BEFORE THE ADJUDICATING OFFICER & PRINCIPAL SECRETARY
(THE INFORMATION TECHNOLOGY ACT 2000/ITAA 2008)
GOVERNMENT OF TELANGANA

Petition No. 01 OF 2017

30th day of September, Two Thousand Nineteen

PRESENT: Sri. Jayesh Ranjan, IAS
Adjudicating Officer & Principal Secretary, ITE&C Department,
Government of Telangana

Application filed on: 4th December 2017

BETWEEN :

Mr. Raja Uttam Kumar,
S/o. Raja Ramendra Prasad,
Age: 48 Years, Occ: Software Engineer,
R/o. Secunderabad-5000009 an NRI
Now in United States of America
Rep. by his GPA holder Muneesh Bajpai .... Petitioner

AND

1. ICICI Bank Limited,
Secunderabad Branch,
G-1, Navketan, SV Road,
Secunderabad.

2. ICICI Bank Limited,
ICICI Bank towers,
Bandra-Kurla Complex,
Mumbai – 400 051,
Represented by its Managing Director &
Chief Executive Officer. .... Respondents

Advocates:
1. For the Complainant: P.V.Krishnamachary, Advocate
2. For the Respondent: S. Nagesh Reddy, Advocate

This application filed Under Section 43A and 46 of the Information Technology Act,2000 is coming on this day before me for final hearing in the presence of Sri. P.V.Krishnamachary, Advocate, for the Petitioner and Sri S. Nagesh Reddy, Advocate for the respondents upon perusing the material papers on record evidence and hearing the arguments from both the sides having stood over for consideration till this day the Court doth Order:-

ADJUDICATION AWARD

The brief facts of the case are that the complainant is an NRI now residing in Union City of California, USA and he is the customer of the respondent ICICI bank having a Non Resident Rupee (NRE) Bank account bearing Number 004801079178 with the Respondent Bank, Secunderabad Branch at G-1, Navketan, S.D. Road, Secunderabad, Telangana State holding both Fixed Deposit Accounts and Savings bank account. The customer operates the account through the Internet Banking facility using a password based access. For some of the transactions like the closure of Fixed Deposits, the OTP based second factor authentication is also used.

2. During December 2015, the customer allegedly suffered a loss of Rs.43,07,525/- on account of two sets of unauthorized transactions passed through the account. One set of transactions related to the unauthorized fund transfer from the NRE account by creating fake beneficiary accounts and transferring funds to them. The second set of transactions involved premature closure of Fixed Deposits and credit of proceeds to the NRE Savings Bank account for further transfer. These transactions continued for nearly 15 days without being flagged.

3. The following fixed deposits were closed and credited to his A/c. No.004801079178 of ICICI Bank and from that account those amounts were transferred to Ac No. 189900101002278 of corporation bank, Varalakshmi Nagar Maduravoyal Thiruvallur District, Chennai Through NEFT.

Sl. No	Date	Amount credited in Rs.
1	07-12-2015	10,00,000
2	11-12-2015	4,95,000
3	11-12-2015	5,00,000
4	14-12-2015	4,75,000
5	14-12-2015	5,25,000
6	18-12-2015	2,60,000
7	18-12-2015	3,80,000
8	18-12-2015	3,60,000
9	21-12-2015	3,12,525
	Total amount	**43,07,525**

4. The fraud was identified nearly a month later by the Petitioner when he could not log into his account and therefore called the call center of the Bank to enquire the reasons and the bankers registered his complaint No.SR397566171 for the fraudulent withdrawals.

5. The complainant has also filed a Police Complaint at the instance of the Bank and investigations have been in progress vide FIR No.3 of 2016, dt.26.02.2016 under Section 66 r/w 43 (a) of IT Act 2000/ITAA 2008 and Section of 420 Indian Penal Code 1860 on the file of the Cyber Crime Police CID, Telangana State, Hyderabad. One of the identified fraudsters has been arrested on 30.03.2017 while one other is reported to be abroad and the others are shown absconding.

6. Heard both the parties and their detailed arguments. Written submissions have also been submitted by both the parties. The Petitioner examined as PW-1 and marked the following documents as exhibits

1. Exhibit A-1 : E-Mail date 27.12.2016
2. Exhibit A-2 : Email dated 17.3.2016
3. Exhibit A-3 :Email dated 23.03.2016.
4. Exhibit A-4 :Email dated 08.03.2016

5. Exhibit A-5 :E-Mail date 11.03.2016
6. Exhibit A-6 :FIR No.03/2016 dated 26.02.2016 along with remand case dairy
7. Exhibit A-7 : Special power of attorney date 05.5.2017
8. Exhibit A-8 : E-Mail date 15.5.2012
9. Exhibit A-9 : E-Mail date 12.05.2012
10. Exhibit A-10 : E-Mail date 11.5.2012
11. Exhibit A-11 : E-Mail date 10.5.2012
12. Exhibit A-12 : E-Mail date 10.05.2012
13. Exhibit A-13 : E-Mail date 09.5.2012
14. Exhibit A-14 : E-Mail date 7.8.2012
15. Exhibit A-15 : E-Mail date 12.10.2011

7. The respondent bank adduced evidence of RW-1 and marked the following documents as exhibits

Ex. B1	---	Power of Attorney dt.21.08.2015
Ex. B2		Copy of executive summary
Ex. B3	---	exchange of e-mails dated 08.12.2015
Ex. B4	---	copy of Cyber Crime Police addressed letter to Respondent dt.26.02.2016
Ex. B5	---	Reply to Cyber Crime Inspector 16.03.2016
Ex. B6	---	Notice issued Under Section 91 of Cr.P.C 28.03.2016
Ex. B7	---	Notice issued under Section 91 of Cr.P.C 17.05.2016
Ex. B8	---	Letter addressed to Inspector Cyber Crime 31.05.2016
Ex. B9	---	Notice issued under section 91 of Cr.P.C 21.06.2016
Ex. B10	---	Letter to Inspector of Cyber Crime dt; 22.07.2016
Ex. B11	---	Notice issued under section 91 of Cr.P.C. 26.07.2016
Ex. B12	---	Letter to Inspector of Cyber Crime dt. 04.08.2016
Ex. B13	---	Notice issued under section 91 of Cr.P.C 10.08.2016
Ex. B14	---	Letter to Inspector Cyber Crime dt. 14.09.2016
Ex. B15	---	Letter to Reserve bank of India from Respondent along with material papers

Ex. B16	---	Letter to the Assistant General manager Department of Banking Supervision RBI, Hyderabad dt.03.11.2016

8. Both parties as well as the Police agree that this is a case of a fraud involving multiple outsiders. Whether there was any assistance from any of the employees of the Bank or whether there was any password compromise from the customer through phishing and whether there was failure of the bank to send timely alerts etc., are points on which the parties have argued.

9. The main contention of the Bank is that the complainant is a victim of a phishing attack where he could have compromised his password by answering a phishing mail or clicking on a malicious hyper link.

10. The Bank also alleges that they had sent OTP to the mobile of the customer as registered in the Bank for premature closure of the Fixed Deposits and probably for the creation of the beneficiaries as well and that they got a positive return response. It is on the ground of such suspected compromise of the password and alleged OTP confirmation that the Bank holds the Customer solely responsible for the loss. The Bank expects the complainant to pursue recovery through the Police.

11. The Complainant denies that there is any Phishing attack on him and any compromise of the password. He is unable to provide any other clue to the possibility of the fraud except the possible involvement of the Bank employees who could be in collusion with the outsiders for mutual benefit. The customer builds his theory of collusion based on the fact that the mobile numbers registered for the account are different from his mobile number.

12. The Police confirm the fraud but have not made investigations sufficient to establish or rule out the insider involvement. Since this forum is only interested in settling the complaint as per Section 46 of the ITA 2000, further criminal investigation is out of scope of this Adjudication.

Observations:

13. The mutual allegations of the Petitioner that there is insider involvement in a fraudulent collusion and that of the Bank that there is a compromise of the Password through Phishing at the customer/Petitioner end require to be established through appropriate evidences.

14. Unfortunately, the Petitioner is not very much in a position to produce any evidence since the fraudulent transactions have occurred in the Bank's electronic premises. The Bank has not produced evidence under the premise that it has some privacy obligations. Even the internal fraud audit report has not been shared to support their view that the cause for fraud was entirely at the complainant's end. During the cross examination of RW-I on 28.02.2019 it was admitted that respondents have not submitted the IP address from where OTP was triggered and not provided the KYC documents.

15. For our purpose we have to ignore the statements and go by whatever evidence is available on record. The fact that a fraud has occurred and a wrongful loss has been caused to the Petitioner is admitted by both the parties and it is not disputed. Hence this forum has the jurisdiction to adjudicate how the wrongful loss has to be compensated and by whom.

16. If there is an insider involvement as alleged by the Petitioner, then there is no doubt that the bank has to bear the loss. However, with the available information, it is difficult to establish insider involvement in the

fraud. Also it would be inappropriate for this forum to go into determining the possibility of criminal involvement of any of the employees of the Bank.

17. This line of investigation is left to the Police who needs to continue their investigations to find out how there was a mismatch of the registered mobile number in the records and whether this is an indication of insider involvement.

18. Had the bank produced the application form for Mobile Registration which is normally obtained in physical form, it would have established if the Banks contention that the registered mobile number had in fact been given by the customer himself. Since the Bank has not produced the copy of such a form, we need to presume that no such form may exist. The non submission of this evidence is sufficient prima facie reason for us to reject the contention of the Bank that the customer alone must be considered as responsible for a wrong mobile number having been registered with the account. Assuming that there is no positive confirmation on this aspect of insider involvement, we shall focus more on the Civil liabilities that arise in this case under ITA 2000.

Negligence Relevant for Section 43 and 43A:

19. The cause of action for this forum to step in cases of frauds such as what this complaint represents arises either because of any of the provisions of Section 43 of IT Act 2000 having been contravened or failure to maintain "Reasonable Security Practice" under Section 43A.

20. Under Section 43A, the Bank which is in possession of sensitive information of the customer fails to maintain reasonable security practices and thereby a wrongful loss occurs, then it would be liable to compensate the customer for the loss. This section is straight forward in the sense that the liability is directly linked to the concept of "Reasonable Security Practice" which we shall discuss later.

21. Under Section 43, any person suffering a wrongful loss on account of contravention of any provision of IT Act 2000 can invoke the section. The liability to pay damages under Section 43 is on the person who without the permission of the owner of a computer

(a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)

(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 there under,

(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) Steals, conceals, 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,

22. Under Section 43, the primary responsibility to compensate lies on the person who commits any of the acts mentioned in the section. It is clear that most of the 10 different sub sections here apply to the perpetrators of the fraud.

23. However, Section 43(g) falls in a different category since if it is established that any person assisted another person to contravene the law, such a person would also be liable directly under Section 43. This liability for the person who assists and who may not be the beneficiary of the fraud is also indicated in Section 84B of ITA 2000 which states,

24. Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

25. Therefore the "Negligence" is relevant both under Section 43 and 43 A. "Reasonable Security" under Section 43A as defined in the Act and the rules include the security as prescribed in law. The security practice mandated by RBI as the regulator of the Banks assumes importance as "Reasonable Security Practice".

26. Hence the security related recommendations by RBI in the form of the Internet Banking in India Guidelines of 2001, E Banking Security Guidelines of 2011 (GGWG recommendations) and the Cyber Security Framework of 2016 all define the "Due Diligence" lack of which makes a Bank liable under Section 43 and Section 43A. The police have already registered an FIR under Section 66 which also indicates that they have taken cognizance of the contravention of Sec.43.

No Evidence of Phishing:

27. The contention of the Bank that the Petitioner would have parted with the password and grid values etc., by responding to a Phishing message etc., is a statement by the Bank and is not supported by any evidence. Coming from the respondent, it may be dismissed as a self serving defence. To make the Petitioner liable, it is necessary to have some proof of phishing. At this point of time, Bank has not produced any evidence that there has been a phishing attack on the customer. In fact there is evidence to the contrary because the complainant has produced some evidence to say that his laptop has been examined and found not to contain any malware as alleged by the Bank.

28. The fact that the debits in the account are spread out over several days and include intermittent FD closures, is inconsistent with the phishing frauds which normally generate a series of debits over a short period with a few minutes gap between different debits. The pattern of debits in this instance is more indicative of manual attack on the Bank server and more in tune with the allegation of the Petitioner that there could be insider connivance with professional fraudsters. The indications are sufficient to reject the Bank's contention of a Phishing attack.

Due Diligence Requirements:

29. The RBI guidelines under the Cyber Security Framework in Banks of 2016 (RBI Circular dated June 2, 2016), RBI has stated

> *"....Among other things, banks should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, wishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc"*

In the same circular, RBI has detailed the expected security measures that Banks need to set up in the form of "Security Operations Center" (SOC). One of the requirements of such SOC is to identify potential Phishing attacks. In the present case, there is no proof adduced by the Bank indicating that the Bank has taken sufficient steps as suggested above.

30. Even as early as in June 2001, RBI made its stand clear on the Bank's responsibilities in protecting the customer's interest through its Internet Banking guidelines. In its circular dated June 14, 2001, RBI stated:-

> *"Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks."*

31. The RBI was clear that the technology based risks need to be covered by the Banks and not be hoisted in the customers.

32. In the same circular dt.14.06.2001, RBI also pointed out the inadequacy of the system of authentication that the Banks allow for internet Banking through passwords by stating as follows:-

> *"From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for*

signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk"

"Under the present regime there is an obligation on banks to maintain secrecy andconfidentiality of customers' accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/other technological failures. The banks should, therefore, institute adequate riskcontrol measures to manage such risks".

33. In the present case, the Respondent Bank has placed its faith only on Password based authentication backed by OTP and further failing to establish a reliable system for registering the customer's mobile and delivery of OTP. The respondent Bank not registered the Mobile alert for the petitioner's Net Banking account and without registering the SMS alert allowing the customer to unsecure Internet Banking is nothing but sheer negligence of the respondent Bank.

34. It is clear from the documents that the "Premature Closure" of Fixed deposits have been handled by the Bank like a savings bank withdrawal responding to requests received through password based entry into the Internet Banking space. The premature closure of fixed deposit being in the nature of a withdrawal of a contract deserves to be treated with multiple levels of authentication which the Bank has distinctly failed to use.

35. The Cyber Security framework mandated by RBI also requires an "Adaptive Incident Response" where the authentication of any unusual transaction has to be elevated to a higher level than normal transaction. The premature closure of FDs as well as the withdrawal of over **Rs. 43.00 lakhs** within a short span of 7 days with moneys transferred through NEFT to third parties calls for being recognized as "Unusual" and identified as fit for some special scrutiny.

36. The Bank does not seem to adopt such an "Adaptive Authentication System" which has facilitated the commission of the fraud. As seen from the above the body corporate of Respondent Bank failed to adopt reasonable security practices and procedures in protecting the sensitive data of the petitioner in the computer resources operated by the respondent bank. Thereby the respondent had caused wrong full loss of money to the petitioner. As such the body corporate respondent bank shall be liable to pay damages by way of compensation to the person affected.

37. Further it is the bounden duty of the Respondent Bank to lodge a complaint with the law enforcement agencies immediately on detection of the fraud. There should ideally not be any delay in filing of the complaint with law enforcement agencies since the delay may result in the loss of relevant documents non availability of witnesses, absconding of borrowers and also the money trail getting cold in addition to asset stripping by the fraudulent borrower. In the present case it is clearly established that the respondent had deliberately avoided to initiate criminal proceedings with law enforcement agencies for the best reasons known to them. Somehow with a great difficulty the complainant got registered a complaint with Police as Ex-A6 which reveals the fraud and the remand case diary established that the fraudulent transfers not made by the complainant and the offence took place within the electronics premises of the Respondent Bank. The Ex-B2

Executive summary reveals that the bank suspect the fishing and eMail hacking techniques must have been used to siphon of the funds since customer claimed to have not parted his personal details and had not received OTPs by FD liquidation alerts sent by the Bank though the grid values also used which is privy only to the customer points to the fact that the same must have been parted by the customer knowingly or unknowingly. Ex-B3 are email alerts sent to the customer Sri Raja Uttam Kumar hot mail showing the messages were sent and **Queued mail for delivery** which is not a conclusive proof of receiving of eMail alerts by the customer. The investigation report and the internal executive summary have not established that the customer compromised his passwords or confidential data to any third party. The contention of the respondent Bank that the customer knowingly or unknowingly compromised is only imaginary and not based on any prudent evidence and there is no conclusive proof that the complainant triggered the grid values. As discussed above, this Court opined that fact findings are left to the investigating agency and the responsibility of the fraud lies on the respondent as the fraud took place in the electronic premises of the respondent bank. It is the primary duty of the bank to protect the money of its customers.

38. In view of the above, it is clearly established that the complainant sustained a loss of **Rs.43,07,525/-** which was admitted by the Respondent also and the said transactions were not made by the complainant and the respondent failed to secure the money deposited by the petitioner with the respondent bank. Since the Fraud has occurred in the electronic premises of the bank, the responsibility for failure to prevent the unauthorized access, failure to keep adequate evidence to support its allegations of phishing as well as pursuing the Police complaint all fall on the Bank. Attempt by the Bank to make the Petitioner/customer responsible for pursuing the Police complaint defies logic and cannot be accepted.

39. Considering the above facts, it is to be concluded that the complainant has suffered a wrongful loss for which he has the right to claim compensation. The liability for paying the compensation does primarily fall on the fraudsters but due to the lack of "Reasonable Security Practice" by the Bank, the liability has also to be undertaken by the Bank. After discharging the liability to the customer, the Bank continues to hold its right to recover the money from the fraudsters and also take recourse to the insurance if available.

ORDER:

Based on the evidences adduced and the relevant documents produced by both the parties, this Court allowed the petition of the complainant by directing the Respondent to pay the following amounts to the petitioner (Complainant).

i. Rs. 43,07,525/- (Rupees Forty Three Lakhs Seven Thousand Five Hundred and Twenty Five Only) towards the damage being the net amount of loss suffered by the complainant on account of the unauthorized transactions. The amount shall be credited to the NRE account from which the amount was withdrawn.

ii. The Bank shall pay an interest @ of 9% per annum on the above amount from 21st December 2015 (The last day when the fraudulent withdrawal occurred) until the date of payment. This amount shall be credited to the NRO account of the complainant.

iii. The respondent ICICI Bank shall pay an amount of Rs.5.00 Lakhs (Rupees Five Lakhs) towards compensation for mental agony/injury suffered by the Petitioner.

iv. The Bank shall pay Rs. 50,000/- (Rupees Fifty Thousand) towards cost of expenses of the applicant.

v. Payments by the Respondent to the Petitioner shall be made within (60) days from the date of this order and in case of delay, penal interest @ 12% (per annum) shall be payable from the date on which the amount payable became due till the amount is paid fully.

Typed to my dictation, given under my hand and seal of this court on this day of 30th September, 2019.

Sd/-
Adjudicating Officer & Principal Secretary to Govt.,
ITE&C Department, Govt. of Telangana

// CERTIFIED TRUE COPY //

30/09/2019

Presenting Officer &
Joint Director (Comm)
ITE&C Department,
Govt. of Telangana

To

1. The Petitioner (Complainant)
(Through his Counsel. Sri. P.V. Krishnamachary, Advocate, Hyd.)

2. The Respondent
(Through their Counsel, Sri. S. Nagesh Reddy, Advocate, Hyd.)