled out personal and confidential information which fraudulently misused by the fraudsters in the company of the Complainant.

(h) While issuing a new SIM card as a precautionary measure an e mail was also sent to the registered e mail id of the subscriber.

(i) The limited allegation that relates to this Respondent is that a duplicate SIM card was obtained in an allegedly illegal manner and on that basis some liability is sought to be foisted on this Respondent otherwise the entire lapse is directly attributable to the complainant who appears to have been negligent and careless in his action.

(j) The Hon'ble Authority has to consider the provisions of section 47 while adjudicating the dispute and none of the parameters in the complaint fall for adjudication as per section 47 of the Act.

(k) In view of above, the complaint may be rejected with compensatory cost.

1.5 On the closure of the arguments by both the parties and after waiting for considerable time to get the report of investigation by the Police, it has been decided that the matter be decided on the merit of the arguments put forth by both the parties for the sake of justice within the limited framework of the IT Act 2000.

1.6 On consideration of the detailed arguments, oral as well as written, put forward by both the parties, and in view of the provisions of the IT Act 2000, the key issues and findings are recorded as follows:-

Issue No. 1: Whether the respondents, who own, control and operate the customers' sensitive personal data and information, have been negligent in implementing and maintaining reasonable security practices and procedures and, thereby, creating a conducive environment for the fraudster with malafide intention to cause wrongful loss to the complainant?

Findings: YES. It is a fact that the service provider controls and operates SIM card carrying the customers' personal data and information which, in mobile technology driven world, facilitates personal, business and financial transaction processes. The customers are using mobile phones to facilitate their business and share sensitive business data and information related to their business activities. In fact, the entire business of the mobile operators critically depends on the use of vast amount of data, both personal and business related, transacted over mobile platforms and constitutes the core of the profits of these operators. Therefore, these service providers need to adopt and adhere strictly to operating procedures related to issuance of SIM

cards which must inter alia include Identity and/or Address verification protocols. It is unfortunate to note that the respondents have failed to establish and maintain basic security measures and practices in this regard by –

(i) Relying on copies of the allegedly forged PAN Card and the letter head of the complainant's business entity and not verifying the same with the original;

(ii) By not even perusing the documents submitted leading to gross omission of failing to notice that the names of the complainant and his father appearing on the forged PAN card have the same middle name 'Shankarrao' and, therefore, created reasonable doubts about the document. The respondents, situated in Maharashtra and dealing primarily with names on daily basis, cannot plead ignorance on this count.

(iii) By not demanding the damaged SIM card;

(iv) By not resorting to calling on the numbers provided on the letter head of the business organization of the complainant for any confirmation;

(v) By not putting in place any online mechanism to facilitate confirmation of certain basic details by the centres spread across the geography of the country.

It is publicly known that service providers such as respondents, through their authorized centres, are not adhering to any security measures leading to a very porous system of obtaining duplicate SIM cards putting the interests of customers with limited resources completely vulnerable to the malicious designs of the fraudsters. Security measures including cyber security measures and consequent standard operating procedures and effective change management strategies are integral part of the business process adopted by these service providers. It is the responsibility of the respondents, who are admittedly big and aspire to be bigger by being competitive,

commercially profitable and customer friendly, to also ensure that a pro-active and predictive security framework is established with contemporary technological measures, consequent standard operating procedures and requisite change management strategy across the organization. A gross failure by the respondents in establishing and implementing reasonable security practice has occurred in this case. In view of the absence of ordinary prudence while verifying the critical documents produced at the time getting the duplicate SIM card issued, the argument of adherence to complex, multilayered guidelines of DOT and TRAI fails to hold the ground. As the internet evolves, quantum processing takes the computing to unimaginable level, Web 3.0 unfolds and Fintech innovations powered by Blockchain, IOT, AI, Machine Learning and Data Analytics bring disruptions the way we engage ourselves personally as well as in business, cybersecurity measures will be under ever growing stress. Mobile telephony being the key gateway in the growth process, the service providers need to appreciate the criticality of establishing and maintaining adequate security measures and practices rather than hiding behind the limitations of the acts/rules and guidelines of regulators.

Issue No. 2: **Whether the contention of the respondent regarding the non-jurisdiction of Adjudicating Officer or exemption of the respondents under Section 79 of the IT Act in the case tenable?**

Findings: NO. The facts of the case clearly establish that the powers conferred on the Adjudicating Officer under the IT Act are limited to ascertaining the acts of omission and commission and consequent wrongful loss/gain to affected/involved persons and, nowhere, it crosses the path of competent criminal or consumer courts as defined in the respective acts. Further, the respondent has erred in entering into the shoes of 'intermediary' as defined in the Section 2(w) of the IT Act. In this present case, the service provider respondents are not 'receiving or storing or transmitting the

record on behalf of another person' but the customer is providing information directly to the respondents for getting the SIM card issued by the respondents. Therefore, the respondents are not 'passive' receivers or storekeepers or transmitters of data and information but 'actors' in the process. In view of above, the respondents are not acting as intermediaries for any other person but are end-consumers of data and information furnished by customers to them. Since the respondents are key providers of mobile technology for voice and data transmission, they become key stakeholders within the IT Eco-System and, therefore, liable under the relevant provisions of the IT Act.

Issue No. 3: Whether wrongful loss has been caused to the complainant on account of the action of the respondents?

Findings: YES. Section 23 of the Indian Penal Code defines "Wrongful loss" as the loss by unlawful means of property to which the person losing it is legally entitled. There is no doubt that the complainant lost the SIM to which he was legally entitled even if it was for a temporary period or even if it might not have caused big or irreversible financial loss to him. In addition, he has definitely suffered mental agony and financial loss in the process leading to complaint and litigation.

1.7 Conclusion: In view of the findings on all the relevant issues as above, I have come to the conclusion that there is enough evidence on record to establish that the respondents have, definitely, been non-serious and negligent in implementing and maintaining reasonable security practices and procedures regarding scrutiny of documents, confirmation of facts, ensuring availability of CCTV recording etc. and, thereby, creating a conducive environment for the fraudster to get unauthorized access to the SIM carrying data/information and related personal and business entitlements of the complainant with malafide intention to cause wrongful loss to the complainant

and, consequently, wrongful gain to itself. It is also evident that irreversible consequences could be avoided by the alert complainant himself. Consequently, I have come to the conclusion that respondents are liable for violation of Section 43A of the IT Act 2000. I have also considered the provisions of Section 47 of the IT Act referred to by the respondents while decided to pass this order.

ORDER

In the light of above, under the powers conferred on me under Section 46 of the Information Technology Act, 2000, I pass the order that the respondents shall pay by way of compensation to the complainant a token amount Rs. 10,000/- (Rupees Ten Thousand Only) to cover the wrongful loss caused, legal costs and for the mental agony suffered by him within a month of this order, failing which a compound interest of 12% compounded monthly will be chargeable.

Order passed on this day of 9th November, 2017 at Mumbai.

(Vijay Kumar Gautam)
Principal Secretary, Information Technology,
Government of Maharashtra,
Mantralaya, Mumbai-32