



IN THE HIGH COURT OF JUDICATURE AT BOMBAY  
ORDINARY ORIGINAL CIVIL JURISDICTION

WRIT PETITION NO.1150 OF 2023

1. Jaiprakash Kulkarni
2. Pharma Search Ayurveda Private Limited ...Petitioners

V/s.

1. The Banking Ombudsman,
2. Bank of Barod (Worli Branch)
3. Reserve Bank of India
4. State of Maharashtra thr.  
Cyber Cell ...Respondents

-----  
Mr. Siddhesh Bhole a/w. Yakshay Chheda, Ms. Anushree Koparkar  
i/b. SSB Legal & Advisory for the Petitioners.

Ms. Aditi Pathak a/w. Parag Sharma, Mr. Vijay Salokhe, Ms. Kirti  
Ojha.

Ms. Megha More i/b. BLAC & Co. for Respondent Nos.1 and 3.

Ms. Anvita Ail a/w. Mr. Naresh H. Manghnani for Respondent No.2.

Mr. Mohit Jadhav, Addl. G. P. for the State.

-----  
CORAM : G. S. KULKARNI

FIRDOSH P. POONIWALLA, J. J.

RESERVED ON : 15<sup>th</sup> MARCH 2024

PRONOUNCED ON : 13<sup>th</sup> JUNE 2024

**JUDGEMENT (Per Firdosh P. Pooniwalla J.):**

1. Rule. Respondents waive service. Rule made returnable  
forthwith. Heard finally by consent of the parties.

2. This Petition deals with a Cyber Fraud and is an example of how increasingly the innocent persons are becoming victims of Cyber Fraud.
3. Petitioner No.1 is a Director in Petitioner No.2, which is a closely held family company of Petitioner No.1. Both Petitioner No.1 and Petitioner No.2 are hereinafter jointly referred to as the Petitioners.
4. The Petitioners had maintained a bank account bearing No.76080200000481 of the Petitioner No.2-Company with Respondent No.2 for the previous 15 to 20 years (“the said bank account”).
5. It is the case of the Petitioners that, on 1<sup>st</sup> October 2022, certain entities/ individuals were added as beneficiaries to the said bank account without any OTP being sent to the Petitioners on the registered mobile number or registered email address.
6. It is further the case of the Petitioners that, on 2<sup>nd</sup> October, 2022, Mr. Vishwanathan Shetty, the accountant of the Petitioner No.2-Company, informed the Petitioners at about 7:45 a.m. that he had received several messages from Respondent No.2 regarding a total sum of Rs.76,90,017/- being debited in several tranches from the said

bank account to various unknown individuals by way of an online transaction.

7. It is also the case of the Petitioners that, since 2<sup>nd</sup> October 2022 was a Sunday and a public holiday, the Petitioners were certain that no transfer requests were initiated by them or any other authorised person and they realized that certain unknown persons had illegally siphoned off the said amount from the said bank account.

8. The Petitioners, within a period of 30 minutes to 1 hour of the aforesaid illegal transactions, informed the Cyber Cell at Worli Police Station, Mumbai and the Bank Manager of Respondent No.2 about the same and were advised to block the Sim Card of the registered mobile number associated with the said bank account.

9. On 3<sup>rd</sup> October 2022, the Petitioner issued a letter to Respondent No.2 narrating the aforesaid incident along with the details of the 20 transactions which took place from the said bank account to several unknown individuals.

10. On 3<sup>rd</sup> October 2022, the Petitioner also lodged a FIR with the Cyber Crime Police Station for offences under Section 379 of the Indian Penal Code, 1860 and Sections 43A and 66 of the Information Technology Act, 2000.

11. On 7<sup>th</sup> October 2022, the Petitioner issued a letter to Respondent No.2 seeking copies of the Security Incident Report as submitted to Respondent No.3, a Cyber Security Incident Report as submitted to CERT-IN and to provide an update on the steps taken to refund the amount of the Petitioner as per the Circular dated 6<sup>th</sup> July 2017 of Respondent No.3-RBI titled Customer Protection-Limiting Liability of Customers in Unauthorized Electronic Banking Transactions.

12. Further, on 7<sup>th</sup> October 2022, the Petitioner also sent emails to the Managing Director of Respondent No.2 inquiring about the steps taken and informing him that the Petitioner has already filed a complaint with Respondent No.1.

13. On 7<sup>th</sup> October 2022, the Petitioner No.1, on behalf of Petitioner No.2, gave an undertaking to Respondent No.2 that Petitioner No.2 was neither connected nor involved with the illegal transactions which took place in the said bank account on 2<sup>nd</sup> October 2022. It is the case of the Petitioners that these undertakings were given on the representation that the Petitioners' grievance would be redressed and the amount would be refunded as per the RBI Circular.

14. On 10<sup>th</sup> October 2022, the Petitioners sent a follow up e-mail to Respondent No.2 inquiring about time within which the said amount of Rs.76,90,017/- would be refunded as per the RBI Circular.

15. On 12<sup>th</sup> October 2022, the Petitioner received an email from Respondent No.3 stating that, since the Petitioner had filed a complaint with Respondent No.3 without filing it first with Respondent No.2, the complaint was not maintainable under Clause 10(2)(a)(i) of the Reserved Bank-Integrated Ombudsman Scheme, 2021. Accordingly, the complaint was forwarded to Respondent No.2 for necessary action.

16. It is the case of the Petitioners that, despite repeated follow up with Respondent No.2, the Petitioners neither received the refund as assured, as per the RBI Circular, nor were the Petitioners provided any update on the process or steps as taken. As a consequence, the Petitioners filed a complaint with the Bank Ombudsman (Respondent No.1) on 12<sup>th</sup> October 2022 for the illegal and unauthorised electronic transfers from the said bank account.

17. The said complaint filed by the Petitioners before Respondent No.1 was rejected by Respondent No.1 by an Order dated 10<sup>th</sup> January 2023 on the ground that the transactions were completed post addition of the beneficiaries and input of valid credentials/2FA known

only to the account holder, and, therefore, there was no deficiency/lapse on the part of Respondent No.2.

18. It is the case of the Petitioners that, despite the specific timelines and procedure as laid down in the RBI Circular as well as the Customer Protection Policy of Respondent No.2, Respondent No.2 had failed to refund the amount illegally debited from the said bank account and Respondent No.1 had wrongly rejected the complaint filed by the Petitioner against Respondent No.2.

19. It is further the case of the Petitioners that Respondent No.2 had informed the Petitioners that, despite the RBI Circular, Respondent No.2 was not willing to refund the amount debited from the said bank account and had asked the Petitioner to approach the beneficiary banks/ police rather than Respondent No.2. It is further the case of the Petitioners that Respondent No.1 had not even considered the fact that the beneficiaries were added without any authority from the Petitioners and without any 2FA (2 Factor Authentication) process being executed by the Petitioners.

20. In these circumstances, the Petitioners have filed the present Writ Petition seeking the following reliefs:-

“A. That this Hon'ble Court be pleased to issue a Writ of Certiorari or any other appropriate Writ, order or direction under Article 226 of the Constitution of India to quash and set

aside the decision of Respondent No. 1 dated 10 January 2023 whereby the Respondent No. 1 has rejected the complaint bearing no. N202223013010460 filed by the Petitioners.

B. That this Hon'ble Court be pleased to issue a Writ of Mandamus or any other appropriate Writ, order or direction under Article 226 of the Constitution of India directing Respondent No. 2 to refund the amount of Rs. 76,90,017/- (Rupees Seventy-Six Lakhs Ninety Thousand and Seventeen Only) to the Bank Account No. 76080200000481 of Pharma Search Ayurveda Private Limited under Rule 6, 9 and 10 of the Reserve Bank of India Circular dated 6 July 2017 'Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions' or under such other rules and / or regulations as framed by Reserve Bank of India;

C. That this Hon'ble Court be pleased to issue a Writ of Mandamus or any other appropriate Writ, order or direction under Article 226 of the Constitution of India directing Respondent No. 2 to refund the aforesaid amount of Rs. 76,90,017/- (Rupees Seventy-Six Lakhs Ninety Thousand and Seventeen Only) along with interest and compensation as per Exhibit 'M' or as may be deemed fit and appropriate by this Hon'ble Court by holding the Respondent No. 2 Bank liable for the breach of the said RBI Circular dealing with Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions dated 6 July 2017;

D. Pass any other Order that this Hon'ble Court may deem fit in the aforesaid facts and circumstances;

E. Costs.”

21. In this Petition, this Court passed an Order dated 26<sup>th</sup> April 2023 which reads as under:-

“1. The Petitioners complain that their corporate current bank account with the Bank of Baroda, Worli Branch was unauthorizedly accessed and an amount of Rs.76,90,107/- was illicitly transferred. The Banking Ombudsman held that there was no deficiency in service. Hence, this Petition.

2. Paragraphs 4(b), (c) & (d) prima-facie indicate that far more information is necessary before we can proceed with the matter. The Petitioners have made a complaint to the Cyber Crime Cell. We will require the logs of the cell phone company that issued the mobile number/SIM used by the Petitioner's accountant Vishwanathan Shetty during the relevant period to see what messages were received on his mobile number. This is necessary because Mr Shetty says that the transactions were

without receipt of any OTP to his mobile number, although that was the only number registered with the bank for net banking purposes. There are some details available at pages 36 to 38. It is unclear how third party transfer or online remittance beneficiaries could have been added without an OTP being received by Mr Shetty.

3. There is additionally other information that we will require which we have indicated to Mr Sakhardande and his attorney, including how Mr Shetty learnt of the insertion of fraudulent entities or persons as beneficiaries and whether the Petitioners are aware of the names of these persons.

4. These details are to be furnished on an Affidavit. We do not require an amendment.

5. The Cyber Crime Cell is requested to make available to the Petitioners and their Advocates access to the Cell Company logs for the purposes of this Affidavit.

6. List the matter on 19<sup>th</sup> June 2023.”

22. As can be seen from the said Order, this Court sought certain information from the Cyber Cell. This information was furnished by the Cyber Police Station, Worli through a letter dated 27<sup>th</sup> May 2023. The said report of the Cyber Cell was put on record by the Petitioner by filing an Affidavit in June 2023. Page 4 of the said report states that, on 1<sup>st</sup> October 2022, when beneficiaries were added to the said bank account, no messages were received from Respondent No.2 on Mobile No.9324265837 which was linked to the said bank account. Hence, beneficiaries were added on 1<sup>st</sup> October 2022 without any message being received on the said mobile number belonging to the accountant of the Petitioners which was registered with Respondent No.2.



23. Further, pages 6 and 7 of the said report show that the messages with respect to logging into the Net-Banking Services on 1<sup>st</sup> October 2022 and adding of beneficiaries to the said bank account were never delivered to the registered mobile number. They show that the OTPs for adding the beneficiaries were undelivered to the registered mobile number. A further perusal of pages 7 and 8 of the said report, which contained the SMS logs of Respondent No.2, show that a total of 15 SMSs were received by the Accountant, Mr. Shetty, on the registered mobile number, on 2<sup>nd</sup> October 2022, from Respondent No.2, regarding the fraudulent transactions undertaken from the said account to the beneficiaries, who were already added on 1<sup>st</sup> October 2022 without any intimation to the Petitioners. The said pages show that, out of the 15 messages that were delivered to the registered mobile number, only two were for OTP and the remaining 13 messages were only debit messages. The Petitioners have stated on Affidavit that Mr. Shetty did not share these two OTPs with anyone. These messages for OTPs were also received by Mr. Shetty at the same time when the other messages of debit transactions were received. Further, the said report also shows that, on 2<sup>nd</sup> October 2022, between 7:44 am and 07:57 am (a total of 13 minutes), the said bank account

of the Petitioner was debited of Rs.76,90,444.70/- in favour of beneficiaries, who had been already added.

24. The said report of the Cyber Cell therefore clearly shows that beneficiaries were added to the said bank account without any intimation of the same being received on the mobile number registered with the bank and that messages were received on the said mobile number only when on the next day (2<sup>nd</sup> October 2022) monies were debited from the said bank account. Thus there was no intimation to the Petitioners about adding of the beneficiaries and the Petitioners only received messages on the registered mobile number when the said bank account was actually debited.

25. After the Petitioners filed the said Affidavit dated June 2023 placing the said report of the Cyber Cell on record, Respondent No.2 filed an Interim Affidavit in Reply dated 31<sup>st</sup> July 2023. In the said Interim Affidavit In Reply, Respondent No.2 submitted that, at the time of addition of the beneficiaries to the Petitioners' said bank account, it was mandatory to login into the bank's website/mobile application by entering confidential information/credentials, i.e., Login ID and Sign on password. This Login ID and Sign On password is known only to the account holder, which in this case were the Petitioners or the Petitioners' assigned persons. It is further stated that,

after entering the correct credentials, the account holder is required to add the details of the beneficiary and, at the end, the account holder has to enter an OTP which is sent through SMS as well as through email on the account holder's registered mobile number and registered email ID respectively. Without the support of such credentials and OTP no beneficiary could be added in a bank account. Even if the mobile alert is missed, the same information is sent across via email ID. It was submitted that, therefore, the addition of beneficiaries was carried out with the knowledge of the Petitioners or of the person who was having access to the confidential credentials and to the e-mail/SMS. It was submitted that these credentials were being compromised from the end of the Petitioners and/or their personnel which indicate negligence on the part of the Petitioners only.

26. In the said Interim Affidavit in Reply, Respondent No.2 further submitted that all the transactions were initiated and completed upon proper validation of customer's credentials. It was further stated that all fund transfers were authenticated and all alerts were also sent to the email address of the customer. Hence there was no deficiency or lapse in the process or system at the bank's end. Respondent No.2 further submitted that, in these circumstances, the negligence was that of the

Petitioner or their personnel and Respondent No.2 could not be held liable.

27. Thereafter, Respondent No.2 filed an Additional Affidavit in Reply dated 27<sup>th</sup> October 2023. In the said Affidavit it was submitted that the Petitioner was negligent in dealing with the matter. It was submitted that, besides the safeguards taken by the bank as detailed in the Interim Affidavit in Reply dated 31<sup>st</sup> July 2023, there were 14 emails generated and served/delivered on the registered email ID of the Petitioner which were pertaining to the OTP, successful login and successful addition of beneficiaries on 1<sup>st</sup> October 2022. It was submitted that the Petitioners and/or their accountant were hand-in-glove with the fraudsters, due to which they purposely ignored these emails.

28. In these circumstances, when the matter came up for hearing on 15<sup>th</sup> February 2024, this Court passed the following Order:-

“ We have heard the learned Counsel for the parties on the pleadings, which have so far come on record.

2 After perusing the documents and more particularly on examining the details of the messages delivered and non-delivered on the registered mobile number of the Petitioners, we require a further clarification. The clarification would be in regard to the details which are set out at page 26 of the Additional Affidavit filed on behalf of the Petitioners, we would require Certificate either from the ‘Police Authorities’ or from the concerned ‘Mobile Company’ (Cyber Crime Branch) in regard to the messages which are shown under the heading ‘calls barred’ in the context of the operational changes which are stated to be

fraudulently made in the bank accounts of the Petitioners on e bank accounts of the Petitioners on 1<sup>st</sup> October, 2022.

3 The Petitioners' contention that, they had not received any 'sms/messages' in regard to other operational changes being made in the current account of the Petitioners from which the amounts have been siphoned off, needs to be certified by the said Police Authorities or the Mobile Company, that the non-delivery of such messages, was in fact, and as to what as urged by the Petitioners to be part of not only the hacking of the bank account, which was operated under the online banking system, but also the mobile number being hacked so as to prevent messages from the bank being noticed by the Petitioners.

4 The contention is that if the concerned mobile number was not to be a part of the hacking / fraud of the person who has siphoned off of the money from the Petitioners bank account, then certainly the Petitioners could have become aware that there are unauthorized operational changes, being made in respect of their bank account.

5 Accordingly, let the relevant material on an affidavit be placed on record by the Petitioners one day prior to the adjourned date of hearing. Copy of the same be also furnished to the learned Counsel for the Respondents.

6 If in the aforesaid context, the Petitioners approach the Cyber Cell or the concerned Mobile Company seeking necessary information, the same be furnished to the Petitioners or in the alternative, the same be made available to the Court by such agencies deputing their respective representatives, when the Court hears the matter on the adjourned date.

7 We also direct the Reserve Bank of India to file Reply Affidavit as the peculiar circumstances of the case would certainly warrant the Reserve Bank of India to respond.

8 As despite service, Reserve Bank of India is not represented, Advocate for the Petitioners to serve a fresh notice to the concerned officer of the Reserve Bank of India as also on the panel Advocates.

9 Stand over to 22<sup>nd</sup> February, 2024 – HOB.

10 Parties to act on an authenticated copy of this order.”

29. As can be seen from the aforesaid Order dated 15<sup>th</sup> February 2024, this Court sought further information and clarification in

respect of the remark “Call Barred” which was found in the said Cyber Cell Report and which was being relied upon by the Petitioners to submit that, on 1<sup>st</sup> October 2022, the messages regarding adding of beneficiaries had not been received on the mobile number registered with the bank.

30. Thereafter, the Cyber Cell of the Worli police station made another report which was forwarded by a letter dated 6<sup>th</sup> March 2024. This second report of the Cyber Cell was placed on record by the Petitioners by an Affidavit dated 6<sup>th</sup> March 2024. The said second report of the Cyber Cell states categorically at page 1 that, on 1<sup>st</sup> October 2022, no SMS was received from Respondent No.2 bank on the mobile number registered with the bank, being 9324265837. At page 1, it is further stated that, on 2<sup>nd</sup> October 2022, out of the total 23 SMSs, 20 were in respect of transactions and 3 were for OTPs. This information appearing on page 1 and part of page 2 of the said report was on the basis of CDR obtained from the service provider- Airtel. Further at page 2 of the said report, it is mentioned that, on the basis of the Order dated 15<sup>th</sup> February 2024 of this Court, a query was put to Airtel to explain the meaning of “Call Barred” and its operational consequences in detail to facilitate investigation. It is

further stated at page 2 that, on the said query being put to Airtel, it had replied as follows:-

“As per our CDRs there is nowhere reflecting term “Call Barred, hence it is not possible to explain exact meaning for the same”.

31. This shows that the term “Call Barred” was coined by Respondent No.2 and not by the service provider. This further substantiates the fact that, on 1<sup>st</sup> October 2022, when beneficiaries were added to the said bank account, no intimation was received by the Petitioners on their registered mobile number. Further, at pages 3 to 5 of the said report, the Cyber Cell has stated that, on 1<sup>st</sup> October 2022, no SMSs were received on the registered mobile number from Respondent No.2, and on 2<sup>nd</sup> October 2022, out of 23 SMSs received on the said registered mobile number, 20 SMSs were for the deduction of the amount of Rs.76,90,44.70/- and only 3 SMSs were for OTPs. The second report of the Cyber Cell, based on the information received from the mobile operator, Airtel, again clearly shows that, on 1<sup>st</sup> October 2022, when beneficiaries were added to the said bank account, no intimation was received by the Petitioners on the registered mobile number.

32. Further, Respondent No.2 also filed an Affidavit, being Additional Reply dated 15<sup>th</sup> February 2024, wherein it annexed a report provided by the IT- Operations team of Respondent No.2. The said Affidavit and the said report annexed to it (at pages 48 and 49 ) states that all the alerts were delivered on the registered email ID of the Petitioners on 1<sup>st</sup> October 2022 as well as 2<sup>nd</sup> October 2022. Hence it was the submission of Respondent No.2 that, even if the Petitioners had not received SMS messages when beneficiaries were added to the said bank account, they had definitely received email messages in that regard on the email ID registered with Respondent No.2. In the light of this Affidavit filed on behalf of Respondent No.2, this Court, by an Order dated 7<sup>th</sup> March 2024, gave the Petitioners leave to amend to implead the State of Maharashtra, through the Cyber Cell, as Respondent to the Petition. Further, by the said Order, it was directed that the Cyber Cell would be required to place on record on Affidavit as to how the emails which were generated by the bank in regard to the changes being made in the banking instructions were not received by the Petitioners, i.e., the emails, the details of which were set out at pages 48 and 49 of the Additional Affidavit in Reply filed by Respondent No.2.



33. Pursuant to the said Order, the Cyber Cell filed a 3<sup>rd</sup> report before this Court through a letter dated 14<sup>th</sup> March 2024. The said report states that an email dated 18<sup>th</sup> October 2022 was sent by the Cyber Cell to Rediff mail to get the information as to whether any emails had been received by the Petitioners on email [ID-vishyn@rediffmail.com](mailto:ID-vishyn@rediffmail.com) registered with the bank in respect of the concerned transactions. It is thereafter stated that an email was received from Rediff mail and in the said email information, namely Login IP address of [vishyn@rediffmail.com](mailto:vishyn@rediffmail.com) and contact address of [vishyn@rediffmail.com](mailto:vishyn@rediffmail.com) had been submitted. It is further stated in the report that the said information had been perused and upon pursuing the contact address of the email, namely [vishyn@rediffmail.com](mailto:vishyn@rediffmail.com) of the Petitioner, it was found that the Petitioners had not received any email on the email ID [vishyn@rediffmail.com](mailto:vishyn@rediffmail.com) from the email ID [donotreply@bankofbaroda](mailto:donotreply@bankofbaroda) of Respondent No.2. Thus, the said third report of the Cyber Cell categorically states that, contrary to what was alleged by Respondent No.2 in the report of its IT operations team at pages 48 and 49 of its Additional Affidavit in Reply, no emails were received on the said registered email ID of the Petitioners from Respondent No.2 either on 1<sup>st</sup> October 2022 or on 2<sup>nd</sup> October 2022.

34. Thus, the three reports of the Cyber Cell show that, when the beneficiaries were added to the said bank account of the Petitioners, the Petitioners did not receive any intimation in respect of the same either through SMS on the mobile number registered with the bank or any email on the email ID of the petitioner registered with the bank. We are satisfied from these three reports of the Cyber Cell that the Petitioners have not been negligent in respect of the debits made in their said bank account with Respondent No.2. On a perusal of the said three reports we are also satisfied that there is no collusion of the Petitioners with the persons/fraudsters who have debited the said bank account of the Petitioners. In the light of these three categorical reports by the Cyber Cell, which have been made after receiving information from the mobile service provider Airtel and the email service provider, Rediff mail, we are unable to accept the submission of Respondent No.2 that there was any negligence on the part of the Petitioners or that they had colluded with the persons/fraudsters who had debited the bank account of the Petitioners. In our view, from the said three reports of the Cyber Cell it is clear that both the bank and the Petitioners have been victims of fraud by third party fraudsters.

35. Respondent No.3-RBI has filed an Affidavit dated 13<sup>th</sup> March 2024 wherein it annexed its Circular dated 6<sup>th</sup> July 2017 in respect of

Limiting Liability of Customers in Unauthorized Electronic Banking Transactions. Paragraphs 6, 9 and 12 of the said Circular are relevant for the purposes of the present matter and are set out hereunder:-

**“(a) Zero Liability of a Customer**

6. A customer's entitlement to zero liability shall arise where the unauthorised transaction occurs 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 where the 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.

**Reversal Timeline for Zero Liability/ Limited Liability of customer**

9. On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. The credit shall be value dated to be as of the date of the unauthorised transaction.

**Burden of Proof**

12. The burden of proving customer liability in case of unauthorised electronic banking transactions shall lie on the bank.”

36. Further, Respondent No.2 has framed its own policy called the Consumer Protection Policy (Unauthorized Electronic Banking Transactions). The relevant portions of the said policy are as under:-

**Scenario 3: Third Party Breach - Unauthorized Electronic Banking Transaction happened due to Third Party breach:**

**Customer Liability** - Customer Liability will be ascertained based on the time taken by the customer to report the unauthorized

electronic banking transaction as per Table 1 & Table 2 mentioned in Annexure 1.

**Customer Right** - In such cases where customer has suffered loss due to third party breach where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system, and the customer has notified the Bank **within seven working days**. Customer is having the right to get the compensation from Bank, which is limited upto the value date unauthorised electronic banking transaction amount as per Table 1 - & Table 2 of Annexure 1. In such cases where customer has notified the unauthorized transaction to Bank after 7 days, Bank will have no liability, and this will suitably be communicated to the customer. Bank will try to pass the customer claim through Bank's Insurance Agency for that channel if available on best effort basis.

**Customer Obligation** - Customer is required to check the SMS / Email alert/ account statement and approach the Bank as soon as the customer becomes aware of the unauthorized electronic banking transaction debit

Table – 2

**Overall liability of the customer in third party breaches in such Unauthorized Electronic Banking Transaction where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system**

<b>Time taken to report the fraudulent transaction from the date of receiving the communication</b>	<b>Customer liability</b>
Within 3 working days	Zero liability
Withing 4 to 7 working days	The transaction value of the amount mentioned in table 1, whichever is lower
Beyond 7 working days	100% liability

37. Both as per the said RBI Circular and the said Policy of Respondent No.2, a customer has zero liability when the unauthorized transactions occur due to a third party breach where the deficiency lies neither with the bank nor with the customer but elsewhere in the system and the customer notifies the bank regarding

the unauthorized transactions within a certain time frame. Therefore, both as per the RBI Circular and the said Policy of Respondent No.2, the liability of the Petitioners in respect of the said unauthorized transactions would be zero as the unauthorized transactions have taken place due to a third party breach where the deficiency lies neither with Respondent No.2 nor with the Petitioners, as already held hereinabove on the basis of the said three Cyber Cell reports. In these circumstances, as per the RBI Circular and as per the Policy of Respondent No.2, the Petitioner is entitled to refund of the said amount from Respondent No.2. In this context, it is also important to note that, as per paragraph 12 of the RBI Circular, the burden of proving customer liability in case of unauthorized electronic bank transactions lies on the bank. In the present case, Respondent No.2 has no acceptable material to fasten any such liability on the part of the Petitioners. On the contrary, the three Cyber Cell Reports clearly show that the unauthorized transactions have taken place without any intimation to the Petitioners either on their mobile number registered with Respondent No.2 or on their email ID registered with Respondent No.2. For all the aforesaid reasons, Respondent No.2 will have to be directed to refund the amount illegally and unauthorizedly debited from the bank account of the Petitioners, to the Petitioners.

38. Further, for all the aforesaid reasons, Order dated 10<sup>th</sup> January 2023 of Respondent No.1 will also have to be quashed and set aside.

Paragraphs 2 and 3 of the said Order read as under:-

2. The complaint was examined in the light of the submissions and documents furnished by the bank. It is established that the transactions were completed post addition of beneficiaries and input of valid credentials/ 2FA known only to the account holder. Post reporting of the unauthorized transactions the bank also took up the matter with the beneficiary bank. No deficiency / lapse on the bank's part could be established. The bank has also intimated its stand to the complainant vide their email dated 09/01/2023.

3. Accordingly, the complaint has been closed under clause **16(2)(a)** of the Reserve Bank - Integrated Ombudsman Scheme, 2021, which reads as under:

"Complaint is rejected under Clause 16(2)(a) of the Reserve Bank - Integrated Ombudsman Scheme, 2021 :  
'In the opinion of the Ombudsman, there is no deficiency in service'

39. A perusal of the said findings shows that, while Respondent No.1 came to the conclusion that there was no deficiency/lapse on the part of Respondent No.2, Respondent No.1 did not make any proper inquiry as to whether the debit transactions had taken place with the authorisation of the Petitioners. Respondent No.1 has merely stated that it was established that the transactions were completed post addition of beneficiaries and input of valid credentials/2FA known only to the account holder. Respondent No.1 failed to appreciate that the adding of the beneficiaries and the debit transactions from the bank account of the Petitioners took place without any intimation to

the Petitioner either on their mobile number registered with Respondent No.2 or on their email ID registered with Respondent No.2, as is demonstrated by the 3 Cyber Cell Reports. In these circumstances, the Order dated 10<sup>th</sup> January 2023 would be required to be quashed and set aside.

40. In the light of the aforesaid discussion we pass the following Orders:

(a) Order dated 10<sup>th</sup> January 2023 passed by Respondent No.1 is hereby quashed and set aside.

(b) Respondent No.2 is directed to refund to the Petitioner an amount of Rs.76,90,017/- within a period of six weeks from the date of pronouncement of this Order with interest at the rate of 6% per annum from 2<sup>nd</sup> October 2022 till date of payment.

41. Rule is made absolute in the aforesaid terms.

42. In the facts and circumstances of the case there will be no order as to costs.

**(FIRDOSH P. POONIWALLA, J.)**

**(G. S. KULKARNI J.)**