PLR PLRonline
2022 PLRonline 0398 (Mad.)

HIGH COURT OF JUDICATURE AT MADRAS
Before: Ms. Justice P.T.Asha
ICICI BANK LIMITED – Appellants
Versus
UMA SHANKAR SIVASUBRAMANIAN – Respondents
C.M.A.No.2863 of 2019
(RESERVED ON: 04.07.2022, PRONOUNCED ON: 09.11.2022)

(i)Phishing – Is a form of an internet fraud – Like the name and its pronunciation it means "throwing a bait to catch the fish" which in the case of internet phishing is the person receiving the e-mail – However, phishing e-mails are sent from email addresses which look identical to the genuine e-mail address with very minute changes which are visible only to a discerning eye – At a glance it would look like the genuine e-mail address thereby luring the user to part with his vital details. [Para 19]

(ii)Information Technology Act , Sections 43(a), 43(b), 43(8), 46(1) – Domain name – Identical – Phishing E-mail received and the e-mail ID in the admitted documents appear to be one and the same and it is identical – The domain name in both is the same, namely, icici.com – Domain name is an unique feature – Bank has not categorically stated that the e-mail address from which the phishing e-mail has emanated is not that of the Bank and why the Bank thinks it is a fictitious e-mail address – Complaint therefore falls within the provisions of Sections 43(a) and 43(b) of the ITA, which gives jurisdiction to the adjudicating authority under Section 46(1) to consider the complaint – From the fact that the Bank has not been able to establish that the e-mail address from which the phishing e-mail had been sent does not belong to the Bank, the only conclusion that can be arrived at is that the address has been compromised by somebody working within the Bank – Therefore, the complaint will also come within the provisions of Section 43(8) of the ITA. [Para 19]

(iii)Cyber fraud – Unnatural transaction – Banks liability – Email from same domain name as that of the bank – Not denied by bank – Conclusion that there has been connivance at the Bank's end with the fraudster – Bank account of complainant with bank – Normal withdrawals from the account is only within the range of Rs.20,000/- – On one day a huge amount of over Rs.6 lacs was withdrawn within a gap of 15 minutes with each withdrawal being a sum of Rs. 1lacs – Bank should have noticed an unnatural transaction and should have raised a red flag – Case of the complainant that he has not received any SMS alert or e-mail confirmation and would have immediately stopped the transaction – No documents filed by bank to show that such alert has been sent by the Bank – Bank intimated complainant only after the transaction has concluded and that too beyond the banking hours in the form of a telephone call and not by way of an e-mail alert or SMS alert – Though the complainant has immediately denied the transaction, no steps have been taken to freeze the account of the beneficiary account held with the bank – Bank appropriated some amount towards its loan dues and permitted cash withdrawals from the fraudsters account – Only conclusion that can be drawn is that there has been connivance at the Bank's end with the fraudster to take away the complainant's money – Bank despite coming to know that the beneficiary/fraudster had committed a fraud especially when the complainant had denied that he had transferred money to the beneficiary account, the Bank has not taken any steps to lodge a complaint with the Cyber Police – They have only directed the complainant to lodge a complaint thereby washing their hands of the entire transaction – Bank liable. [Para 19]

(iv)Cyber fraud – Duties of banks – Bank even after coming to know that the account of the complainant has been tampered / manipulated and a fraudulent transaction has taken place did not take any steps to independently lodge a complaint against the fraudulent party into whose account the money had been transferred Bank negligent – They have only directed the complainant to lodge a complaint thereby washing their hands of the entire transaction, which in the considered opinion of this Court does not augur well for a banking institution which works only on the trust of the customers. [Para 19, 21]

(v)Cyber fraud – Duties of banks – Cyber awareness – In this age of advancement in technology where predators are waiting in the wings in the virtual world as the whole world is connected through digitalization, the role of the Bank towards protecting the interests of its customer assumes greater significance – A strong cyber security is therefore the order of the day and Banks should not only provide it but educate its customers on the potential threats – In a country like ours where the bulk of the citizenry are illiterate, this becomes all the more necessary. [Para 21]

Held,

The grievance of the complainant is that he has been lured into divulging his confidential information from the registered e-mail address of the Bank from which he has been receiving the periodic statement of accounts. The Bank has simply contended that the complainant is the victim of a phishing e-mail. Phishing is a form of an internet fraud. Like the name and its pronunciation it means “throwing a bait to catch the fish” which in the case of internet phishing is the person receiving the e-mail. However, phishing e-mails are sent from email addresses which look identical to the genuine e-mail address with very minute changes which are visible only to a discerning eye. At a glance it would look like the genuine e-mail address thereby luring the user to part with his vital details. However in the case on hand a perusal of the e-mail I.D of the phishing e-mail and the e-mail ID in the admitted documents appear to be one and the same and it is identical. The domain name in both is the same, namely, icici.com. The domain name is an unique feature. The Bank has not categorically stated that the e-mail address from which the phishing e-mail has emanated is not that of the Bank and why the Bank thinks it is a fictitious e-mail address. The complaint therefore falls within the provisions of Sections 43(a) and 43(b) of the ITA, which gives jurisdiction to the adjudicating authority under Section 46(1) to consider the complaint. From the fact that the Bank has not been able to establish that the e-mail address from which the phishing e-mail had been sent does not belong to the Bank, the only conclusion that can be arrived at is that the address has been compromised by somebody working within the Bank. Therefore, the complaint will also come within the provisions of Section 43(8) of the ITA. The conduct of the Bank during this transaction and particularly its conduct thereafter leaves much to be desired. The complainant has a saving bank account (NRE) with the Bank’s Tuticorin Branch. This apparently is the Bank account to which the complainant has been remitting money for his people back home. The withdrawals for the month of August 2007 reveal that in total a sum of Rs.50,000/- has been withdrawn and each withdrawal is only within the range of Rs.20,000/-. That being the case on 04.09.2007, when a huge amount of Rs.6,46,000/- was being withdrawn within a gap of 15 minutes starting from 10.10 a.m to 10.25 a.m with each withdrawal being a sum of Rs.1,00,000/-, the Bank should have noticed an unnatural transaction and should have raised a red flag. It is the categoric case of the complainant that he has not received any information about the withdrawals in the form of SMS alert or in the form of e-mail confirmation. Had the complainant been put on notice, he would have immediately stopped the transaction. The withdrawals have taken place between 06th and 7th September 2007. On 06.09.2007, a sum of Rs.5,00,000/- has been withdrawn in 5 tranches of Rs.1,00,000/- each. On 07.09.2007, another sum of Rs.1,00,000/- and thereafter, a sum of Rs.46,000/- has been withdrawn. The Bank has intimated the complainant only after the transaction has concluded and that too at 1800 hours (UAE time) which means the call had been made by the Bank at 07.30 p.m (Indian time) beyond the banking hours in the form of a telephone call and not by way of an e-mail alert or SMS alert. Though the complainant has immediately denied the transaction, no steps have been taken to freeze the account of the

5th respondent. On the contrary, the Bank appropriated Rs.35,000/- from out of this money transferred to the 5th respondent-s account towards the 5th respondent-s outstanding to them and permitted the cash withdrawal from the 5th respondent-s account. The Bank would contend that they have provided an alert to the complainant. However, no documents whatsoever had been filed to show that such alert has been sent by the Bank to the complainant. In the absence of the above, the only conclusion that can be drawn is that there has been connivance at the Bank-s end with the fraudster to take away the complainant-s money. Another factor which compels this Court to arrive at this view is that despite coming to know that the 5th respondent had committed a fraud especially when the complainant had denied that he had transferred money to the 5th respondent, the Bank has not taken any steps to lodge a complaint with the Cyber Police. On the contrary, they have only directed the complainant to lodge a complaint thereby washing their hands of the entire transaction, which in the considered opinion of this Court does not augur well for a banking institution which works only on the trust of the customers.

In the instant case, the Bank even after coming to know that the account of the complainant has been tampered / manipulated and a fraudulent transaction has taken place did not take any steps to independently lodge a complaint against the 5th respondent into whose account the money had been transferred. In this age of advancement in technology where predators are waiting in the wings in the virtual world as the whole world is connected through digitalization, the role of the Bank towards protecting the interests of its customer assumes greater significance. A strong cyber security is therefore the order of the day and Banks should not only provide it but educate its customers on the potential threats.

Tony Enterprises, v. Reserve Bank of India, 2019 PLROnline 3401 Ker.

Amitabha Dasgupta v. United Bank of India (2021) SCC Online SC 124 , referred to.

For Appellant: Mr.Shivakumar for M/s.Shivakumar and Suresh, For Respondent-1: Mr.M.L.Sribathi, For Respondents 2 and 3 : Given up, vide order dated 17.10.2009, For Respondent-4 : Served – No appearance, For Respondent-5 : Dr.S.Surya, Additional Government Pleader

JUDGEMENT

The 1st and 2nd respondents before the Adjudicating authority, have filed the above civil miscellaneous appeal challenging the order passed by the Telecom Disputes Settlement and Appellate Tribunal, New Delhi in Cyber Appeal No.1 of 2010 and Review Application No.2 of 2019 in and by which, the Appellate Tribunal had modified the judgment dated 12.04.2010 made by the Adjudicating Officer under the Information and Technology Act, 2000 in Petition No.2462 of 2008.

A. Facts of the case:

Complainant-s case:-

2. The facts briefly constituting the complaint are herein below narrated. The parties are referred to in the same rank as set out before the Adjudicating authority. The appellants herein who were arrayed as respondents 1 and 2 before the Authority are collectively referred to as the Bank herein.

(i) The complainant would submit that he was employed in Abu Dhabi having his permanent address at Tuticorin. He had maintained a saving bank account (NRE) with ICICI Bank, V.E.Road, Tuticorin. The said account was also activated with an internet banking facility. The complainant would submit that he has been receiving regular statements of account from an e-mail address customercare@icicibank.com. At the end of August 2007, his account had a balance of Rs.6,20,846/-. On 04.09.2007, his account was credited with a sum of Rs.25,200/- towards the interest and the balance had increased to a sum of Rs.6,46,046/-. On 07.09.2007, he had received a telephone call from a staff of the ICICI Bank, Mumbai, at around 1800 hours (UAE time) enquiring as to whether he had transferred any money to the 5th respondent (4th respondent herein) on 6th and 7th September 2007. The complainant had denied the transfer. The respondent-Bank immediately asked him to lodge a complaint with the banker’s customer care at Mumbai against his transfer and they

had shared the telephone number of the customer care centre. Immediately, the complainant had lodged a complaint, which was also registered. The complainant had also sent the complaint by facsimile and e-mail. By their letter dated 13.09.2007, the Bank and its customer care centre requested a month's time to process the complaint and they had also advised the complainant to lodge a police complaint.

(ii) The complainant would submit that thereafter, there was no proactive steps taken by the Bank. Therefore, his complaint did not yield the desired results. Meanwhile, the complainant had received the statement of account which would show that the entire sum of Rs.6,46,000/- was unauthorisedly transferred out of the complainant's account between 06th and 07th September 2007 to the credit of the current account of the 5th respondent. It also revealed that from out of the above sum the Bank had adjusted a sum of Rs.35,000/- towards the outstanding due from the 5th respondent to the Bank and regularised their account. That apart, a total sum of Rs.4,60,000/- was paid out in cash from the account of the 5th respondent against the cheque to some persons. The 5th respondent thereupon retained a sum of Rs.1,50,171/-.

(iii) The complainant on 24.10.2007 had lodged a complaint with the Police at Tuticorin, which was subsequently transferred to Cyber Crime PS, Chennai. Thereafter, the complainant had made a fresh complaint before the Cyber Crime Police. The Bank took a stand that the e-mail address in which the phishing had taken place was not generated by them. The Bank also took a stand that they are unable to reach the current account holder, the 5th respondent herein. The complainant would submit that an e-mail address within parenthesis cannot be changed except by an expert or with the assistance of special tools. The complainant strongly suspected an insider hand. The further reason for entertaining the above suspicion was on account of the fact that the 5th respondent had opened an account just 3 years prior to the incident. The account was overdrawn and a sum of Rs.35,000/- remained outstanding. The last of the transaction had taken place on 01.04.2007. The complainant would submit that despite all these anomalies, the respondent-Bank has not exercised any caution when such a huge sum of Rs.4,60,000/- has been withdrawn on a single day within a short span of 15 minutes. Further, the Bank has not issued its statutory messages when such a huge sum has been withdrawn from the complainant's account where the normal transaction for a month did not exceed Rs.50,000/- Further, the Bank had not come clear about the 5th respondent and interestingly, no police complaint had been lodged by the Bank. The Bank has also enriched itself with this fraudulent act by appropriating a portion of money to their outstanding dues from the 5th respondent. The complainant would further submit that the Bank had not complied with the Information Security Prescription mandated by the Reserve Bank of India, vide its circular dated 14.06.2001. The complainant would further state that there was a gross negligence on the part of the Bank and contended that the entire proceedings violates Section 66 of the Information Technology Act (hereinafter referred to as "ITA"). The complainant therefore accused the Bank of violating Sections 66, 43 and 85 of ITA.

B. Counter of respondents 1 and 2

3. The Bank in its counter statement had admitted the following facts:

(i) That the account of the complainant has been fraudulently debited and unauthorisedly credited to the account of the 5th respondent, who is also. a customer of the respondent-Bank

(ii) That the 5th respondent is holding a current account, which was overdrawn for over 2 years.

(iii) That they are also beneficiaries by reasons of this transaction.

(iv) That the Bank had not provided the CCTV footage to show that the identity of the person, who has withdrawn the amounts from the account of the 5th respondent.

4. The Bank had further stated that the complainant had earlier filed the very same complaint before the Banking Ombudsman. It is their contention that the Bank cannot be held liable to compensate the complaint, since it is the complainant, who has volunteered to disclose all his information to a phishing e-mail. The respondent-Bank has time and again cautioned its customers from providing their details to fraudulent e-mails. The Bank had also questioned the jurisdiction of the adjudicating authorities by contending

that the issue involves an elaborate enquiry and evidence which cannot be navigated by an adjudicating authority. A statement was also made that the complainant was aware that the phishing e-mail emanated from the IP address of the 5th respondent. (This statement is far from the truth, since the complainant has been repeatedly requesting the Bank to give the IP address from which the phishing e-mail had emanated). The respondent-Bank would submit that they had offered the following internet facilities:

(a) Transfer of funds

(b) Enquiry about the balance

(c) Details about the transaction in the account.

(d) Payment for bills

(e) Statement of Accounts, etc.,

5. The bank had further submitted that they have periodically given details about the various safeguards that are required to be followed by customers, who opt for Net Banking facilitates. They are updated about the security aspects of internet banking through various channels like monthly / quarterly statements, posters located at ATM-s, display at branches and mainly through the website of the Bank (www.icicibank.com) and security measures that had to be adopted for safeguarding the account. The Bank had also stated that while offering the internet banking service, the complainant has agreed to the following terms and conditions.

1. The user unconditionally undertakes to have the user ID provided by 100 Bank changed and ensure that the same is kept confidential and not to let any unauthorized person to have access to the same.

2. Neither ICICI Bank nor its Affiliates shall be liable for any unauthorized transactions occurring through the internet banking and the user fully indemnifies and holds ICICI Bank harmless against any actions, suit, proceeded against it.

The Complainant having unconditionally agreed for the said Terms and Conditions had negligently disclosed the confidential information such as ID and Password and thereby had fallen prey to the phishing mail.

6. The Bank would further contend that they had diligently followed the KYC details with reference to the 5th respondent. They would also contend that they had done a detailed investigation through their complaint wing and the IP address pertaining to the transaction has been secured. The details of the IP address has been reproduced in the counter statement. A perusal of which would show that since the complainant had disclosed his confidential information and password by responding to the phishing e-mail, he had allowed an unauthorized transaction by a fraudster. The complainant having himself compromised his details cannot hold the Bank responsible for the loss sustained by him. The Bank would justify the adjustment of a sum of Rs.35,000/- from out of the amounts clandestinely transferred from the complainant's account by stating that they had only exercised their banker's right of set off as soon as money had come to the account to the 5th respondent which was overdrawn. The Bank would submit that they not only use the password as the source of authentication but also adopt mobile alters / SMS confirmation. However, interestingly, nowhere in the counter is it stated that this source of authentication has been adopted in the case of the complainant particularly the mobile alert / SMS confirmation. The Bank sought to have the appeal dismissed.

7. The 5th respondent had not entered appearance or contested the complaint.

C. Adjudicating Authority:

8. The Adjudicating Authority, by its judgment dated 12.04.2010, had first dealt with the issue of maintainability since the Bank had questioned the jurisdiction of the adjudicating authority to consider the complaint. The adjudicating authority had observed that since the offences come within the scope of Section 43 and 85 of the ITA, the complaint was very much maintainable before the adjudicating authority who was the authority constituted under the Act to try the complaints.

9. On perusing the evidence and the submissions of the learned counsels, the adjudicating authority has observed that an e-mail had been received by the complainant

from the regular e-mails address of the Bank. However, the Bank had not taken any steps to distinguish e-mails arriving from their official server and e-mails arriving from elsewhere. They had further pointed out that there is no layer of authentication in the case of the transaction now under consideration. The Bank had not insisted on digital signature and there is no layer of protection to help the customer to identify a phishing e-mail from an authentic e-mail. The withdrawal of money from the account was possible, since the Bank had not provided the sufficient precautions. In fact, the communication from the Bank itself was from a gmail account, which clearly pointed out to the fact that the Bank had no safe and standard mode of communication. That apart, it was rather strange that the Bank had not filed a complaint but had only asked the customer to file a complaint. This assumes significance since the person into whose account the money was transferred is also a customer of the Bank's Mumbai Branch. It was the indifference and systemic failure displayed by the Bank, which had resulted in a huge loss to the complainant. The complainant has neither received an SMS nor an e-mail alert from the Bank. Even after being put on notice about the fraud committed, the Bank did not take steps to involve the police in the investigation. The authority found it rather strange that the Bank had not been alerted when such a large amount has been transferred from the account of the complainant to a dormant account of the 5th respondent, where the transaction had stopped as early as on 01.04.2007. That apart, the attempts made by the Bank to secure the 5th respondent leaves much to be desired. Ultimately, the complaint was allowed and a sum of Rs.12,84,327/- was awarded. The details of which are herein below:

Financial loss to the complainant = Rs.4,95,829/-

Interest at 12% per annum from the date of financial loss suffered by the petitioner = Rs.1,60,648/-

Adjudication fees = Rs. 27,950/-

Financial loss on travel and incidental expenses = Rs.6,00,000/-

D. Appellate Tribunal:

10. Challenging the said order, the Bank filed an appeal before the Telecom Disputes Settlement and Appellate Tribunal, New Delhi in Cyber Appeal No.1 of 2010. The Appellate Tribunal raised a query as to why the respondent-Bank had not responded to the e-mail from the complainant as to how the sub domain is created. The Appellate Tribunal has also found that the Bank had not provided required precaution to prevent the misuse of the internet banking facility and therefore, confirmed the judgment passed by the Adjudicating authority. However, the Appellate Tribunal had partly allowed the appeal by rejecting the levy of a sum of Rs.6,00,000/- towards the incidental expenses. The Bank was held liable to pay a sum of Rs.7,34,327/- to the complainant.

11. The complainant had filed a review to this order on the ground that the year of the judgment had been wrongly typed as 10.01.2018 instead of 10.01.2019 and also no amounts had been granted towards the incidental expenses. The Appellate Tribunal had awarded a sum of Rs.50,000/- towards consolidated costs and allowed interest at the rate of 12% on the entire amount now awarded, i.e Rs.4,95,829/-, 1,60,049/- and Rs.27,850/-. It is challenging the appeal as well as the review that the respondent-Bank is before this Court.

E. Submissions:

12. The learned counsels on either side had made their oral as well as written submissions.

13. The learned counsel for the Bank had given a concise statement of the dates and events starting from the opening of the account, which is verbatim extracted herein below as there was no objection to this statement by the learned counsel for the complainant.

Sl.No. Date Description of document

Sl.No.	Date	Description of document
1		The first Respondent is a NRI working at Abu Dhabi, UAE. He had a Savings bank Account (NRE) with the first Appellant bearing A/c. No. 613901200505.
2		The first respondent had also opted for internet banking facility for the above mentioned account.
3	02.09.2007	First Respondent had shared the credentials of the internet banking account, like user ID, password, Debit Card number and PIN number, in a website link, sent to him by email with the domain name of icicibank.com
4	06/07th September 2007	A sum of Rs.6,46,000/- was debited from the said account of the first respondent and was transferred to the Account No. 623505378469 held by one M/s. Uday Enterprises, with the second Appellant Branch, by way of seven (7) transactions.
5	06/07th September 2007	The said M/s Uday Enterprises, in turn withdrew a sum of Rs. 4,60,000/- from their account.
6	07.09.2007	The first Respondent claims that he had received a phone call from the 2nd Respondent about the debits and that he was advised to complain if he had not done the same.
7	–	The first Respondent had given a complaint to Customer care and reference number SR 37195467 was assigned
8	10.09.2007	The first respondent had emailed a complaint to the Appellants, wherein he has admitted that he had furnished the internet banking account details along with password by way of reply to the phishing mail. Reply was sent by the bank that the matter was being investigated and it would be reverted as to the resolution and that the amounts in the account of Uday Enterprises has been freezed.
9	20.10.2007	Mail by bank staff reporting the update on investigation stating that it is actually a Actual Infinity Phishing Fraud; amounts were withdrawn from the account of M/s. Uday Enterprises by self cheques across the counter; the Bank is not liable for the unauthorized transactions; the KYC of the account has

Sl.No.	Date	Description of document
		been verified which disclosed that the account was opened after obtained the KYC documents; and that the company is now not available in the address given said to have been vacated.
10	24.04.2008	The Appellant bank had also confirmed that it was a case of actual Infinity Phishing Fraud and a criminal case has to be lodged with the police by customer, on the basis of their investigation.
11	17.07.2008	The Appellant bank had transferred a sum of Rs.1,50,171/- which was lying in ICICI Bank in M/s Uday Enterprises account to the first respondent's account.
12	–	The first respondent states to have given a compliant to the Superintendent of Police in Tuticorin.
13	06.02.2008	The first respondent is said to have lodged a fresh complaint to the Cyber Crime Cell, CCB at Chennai
14	–	The first respondent preferred a complaint against the Appellants and Respondents 2 to 4 herein before the Adjudicating Officer under Section 43, read with section 46 of the Information Technology Act, 2000, for adjudication.
15	19.02.2009	The Appellants filed a counter to the said complaint before the Adjudicating Officer stating that there was no mistake on its part and it was a clear case of phishing fraud and the bank was not responsible for the same in any manner under section 43 of the Act.
16	12.04.2010	Order was passed by the Adjudicating Officer in the Complaint Petition No. 2462 of 2008 in which the Appellants (ICICI Bank) were directed to pay Rs.4,95,829/- with 12% interest from 06.09.2007 and with travelling and adjudicating expenses of Rs.6,00,000/- totaling to a sum of Rs. 12,85,000/- to the first respondent.
17		Aggrieved by the Order the Appellants preferred Appeal No. 1 of 2010, before TDSAT (Appellate Authority),under section 57 of the IT Act, 2000.

Sl.No.	Date	Description of document

18	02.06.2010	The First Respondent filed his reply in Appeal No. 1 of 2010 before the TDSAT (Appellate Authority).
19	10.01.2019 (wrongly stated as 10.01.2018)	Order was passed in Cyber Appeal No.1 of 2010 by TDSAT (Appellate Authority), granting partial relief, in so far the adjudicating expenses granted by the Adjudicating Officer was reduced to Rs. 50,000/-, while confirming the other part of the order.
20	19.01.2019	Review application was filed by the first respondent stating that there is a mistake in the date of order, the year of the IT Act is wrongly stated and that the interest for the period pending appeal should be awarded.
21	03.04.2019	Order was passed by TDSAT in R.A. No. 1 of 2019, correcting the date of order and year of the Act and holding interest payable during the period of appeal, but however to give credit to the amount deposited and the accrued interest.
22	April 2019	Aggrieved by the Order the Appellants have preferred the present Civil Miscellaneous Appeal under Sec. 62 of the Information Technology Act.

14. Mr.Shivakumar, learned counsel appearing for the Bank would submit that the complainant had received a phishing e-mail from the e-mail address “ICICI Bank <customercare@icicibank.com> on 02.09.2007. The Bank would complain that without confirming either through phone or e-mail as to the authenticity of the e-mail, the complainant has proceeded to share all his confidential details. With this information, the fraudster had transferred the money. The Bank would deny sending such an e-mail. They have also contended that the person who has accessed the e-mail of the complainant has used the confidential information to transfer the amounts to the account of the 5th respondent. The Bank cannot be held responsible for the transaction. The learned counsel would submit that after the complaint was given by the complainant to the Bank, they had conducted a detailed investigation, which confirmed, it was the case of actual infinity phishing fraud and these transactions had taken place only on account of the negligence on the part of the complainant. By sharing their confidential information to the phishing e-mails, no negligence can be fastened on the Bank. As soon as the Bank had come to know that the transaction thereunder a sum of Rs.4,60,000/- has been withdrawn, a sum of Rs.1,50,171/-, which is lying to the credit of the said 5th respondent, has been frozen by the Bank. He would further argue that the provisions of Section 43(g) of the ITA will not apply to the facts of the instant case, since it is not a case of gaining any access to the computer system or internet. On the contrary, the complainant himself has parted with his confidential details. The learned counsel would further submit that the phishing fraud does not come within the provisions of Section 43(g) of the ITA.

15. It is also the contention of the learned counsel for the Bank that nowhere in the complaint does the complainant state that the Bank has provided the assistance to facilitate access to the respondent’s e-mail. The learned counsel would further submit that the authorities below have misconstrued the word “assistance” provided under Section 43(g) of the ITA. In the instant case, no assistance had been provided by the Bank. The Authorities below have not discussed the evidence, which has prompted them to invoke Section 43 of the ITA. He would submit that the Bank had been periodically cautioning the customers from revealing their details to strange e-mails, despite which the complainant

has parted with his information. It is the contention of the learned counsel for the Bank that since the credentials of the complainant had been compromised due to his own conduct, the Bank cannot be held liable. Therefore, they would pray that the appeal be allowed and the order of the authority below has to be set aside.

16. Per contra, the learned counsel for the complainant would submit that the complainant had received an e-mail from the e-mail address of the Bank, which is the address from which the periodic statements were received by the complainant from the Bank. The complainant would contend that it is not a case of similar e-mail address being used to get the vital information from the complainant but it is the very same e-mail address with the domain name from which the information had been received. This according to the learned counsel for the complainant is a case of an active involvement of staff of the Bank. The learned counsel would further submit that even assuming for a minute the complainant had fallen prey to a phishing e-mail, the Bank by not providing the necessary alerts particularly when a high value transaction was being done in an account where normally the monthly transaction was at Rs.50,000/- has failed to help the complainant mitigate his loss. Had the Bank sent a SMS when the first amount of Rs.1,00,000/- was transferred from the complainant-s account to the 5th respondent-s account the complainant could have immediately reacted. The Bank ought to have raised a red flag particularly when the 5th respondent had been a dormant account for over 3 years and all of a sudden, a huge sum of Rs.6,46,000/- had been transferred to the account of the 5th respondent, which was already over drawn. Another lapse on the part of the respondent-Bank is that they have refused to part with the CCTV footage, which would have shown the person who had withdrawn the amounts from the account of the 5th respondent by depositing cheques. By not providing these details, the Bank appears to be withholding vital evidence. It is only after the transactions had taken place and that too after a day, that the bank had deemed it fit to shoot out a call to the complainant enquiring as to whether the complainant has authorised the transfer of such a huge sum. Though the complainant had denied such a transaction and though the 5th respondent is also a customer of the Bank at Mumbai Branch, the respondent-Bank has not deemed it fit to file a police complaint, which would be the natural reaction, if the Bank had nothing to do with the transaction. The learned counsel would further submit that though the Bank claims that they had several sources of authentication in the form of OTP, SMS alert, e-mail alerts etc., no document whatsoever has been produced to the authorities below that these sources of authentication was made available in the case of the complainant. From the above, it is clear that the complainant has not received any alert. Therefore, the learned counsel would submit that it is clearly evident that there is an involvement of the Bank staff. Therefore, they would pray that the order passed by the Appellate Tribunal be upheld.

F. Discussion:

17. Before discussing the merits of the case on hand, it is necessary to extract some of the provisions of the ITA which has relevance to the case on hand.

Section 43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,

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

(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, he shall be liable to pay damages by way of compensation not exceeding one crore rupees 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, daia 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.

46. Power to adjudicate.

(1) 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, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer-for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred oh the Cyber Appellate Tribunal under sub-section (2) of section 58, and—

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

85. Offences by companies.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section,—

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

18. Section 62 of the Information Technology Act, 2008 gives power to the High Court to re-appreciate the order of the Cyber Appellate Tribunal on the question of fact as well. Section 62 would read as follows:-

62. Appeal to High Court.-

"Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order: Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days".

In the instant case, from the arguments put forward by either party, it is clear that the same does not give rise to any question of law but is only re-appreciation of the evidence on record.

19. The grievance of the complainant is that he has been lured into divulging his confidential information from the registered e-mail address of the Bank from which he has been receiving the periodic statement of accounts. The Bank has simply contended that the complainant is the victim of a phishing e-mail. Phishing is a form of an internet fraud. Like the name and its pronunciation it means —throwing a bait to catch the fish— which in the case of internet phishing is the person receiving the e-mail. However, phishing e-mails are sent from email addresses which look identical to the genuine e-mail address with very minute changes which are visible only to a discerning eye. At a glance it would look like the genuine e-mail address thereby luring the user to part with his vital details. However in the case on hand a perusal of the e-mail I.D of the phishing e-mail and the e-mail ID in the admitted documents appear to be one and the same and it is identical. The domain name in both is the same, namely, icici.com. The domain name is an unique feature. The Bank has not categorically stated that the e-mail address from which the phishing e-mail has emanated is not that of the Bank and why the Bank thinks it is a fictitious e-mail address. The complaint therefore falls within the provisions of Sections 43(a) and 43(b) of the ITA, which gives jurisdiction to the adjudicating authority under Section 46(1) to consider the complaint. From the fact that the Bank has not been able to establish that the e-mail address from which the phishing e-mail had been sent does not belong to the Bank, the only conclusion that can be arrived at is that the address has been compromised by somebody working within the Bank. Therefore, the complaint will also come within the provisions of Section 43(8) of the ITA. The conduct of the Bank during this transaction and

particularly its conduct thereafter leaves much to be desired. The complainant has a saving bank account (NRE) with the Bank's Tuticorin Branch. This apparently is the Bank account to which the complainant has been remitting money for his people back home. The withdrawals for the month of August 2007 reveal that in total a sum of Rs.50,000/- has been withdrawn and each withdrawal is only within the range of Rs.20,000/-. That being the case on 04.09.2007, when a huge amount of Rs.6,46,000/- was being withdrawn within a gap of 15 minutes starting from 10.10 a.m to 10.25 a.m with each withdrawal being a sum of Rs.1,00,000/-, the Bank should have noticed an unnatural transaction and should have raised a red flag. It is the categoric case of the complainant that he has not received any information about the withdrawals in the form of SMS alert or in the form of e-mail confirmation. Had the complainant been put on notice, he would have immediately stopped the transaction. The withdrawals have taken place between 06th and 7th September 2007. On 06.09.2007, a sum of Rs.5,00,000/- has been withdrawn in 5 tranches of Rs.1,00,000/- each. On 07.09.2007, another sum of Rs.1,00,000/- and thereafter, a sum of Rs.46,000/- has been withdrawn. The Bank has intimated the complainant only after the transaction has concluded and that too at 1800 hours (UAE time) which means the call had been made by the Bank at 07.30 p.m (Indian time) beyond the banking hours in the form of a telephone call and not by way of an e-mail alert or SMS alert. Though the complainant has immediately denied the transaction, no steps have been taken to freeze the account of the 5th respondent. On the contrary, the Bank appropriated Rs.35,000/- from out of this money transferred to the 5th respondent-s account towards the 5th respondent-s outstanding to them and permitted the cash withdrawal from the 5th respondent-s account. The Bank would contend that they have provided an alert to the complainant. However, no documents whatsoever had been filed to show that such alert has been sent by the Bank to the complainant. In the absence of the above, the only conclusion that can be drawn is that there has been connivance at the Bank-s end with the fraudster to take away the complainant-s money. Another factor which compels this Court to arrive at this view is that despite coming to know that the 5th respondent had committed a fraud especially when the complainant had denied that he had transferred money to the 5th respondent, the Bank has not taken any steps to lodge a complaint with the Cyber Police. On the contrary, they have only directed the complainant to lodge a complaint thereby washing their hands of the entire transaction, which in the considered opinion of this Court does not augur well for a banking institution which works only on the trust of the customers.

20. In a judgment of the Kerala High Court reported in (2019) PLROnline 3401 (Ker.) [*Tony Enterprises v. Reserve Bank of India, and other*s (W.P(C) No.28823 of 2017) and *Cherian C.Karippaparampil v. Reserve Bank of India,* (W.P(C) No.28824 of 2017)] a learned Single Judge of the Court was considering a case of a SIM swapping fraud to gain access to bank accounts of the petitioners therein and to withdraw money from their bank accounts. The customers who were the victims of this fraud had moved the Court seeking a declaration to the effect that they have zero liability to the Bank in the light of the Circular issued by the Reserve Bank of India. The petitioners in both these Writ Petitions had availed the online banking facility offered by the Bank. The respondent-Bank had taken a defence that the login ID, password and telecom number are only known to the petitioners and that without laches on their part, fraudsters would not gain access to their accounts. In the course of the discussion, the learned Judge has discussed the master circular dated 06.07.2017 protecting customers in unauthorised electronic banking transactions. The circular states as follows:-

> "12. The Reserve Bank of India issued a master circular dated 6.7.2017 protecting customers in unauthorised electronic banking transactions. The circular states that a customer has zero liability in the following events:
>
> (i) Contributory fraud/negligence/deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer)
>
> (ii) Third party breach whether deficiency lies neither with the bank nor with the customer but lies elsewhere in the system and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorised transaction.

The learned Judge observed that the banking transaction is both contractual and fiduciary and discussed the obligation cast upon a Bank qua its customer.

"14. Banking transaction is both contractual and fiduciary. The bank owes a duty to the customer. Both have a mutual obligation to one and another. The bank, therefore, is bound to protect the interest of the customer in all circumstances. The technology as adverted has its own defect. Online transactions are vulnerable. Though the bank might have devised a secured socket layer connection for online banking purpose which is encrypted , this security encryption can be hacked using different methods. The well known hacking modes are phishing, trojans, session hijacking, key logger, etc. The public WiFi is the easiest target for hackers. NORTON, a leading cyber security provider in its web page refers to the risk of using public WiFi. The unencrypted network in public WiFi allows hackers to collect data easily. WiFi snooping using software allows hackers to access everything online while the user is active in online. The possibilities of fetching data relating to the banking account while the customer using online transaction, by the hackers, cannot be overruled in banking transaction. The bank can identify fraud risk and also devise mechanisms to protect customers. There are counter technologies to identify location behaviour of operators also. It is for the bank to secure the safety of online banking transactions.

Defining a □disputed transaction□:

15. A □disputed transaction□ in this context has to be understood as a transaction prima facie tainted by fraud.

Ultimately, the learned Judge held that the amounts withdrawn from the petitioner's account has to be restored to them without prejudice to the bankers right to proceed against the persons who are responsible for the disputed transactions through a civil court.

21. The Hon'ble Supreme Court in the judgment reported in (2021) SCC Online SC 124 [*Amitabha Dasgupta Vs. United Bank of India and Others*] was considering a case where the Bank had broken open the locker of the appellant therein for non-payment of rents and subsequently, the locker had been reallocated to another customer. The appellant therein had filed a consumer complaint before the District Consumer Forum (-District Forum-). The District Forum had allowed the complaint and this was confirmed in part by the State Commission. The revision against the order of the State Commission was dismissed and the National Commission accepted the State Commission's finding on the limited jurisdiction of the Consumer Forum to adjudicate on the recovery of the contents of the locker. Therefore, the customer had moved the Hon'ble Supreme Court. The learned Judges had in very great detail discussed the duty and care that a Bank has to exercise with regard to Locker Management and the kind of records that have to be maintained. The learned Judges had set out some of the procedures that have to be followed by the Bankers while allocating and operating the lockers. The learned Judges found fault with the Bank for having opened the locker without any prior notice to the customer. They had observed as follows:- "breaking open of the locker was in blatant disregard to the responsibilities that the bank owed to the customer as a service provider" and had made the following observations regarding a Bank's duty in the light of the advancing technology in conclusion:-

"55. Before concluding, we would like to make a few observations on the importance of the subject matter of the present appeal. With the advent of globalization, banking institutions have acquired a very significant role in the life of the common man. Both domestic and international economic transactions within the country have increased multiple folds. Given that we are steadily moving towards a cashless economy, people are hesitant to keep their liquid assets at home as was the case earlier. Thus, as is evident from the rising demand for such services, lockers have become an essential service provided by every banking institution. Such services may be availed of by citizens as well as by foreign nationals. Moreover, due to rapid gains in technology, we are now transitioning from dual key-operated lockers to electronically operated lockers. In the latter system, though the customer may have partial access to the locker through passwords or ATM pin, etc., they are unlikely to possess the technological know-how to control the operation of such lockers. On the other hand, there is the possibility that miscreants may manipulate the technologies used in these systems to gain access to the lockers without the customers- knowledge or consent. Thus the customer is completely at the mercy of the bank, which is the more resourceful party, for the protection of their assets."

In the instant case, the Bank even after coming to know that the account of the complainant has been tampered / manipulated and a fraudulent transaction has taken place did not take any steps to independently lodge a complaint against the 5th respondent into whose account the money had been transferred. In this age of advancement in technology where predators are waiting in the wings in the virtual world as the whole world is connected through digitalization, the role of the Bank towards protecting the interests of its customer assumes greater significance. A strong cyber security is therefore the order of the day and Banks should not only provide it but educate its customers on the potential threats. In a country like ours where the bulk of the citizenry are illiterate, this becomes all the more necessary. In an article Cyber world: Advantages and its Emerging Threat the writer has quoted from the National Crime Records Bureau to state that in the year 2020-2021 alone 50,030 cyber crimes were reported and in India more than 2200 cyber attacks are committed per day. The figures are mind boggling which makes it imperative for the Banks offering online banking facilities to enhance their cyber security and rush to take steps to mitigate the loss that a customer may suffer on account of such cyber attacks. In the case on hand unfortunately the Bank has sadly failed to take steps in this regard.

22. Therefore, from the above discussion, there is a clear breach of trust as well. The authorities below have at length discussed the manner in which the complainant had been deprived of his money and why the respondent-Bank should be held responsible. I see no reason to overturn this decision and consequently, the civil miscellaneous appeal is dismissed. No costs.