TELECOM DISPUTES SETTLEMENT & APPELLATE TRIBUNAL
NEW DELHI

Dated 20th December,2019

Cyber Appeal No.3 of 2018

Bank of India ... Appellant
Versus
Shri Sandeep & Anr. ... Respondents

Cyber Appeal No.5 of 2018

Vodafone Idea Ltd. ... Appellant
Versus
Shri Sandeep Singhal & Anr. ... Respondents

BEFORE:

HON'BLE MR. JUSTICE SHIVA KIRTI SINGH, CHAIRPERSON

Cyber Appeal No. 3 of 2018

For Appellant	:	Mr.Umesh Deshpande,Advocate
For Respondent no. 1	:	Mr.Tejveer Singh Bhatia,Advocate Mr.Rohan Swarup,Advocate Mr.Kunal Vats,Advocate Ms.Vishaka Ahuja,Advocate Mr.Kartikey Pant,Advocate
For Respondent No. 2	:	Mr.Balbir Singh, Sr. Advocate Mr.Devesh Kumar Chaudhry,Advocate Mr.S.N.Thyagarajan, Advocate Ms.Akanksha Banerjee,Advocate Mr.Shyam Gopal,Advocate

Cyber Appeal No. 5 of 2018

For Appellant	:	Mr.Balbir Singh, Sr. Advocate Mr.Devesh Kumar Chaudhry,Advocate Mr.S.N.Thyagarajan, Advocate Ms.Akanksha Banerjee,Advocate Mr.Shyam Gopal,Advocate
For Respondent No. 1	:	Mr.Tejveer Singh Bhatia,Advocate Mr.Rohan Swarup,Advocate Mr.Kunal Vats,Advocate Ms.Vishaka Ahuja,Advocate Mr.Kartikey Pant,Advocate
For Respondent No. 2	:	Mr.Umesh Deshpande,Advocate

JUDGEMENT (ORAL)

At the outset, it is recorded that learned counsel for Vodafone Mobile Services Ltd., Appellant in Cyber Appeal No.5 of 2018 and Respondent No.2 in the other Appeal, has informed that the name of the above corporate entity now stands changed to Vodafone Idea Limited. He prays that this change may be recorded and the changed name should appear in the judgement. This prayer has not been opposed by the learned counsel for the other side and hence the change in the name of Vodafone Mobile Service Limited to that of Vodafone Idea Limited is recorded and the cause title of this judgement and order is accordingly modified so as to reflect the name of

Vodafone Idea Ltd. As prayed, learned counsel is permitted to file amended memo of parties.

2. For sake of convenience, the facts shall be referred from the records of Cyber Appeal No.5 of 2018, unless specifically stated otherwise.

3. Both the Appeals arise out of and are directed against the same order dated 19.5.2018 passed in Complaint No.14/2016 by Shri S V R Srinivas, Principal Secretary, Information and Technology, Government of Maharashtra in the capacity of Adjudicating Officer (AO) exercising jurisdiction under section 46 of the Information Technology Act,2000. Since parties and the issues are common, both the Appeals have been heard together and shall be governed by this common judgement.

4. The proceedings before the learned AO commenced on filing of a complaint on 14.12.2015 by the complainant, Sandeep Singhal, a businessman residing at Nagpur. The complaint contains all the relevant informations with respect to both the respondents, Bank of India, Rana Pratap Nagar Branch, Nagpur and Vodafone Cellular Ltd., Maharashtra. The particulars of claims show that Rs. 18,75,381.41 has been claimed towards actual losses sustained because of alleged negligence of the bank and/or because of negligence of M/s. Vodafone in illegally issuing the duplicate SIM Card to an imposter. Rs. 5 lakhs have been claimed towards actual costs on account of

travelling and litigation expenses etc. Rs 10 lakh has been claimed towards damages on account of mental agonies caused to the complainant.

5. Parties are on issues only on those facts which are in the nature of allegations of negligence/lapses or illegality. The general facts are, however, not in controversy. The complainant is proprietor of Umasan Enterprises and has two Cash Credit Accounts with the concerned Branch of Bank of India, Nagpur. The accounts bearing nos. 872230100000612 and 872230100000712 are in operations since last 30 years in the name of concerned Umasan Enterprises. The accounts have one common unique Customer ID which are operated either by the complainant or in his absence by his wife Smt.Anju.

6. The complainant was enjoying a limited Net Banking Services having only the facility of Intra Banking without facility for RTGS/NEFT transactions to any other bank, except Bank of India Branches. The complainant used to make various payments through such facilities only to Government Departments. Other payments used to be only through cheques. Both the bank accounts were linked with the complainant's mobile bearing a particular number. SMS and OTPs relating to the accounts were received on the said mobile number. The mobile had a Post Paid Card of Vodafone as the telecom service provider. The complainant was using the mobile number for the last 15 years and in March 2010, on the asking of Vodafone, he had filled the KYC

forms and submitted on 26.3.2010. That form had many details of the complainant, his landline numbers, photographs and signatures. Between 22.8.2015 and 28.8.2015, the complainant and his wife and son were at Mumbai for a business tour. On 25.8.2015, at around 3.00 PM, the wife of complainant received a call from the Bank to inquire whether certain transactions of huge amount were being made by them through Net Banking. At that time mobile phone of the complainant was switched off though it was in working condition, till the noon of 25.8.2015. The complainant's wife informed that no such transactions were made by them. Since complainant's mobile had stopped working, she gave information to the complainant through his son's mobile. The complainant called the Bank to make enquiries and learnt that in total a huge amount of Rs. 18.50 lakhs had been debited from his Cash Credit Account No. 872230100000712. On learning about the fraudulent transfers to unknown persons in different branches of the Bank, the complainant asked the Bank to freeze both the accounts although till then, no transfer had been made from the other account. This direction was because both the accounts were having same customer ID. Request was also made to freeze the accounts where the money had been transferred fraudulently. On 26.8.2015, at around 9.15 AM. the complainant's wife received information from the Bank that an amount of Rs. 11.50 lakhs had been transferred from other account no. 872230100000612 also, to different accounts. However, no loss was caused from this account because the transactions were immediately reversed and the account was frozen. On the instructions

of the complainant, his younger son lodged a police case at Nagpur on 25.8.2015 for the fraudulent withdrawal of Rs. 18.50 lakhs. A further complaint to the police was made on the next date also in respect of illegal transactions from the other account on 26.8.2015.

7. The complainant as soon as he realized that his SIM card has been de-activated, approached the nearest Vodafone Store in Mumbai where he learnt that a duplicate SIM card had been issued at Malegaon, Nasik. The request was made on 24.8.2015 at 1858 hours on the basis of fake and forged documents. The duplicate SIM card was issued on 24.82015, but was activated on the next day at 1310 hours and till then complainant's mobile was active. The SIM was issued and activated without verifying the claim and cross-checking the documents submitted by the imposter, with the original identity documents of the complainant submitted with KYC form. It is alleged that duplicate SIM was issued without following the guidelines framed for the purpose, without verifying the documents of imposter and without ascertaining the imposter's identity. The documents of the complainant relating to his identity in KYC as well as documents submitted by the imposter are available on record and a comparison shows that actually there could have been no scope to accept the claim of the imposter if the two sets of documents had been compared even casually. The photographs and signatures are quite different.

8. The complainant has alleged that it was because of negligence and irresponsible behaviour of the respondents in handling the account and personal details of the complainant that led to aforesaid losses to the complainant without their being any fault on his part.

9. With the help of materials contained in the police report available on record and other details, the complainant has made serious allegations against the Bank to the effect that:

(i) It had not followed the RBI guidelines dated 2.7.2012 and in particular clause 2.8 of the circular regarding Money Mule Accounts was violated by not taking sufficient precautions.

(ii) the beneficiary accounts were opened very recently, had very small size of balance and were mostly not in compliance of KYC guidelines.

(iii) The verification of address of the beneficiary account holders was not done, in violation of KYC norms.

(iv) The complainant has disclosed that the transactions details provided by the I. T. Department of Bank give the details of IP addresses located in Nigeria which were used for fraudulent transactions on 25.8.2015. The same IP Address had been used in an attempt to hake petitioner's account earlier also on 7.8.2015 but no serious follow up action was taken by the Bank.

10. In the proceedings before the learned AO, the respondents in the complaint petition i.e. the Bank and Vodafone appeared after notice. Their lawyer's name

appears in the order under appeal. The stand of the Bank was that it had taken all the necessary precautions and acted proactively and as a result, the loss was confined to Rs. 18.50 lakhs from only one of the accounts. However, the stand of the Bank is that fraudulent transfer of money from complainant's account was entirely on account of lapses on the part of Vodafone in issuing duplicate SIM to the fraudster without taking any precautions necessary for KYC. On the other hand, the stand of Vodafone is that it had no knowledge or awareness about the mobile connection being used for the purpose of operating bank accounts opened by the complainant with the Bank. According to Vodafone, it is not at all connected with the fraudulent withdrawal of money from complainant's account and that it issued the duplicate SIM card to an imposter in good faith after complying with the necessary formalities for issuance of another SIM card when it is reported to be lost.

11. Learned AO has undoubtedly written a short order wherein on the basis of relevant facts pleaded by the parties and also after taking into account their submissions and in the case of Vodafone written submissions, it has been held that the Bank seems to have followed all the norms but there was delay in freezing the beneficiary accounts of fraudulent transfers and such delay led to the financial loss. The Bank also failed to notice that the IP Address was based in Nigeria. These findings of the learned AO do not hold the Bank responsible for the fraud or even

guilty of not having adequate security measures. Since the loss could not be minimized by freezing the beneficiary accounts immediately, the Bank was also held liable to pay Rs. 3.5 lakhs to the complainant as compensation. It is for obvious lacunae in security measures which can discourage such frauds if implemented promptly.

12. So far as the case of Vodafone is concerned, the learned AO has, at the outset, identified the main issue as per his understanding in following words:

"The order pertains to loss on account duplicate SIM card given to a person who allegedly was not real owner of the mobile SIM card".

In his short order, the AO has referred to Police case lodged in respect of fraud, in Pratap Nagar Police Station on 25.8.2015. He has noted that the matter was investigated by the police who made some arrests and came to conclusions on the basis of documents and the pleas of the parties including the Bank and Vodafone. Learned AO has noticed that the plea of the complainant and the Bank against Vodafone are similar and the report of the Investigating Officer of the concerned police station is along the same lines.

13. After noticing the stand of Vodafone, learned AO has indicated that it has noted the averments and the written statement of the complainant as well as the respondents and he found that the loss was caused to the complainant due to the duplicate SIM Card issued to the alleged imposter without following the KYC norms.

14. According to learned AO, respondent no. 2 (Vodafone) should have thoroughly checked all the relevant documents before issuing a duplicate SIM as per Telecom guidelines. Even the signature of the complainant and the alleged imposter should have been properly tallied but this was not done by Vodafone. It was because of the duplicate SIM that money was transferred to the imposter causing loss of Rs. 18.50 lakhs to the complainant.

15. Due to the aforesaid findings, mainly against Vodafone, learned AO awarded Rs. 15 lakhs as compensation to be paid by Vodafone to the complainant.

16. Learned counsel for the Bank has pleaded for allowing Cyber Appeal No. 3 of 2018 in the light of relevant facts showing that the bank was proactive and informed the wife of the complainant that complainant's mobile had been deactivated. The findings of learned AO that the Bank seems to have followed all the norms, has been highlighted to support the plea that Bank should not be held liable for the loss to the complainant rather it had helped in recovery of money that had been transferred on 26.8.2015 from the other account and hence, the entire loss should be recovered from Vodafone.

17. On behalf of Vodafone, learned senior counsel has placed entire relevant provisions of the Information Technology Act, 2000 (hereinafter referred to as "the Act") and also of The Information Technology(Qualification and experience of

Adjudicating Officers and manner of Holding Enquiry) Rules, 2003 (hereinafter referred to as "the Rules").

18. Before adverting to the relevant provisions, it is indicated that the purpose of highlighting the statutory provisions and the relevant rules appears to vindicate the defence of Vodafone that as a Telecom Service Provider, it cannot be held guilty either under section 43 or section 43 (A) of the Act . The AO has to hold inquiry in a fair and judicious manner and in two stages as indicated in rule 4 of the Rules.

19. According to learned senior counsel, the orders passed by AO must show judicious application of mind because his role is identical to not only Civil Court deciding a claim for compensation for similar losses when the claim is above Rs. 5 crores but also in the same spirit in which inquiry is held or ought to be held under the Foreign Exchange Management Act (FEMA).

20. In large number of similar appeals, Telecom Service providers have taken similar pleas to the effect that in cases of such fraudulent transfer or withdrawal of money from Banks, they are merely intermediaries protected by the section 79 of the Act and their liability, if any, should be limited only to failure or lapses in KYC verifications, which is required for maintaining CAF (Customer Acquisition Form). In other words, the plea of Vodafone is also that lapses in following the procedure for KYC or CAF

can be raised only in appropriate fora through proper proceedings; such allegations cannot be a subject matter of the IT Act, unless it can be shown that the allegations are covered by section 43 or 43 (A) of the Act so as to give jurisdiction to the AO to hold inquiry and award compensation. The plea of intermediary protection under section 79 also must be kept in mind by the AO, but that has not been done.

21. In order to appreciate the aforesaid submissions and contentions on behalf of Vodafone, it will be useful to analyse the various relevant provisions of the Act as highlighted by learned senior counsel.

Section 43 is as follows :

"43. [Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(*a*) accesses or secures access to such computer, computer system or computer network [or computer resource];

(*b*) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(*c*) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(*d*) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(*e*) disrupts or causes disruption of any computer, computer system or computer network;

(*f*) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
(*g*) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
(*h*) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
(*i*) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
(*j*) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]

2[he shall be liable to pay damages by way of compensation to the person so affected.]

Explanation.–For the purposes of this section,–

(*i*) —"computer contaminant" means any set of computer instructions that are designed–
(*a*) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
(*b*) by any means to usurp the normal operation of the computer, computer system, or computer network;
(*ii*) —"computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
(*iii*) —"computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
(*iv*) —"damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
[(*v*) —"computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]"

Sector 43A is as follows :

"43A. Compensation for failure to protect data.–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation – For the purposes of this section –

(i) –body corporate means any company ;and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) –reasonable security practices and procedures means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) –sensitive personal data or information means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

22. Chapter IX of the Act provides for penalties, compensation and adjudication for all civil wrongs. Criminal offences when made out, are governed by provisions in Chapter XI. No special court or forum has been created for trial of offences and hence

these fall within the jurisdiction of competent criminal courts. Provision under section 79 relating to intermediaries is provided in Chapter XII. Section 79A in Chapter XIIA enables the central government to notify examiner of electronic evidence for the purposes of providing expert opinion on electronic form of evidence before any court or other authority. Chapter XIII contains miscellaneous provisions. Under this Chapter, Section 81 provides that this Act shall have effect notwithstanding anything inconsistent therewith contained in other law for the time being in force. The proviso to this section creates an exception only in respect of Copy Right Act, 1957 and the Patents Act, 1970. Sections 87 and 90 contain powers of Central Government and the State Government respectively to make rules.

23. Before considering the main issues argued on behalf of Vodafone, it appears useful to clarify that in a case of present nature, a Telecom Service Provider like Vodafone cannot claim exemption from liability as an intermediary. Section 79 (1) creates the exemption or the protection in following words :

> **"79. Exemption from liability of intermediary in certain cases.**–(*1*) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (*2*) and (*3*), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him."

This protection is further qualified by sub-sections (2) and (3) of section 79 which are as follows :

(*2*) The provisions of sub-section (*1*) shall apply if–

(*a*) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(*b*) the intermediary does not–

(*i*) initiate the transmission,

(*ii*) select the receiver of the transmission, and

(*iii*) select or modify the information contained in the transmission;

(*c*) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(*3*) The provisions of sub-section (*1*) shall not apply if–

(*a*) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(*b*) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.–For the purposes of this section, the expression —third party information‖ means any information dealt with by an intermediary in his capacity as an intermediary.

24. The word 'intermediary' has been defined in Section 2(1) (w). As per the definition, 'intermediaries', with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

25. Telecom service providers are explicitly included as intermediary but as is clear from sub-sections (2) and (3) of section 79, the exemption under sub-section (1) shall apply only when it is providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or

hosted. The exemption further applies only if the intermediary does not initiate the transmission, select the receiver of the transmission or modify the information contained in the transmission. Additionally, for the exemption to be attracted, even as an intermediary it has to observe due diligence while discharging his duties under the Act and also has to observe such other guidelines as the Central Government may prescribe. Sub section (3) limits the exemption in categorical terms by providing that sub section (1) granting exemption shall not apply if the intermediary has conspired or abetted or aided or induced in any way in the commission of an unlawful act and also if on getting knowledge of misuse of its services with the help of any offending information, data or communication in commission of the lawful act, it fails to expeditiously remove or disable access to such material. The explanation at the end of section 79 limits the meaning of the expression "third party information" to any information dealt with by an intermediary in his capacity as an intermediary.

26. When a Telecom Service Provider is able to show that it is handling only the information, data or communication link for any third party then subject to provisions in sub-sections (2) and (3), it can lawfully claim exemption from liability but such exemption clearly cannot apply when the Telecom Service Provider is dealing with matters which are not related to third parties but with its own customers with whom it already has a service contract and whose personal data or information has been

collected through CAF or KYC process and as per requirement stored in the data base of such Service Provider. The protection of interest of its subscribers who are not in any way third parties, cannot be covered by exemption granted by section 79 of the IT Act. Hence, there is no requirement of further analyzing the submissions advanced by learned counsel for the complainant that even if section 79(1) was to apply to subscribers and consumers of Vodafone by treating them as third parties, in view of requirement under sub section 2 (b) (ii) and (c), the intermediary is required to observe due diligence and observe or follow other guidelines prescribed by the Central Government such as the Information Technology (Intermediaries Guidelines) Rules, 2011 (hereinafter referred to as the Guidelines Rules of 2011). Under Rule 3 of the Guidelines of 2011, the intermediary is required to follow due diligence while discharging a number of duties enumerated in that rule. One of the duties is to strictly follow the provisions of the Act or any other law for the time being in force. The intermediary is required to also take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011.

27. Once the computer resource of the intermediary contains informations relating to SIM No. and other details of a subscriber, these informations have to be kept secured

and not allowed to be tampered or changed in a casual manner. Such information is required to be secured almost in identical terms as required by section 43A of the Act.

28. For the purpose of determining the jurisdiction of the Adjudicating Officer, the most relevant provision is section 46 in Chapter IX. The parameters of his jurisdiction extends to and is co-extensive with his power to adjudicate as to whether any person has committed a contravention of any provisions of the Act or of any rule, regulation etc. which renders the person liable to pay penalty or compensation under Chapter IX and matters related thereto as provided in the Act. The Central Government is vested with the power to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government as an Adjudicating officer for holding an inquiry in the manner prescribed by the Central Government. The word 'inquiry' has been used in an expansive manner to cover all facets and aspects of adjudication for the purpose of levying penalty or compensation under Chapter IX. The jurisdiction extends to claims for injury or damage not exceeding Rs. 5 crores. For Higher claims the jurisdiction shall remain with the competent Court. The Adjudicating officer is required to grant a reasonable opportunity to the person proceeded against for making representation in the matter. On the basis of inquiry, the AO, if he is satisfied that the person has committed the contravention, may impose or award appropriate penalty or compensation.

29. Since the Adjudicating officer may have to adjudicate claims involving amount upto Rs. 5 crores, he is required to possess prescribed experience in the field of Information Technology together with legal or judicial experience of prescribed nature. The proceedings before the AO are deemed to be judicial proceedings for the purpose of sections 193 and 228 of Indian Penal Code and the AO is deemed to be a Civil Court for certain provisions in the Civil Procedure Code as well as in the Code of Criminal procedure. He has the same powers of a Civil Court which have been conferred on the Cyber Appellate Tribunal.

30. The provisions in the Rules of 2003 further add to the eligibility and qualification for Adjudicating officer. Rule 4 specifies the scope and manner of holding inquiry in respect of contraventions in relation to Chapter IX of the Act. When a complaint is made to the adjudicating officer of a State or Union Territory having jurisdiction on the basis of location of computer system, the AO is required to issue a notice together with all the documents to all the necessary parties, fixing the date and time for further proceedings. The notice is also required to contain important particulars as to the time and place of the alleged contravention, the subject of the contravention and the person against whom the contravention is alleged. On the date fixed, the AO is required to explain to the person or persons to whom notices were issued about the alleged

contravention. If the person pleads guilty, such plea will be recorded and the AO may impose penalty or award appropriate compensation. The person served with notice may in the alternative show cause why an enquiry should not be held for the alleged contravention and why the report alleging the contravention should be dismissed. The AO on the basis of relevant materials can decide for holding an enquiry or to dismiss the report of the matter. If not dismissed, the AO shall proceed to hear the matter, even ex-parte, if required. There is specific power enabling the AO to get any matter or report investigated from an officer in the office of Controller or CERT – IND or from the concerned police officer with a view to ascertain more facts or whether prima facie there a case for adjudication.

31. The AO is required to fix a date and time for production of evidence if he does not dismiss a matter at the initial stage.

32. Rule 5 of the Rules of 2003 provides for passing of a final order by the AO upon consideration of the evidence produced and other records and submissions. If the AO is satisfied, he can award compensation or impose penalty under relevant provisions of the Act or the Rules. Relevant considerations for adjudging the quantum of compensation or penalty have also been indicated in Rule 5(b).

33. Rule 9 gives due primacy to the proceedings before the AO by providing that the same matter shall not be pursued before any Court or Tribunal or any authority in any proceeding what so ever and if there is already filed a report in relation to the same matter, the proceeding before such other Court, Tribunal or Authority shall be deemed to be withdrawn.

Rule 10 enables the AO to impose certain costs for frivolous complaints.

Rule 11 permits compounding of contraventions if any application to that effect is filed by the person proceeded against.

34. Clearly, in respect of contraventions for which provisions have been made in Chapter IX, the AO having jurisdiction is required to exercise all its powers in the light of provisions in the Information Technology Act and the Rules prescribed for the purpose. It requires no reiteration that a statutory authority has to act within the four walls of the statute. In that sense the Act and the rules may be accepted as a complete code to the extent they are relevant and apply to the AO.

35. The orders of the AO are subject to appeal before the Cyber Appellate Tribunal whose powers are now vested in this Tribunal.

36. Section 61 of the Act debars any suit or proceeding before any court in respect of any matter which lies within the jurisdiction of the AO or the Appellate Tribunal.

37. Since the adjudicating officer has been vested with power to adjudicate, under section 46(1) only "for the purpose of adjudging under this chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, ... which renders him liable to pay penalty or compensation.", the relevant provisions under sections 43, 43A, 44 and 45 contained in Chapter IX become relevant because only these provisions specifying various contraventions and penalty vest the AO with the jurisdiction to adjudicate. In a case of present nature involving fraudulent withdrawals from the Bank accounts of account holders, provisions of sections 44 and 45 are not attracted. The only material sections are 43 and 43 A which have already been extracted earlier. These require a closer look for appreciating the jurisdiction of the AO.

38. Section 43 seeks to ensure that computers and computer systems or computer networks are not interfered with, accessed, damaged, disrupted, destroyed in any material way so as to affect their integrity, sanctity or working, by any person who does not have permission of the owner or incharge of the concerned computer. The data, information or computer source code have all been included in various clauses of section 43 with a view to protect these also from unauthorized damage, theft or

extraction. The provisions are clearly to ensure that the wrong doer shall be liable to pay damages by way of compensation to the person affected by such wrong acts. The liability for such civil damages is not affected even if the wrong doer becomes liable for criminal charges for such acts when done with criminal intentions.

39. Clause (g) of section 43 adds a new dimension by extending the liability to pay damages by way of compensation even to those who provide "any assistance to any person to facilitate access to a computer etc. in contravention of the provisions of this Act, rules or regulations made thereunder." This is in addition to clause (a) which by itself makes unauthorized access unlawful so as to attract damages by way of compensation. Since the liability created by clause (g) is only civil in nature it does not require particular motive or frame of mind to attract penalty. The use of the word "any" before the word "assistance" further widens the net. The reach and scope is thus rendered quite wide. In addition to a person doing the acts prohibited by various clauses of section 43, any person who provides any assistance to any person to facilitate unauthorized access is equally liable to pay damages by way of compensation, keeping in view the factors enumerated in section 47 which are relevant for determining the quantum of compensation.

40. In contrast, section 43 A is not for wrong acts which find mention in section 43. It applies only to a body corporate for its negligence in implementing and maintaining

reasonable security practices and procedures. If such negligence by a body corporate possessing, dealing or handling any sensitive data or information causes wrongful loss or wrongful gain to any person such body corporate can be held liable to pay damages by way of compensation to the person affected. The purpose of this provision is to ensure that if a "body corporate", a term which includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities, possesses, deals or handles any sensitive personal data or information which has been defined in the explanation, then it has to be careful and can not be negligent in implementing and maintaining reasonable security practice and procedures which also have been explained with the help of explanation no. (ii).

41. It is always easy for a body corporate or any person such as Bank which stores sensitive data or information to claim that it has installed and put to use the required level of security, practice and procedures and that it should not be held negligent. However, such plea in order to succeed must be proved by bringing on record the details of security practices and procedures; when they were implemented and how these are being maintained. Even such materials may not amount to a successful defence unless the bank is able to further demonstrate with the aid of necessary copies of logs, records and data that in the particular incident which is subject matter of

adjudication, these practices and procedures were actually put to practice and in spite of that the unauthorized or fraudulent transition took place causing loss to the complainant.

42. An important issue arises in matters like the present one-whether the Telecom Service Provider falls under any of the prohibited acts under section 43 or section 43A when clearly the computer, computer system or computer network of a Bank is distinct and separate from the computer etc. of the Telecom Service Provider. The only clause which can often get attracted against a Telecom Service provider in case of present nature is clause (g) of Section 43 if during adjudication it is found on the basis of relevant materials that the Telecom Service Provider has provided assistance to the wrong doer to facilitate unauthorised access to the computer, computer system or computer network leading to violation of one or the other clause of section 43 and unlawful loss or damage to the person affected.

43. The telecom service provider, as discussed earlier, has the details of all persons who are already its customers / subscribers. Such details include personal details including photograph, signature, mobile number etc. and also details of the SIM through which such subscriber is permitted to utilize the Telecom Services. The Scope and variety of Telecom services depend upon technology that is expanding every day. It is lawful and permissible for the subscriber to depend upon communications through the mobile number allotted to him with his Banker and with other persons without threat or

apprehension of unlawful invasion of his privacy. In such a situation transferring the aforesaid facilities by changing the SIM number already available in the personal data or information of the customer/ subscriber can have serious adverse impact upon the subscriber. If such an eventuality happens because the Telecom Service Provider is found to be negligent in implementing and maintaining reasonable security practice and procedures as mandated by Guidelines Rules of 2011 and thereby it has caused wrongful loss to the subscriber, section 43 A can also get attracted against the Telecom Service Provider. The plea that the lapses in verifying the bonafides and authenticity of the person applying for a duplicate SIM amount only to violation of CAF procedure or KYC procedure cannot have any diluting effect upon the rigours of section 43 A. Once the essential ingredients of negligence are attracted and established. The minor penalties for CAF violations or for KYC lapses cannot be treated to be an effective shield against claims arising under sections 43 and 43A.

44. On the basis of above discussion, it can be safely concluded that if the facts and materials are found sufficient, in a case of present nature involving unauthorised / fraudulent transfer of money from a bank with the help of a duplicate SIM issued in the an apparent negligent manner, the Telecom Service Provider which has issued the duplicate SIM and made it operational by including the same in its computer network, can be held liable to pay damages by way of compensation under section 43 A read with Section 43 (g) of the Act. The Telecom Service Provider, in his turn, in an

appropriate case may sue its errant employee/agent for appropriate relief of recovery etc. but that will not be a shield against a claim by an aggrieved subscriber.

45. In order to strengthen the aforesaid conclusion it has been pointed out by the learned counsel for complainant that in respect of already existing customers/ subscribers, the Telecom Services providers have important sensitive personal data which they are possessing, dealing, handling in their computer network.

46. Computer network as defined under 2(1) (j) includes communication devices that has been further defined in Section 2(1) (ha) to mean cell-phones, personal digital assistance or combination of both or any other devise used to communicate, send or transmit any text, video, audio or image.

47. On behalf of Vodafone, it was pointed out that provisions for observing security practices and procedures in the matter of issue of duplicate SIMs has been included in the guidelines of Department of Telecommunications (DoT) only through guidelines dated 1.8.2016 ; the earlier guidelines of 2012 provide guidelines for issuance of SIM to a new subscriber and also for change of SIM from pre- paid to post- paid and vice-versa but not specifically for issue of duplicate SIMs. In reply, learned counsel for the complainant has submitted that the purpose of CAF guidelines is to ensure that SIMs are issued, even originally, only to verified users whose identity and address is

established. This is required inter-alia for national security purpose also. He further submitted that the same consideration would be attracted even when a request is made by someone for deactivating an earlier SIM and for issuing a duplicate SIM. Such applicant cannot be presumed to be the existing subscriber or is authorized representative unless the credentials are fully and diligently verified. He pointed out that while dealing with application for duplicate SIM, the Telecom Service Provider has the added advantage of comparing the particulars of the applicant including his photograph and signature with that of the subscriber already existing in the data base which is required to be maintained under the CAF guidelines issued by DoT. The concern for national security etc. are equally relevant at the time of issue of duplicate SIM. Otherwise it can easily fall in wrong hands and cause additional loss to the original subscriber also. The need for higher level of diligence in matters of security and procedures arises in such cases because the Telecom Service Providers have important duties towards their subscribers not to compromise their personal informations by sheer negligence and lack of security measures. The submissions advanced on behalf of the complainant are found to have merits that even as per 2012 guidelines, the Telecom Service Providers has to adopt all the basic security measures before deactivating the SIM of its subscriber and issuing a fresh SIM card to an applicant, claiming to be an existing subscriber.

48. In several similar matters including in the present case, it has been noticed that at the time of deactivating original SIM and activating the duplicate SIM, the Telecom Service Provider or its authorized representative does not make any attempt to contact the original subscriber on the original SIM or alternative contact numbers, if for nothing else, only to ascertain the response from the other end. If the original SIM is still with the subscriber, deactivation may be delayed by few hours to enable the original subscriber to demonstrate that the applicant of the duplicate SIM card is an imposter.

49. In the present case, the details of the subscriber/complainant as contained in the KYC form available with the Telecom Service Provider contain his photograph and signatures as well alternative telephone numbers. The documents submitted by the imposter who applied for duplicate SIM also contain photograph and signatures but not all the information available in the KYC form of the subscriber. A comparison of the two documents reveals that the photograph of the subscriber is quite different and signature is also apparently different. No expert is required to compare and come to the conclusion that the applicant for the duplicate SIM card was not the subscriber and such a claim was entirely bogus and fraudulent. Clearly the claim of the Telecom Service Provider that the details were verified and checked is incorrect and unacceptable.

50. The judgment by the learned AO has been criticized on the ground that it was passed without proper hearing and without considering relevant documents such as police report. The grievance that the oral hearing was not adequate, has been raised only on behalf of Vodafone and that to in a half -hearted manner without supporting the same with order sheet etc. or certificate of the lawyer. No such grievance has been raised in the memo of appeal preferred by the Bank. The other grievance that the materials on records have not been fully considered, is mainly because the impugned order of the AO is a short one contained in only about three pages. However, while hearing the appeal and passing the present judgment, this aspect was kept in mind and it was found that although the order is short but it does not suffer from any error on the material aspects and does not require interference.

51. In the facts of the case, the major responsibility is found to lie with the Telecom Service Provider and hence, ordinarily, the entire compensation should have been realized from Vodafone but learned AO rightly noticed that the Bank, on 25.8.2015, froze the concerned account of the complainant but freezing of the accounts of beneficiaries in various branches of the same Bank, was not done promptly. Hence there is a contributory negligence on the part of the Bank also and, therefore, imposition of a penalty by way of compensation of Rs. 3.5 lakhs on the Bank also, does not require interference.

52. With a view to remove any doubt, it is made clear that in the facts of the case, the telecom service provider, Vodafone is found liable under section 43(g) and section 43A of the Act whereas the Bank is found liable only under section 43A of the Act.

53. The complainant has not filed any independent appeal but has made averments in its reply that it is entitled to interest and further damages as originally claimed before the AO. For this purpose, a more specific notice was required to be given to appellant before this Tribunal by labeling the claims as cross appeal or cross claim. But that has not been done. Further, the learned AO has not recorded that such claims were pressed before him and has not dealt with them. Hence, the claim for damages etc. in addition to the amount already awarded, is not found acceptable. In the interest of Justice and equity, it must be noticed that as per AO the complainant was entitled to receive Rs. 15 lakhs from Vodafone and Rs. 3.5 lakhs from the Bank within one month of the impugned order dated 19.5.2018. If the amount has not been paid to the complainant still, the same must be paid within one month from today along with interest @ 9% p.a to be calculated from June,2018 till the date of realization.

54. The above interest does not compensate the complainant for the loss of Rs. 18.50 lakhs from August 2015 but it is the minimum interest which must be paid by the appellants in case they have not obeyed the order of AO and have not paid the amount in question within the time granted.

55. The complainant shall be entitled to costs of Rs. 25,000/- in each of the Appeals payable within one month from today, failing which the same shall also carry interest `@ 9% per annum from the date of this judgment till the date of realization. In case the appellants do not pay the decretal money within the time granted by this Tribunal, the complainant shall be entitled to get this judgment executed as a decree through the learned AO by filing an application for that purpose.

56. The Appeals are dismissed with the aforesaid findings and directions along with the MA(s), if any.

.....
(S. K. Singh, J)
Chairperson

sc